

EUROPEAN PRIVACY AND HUMAN RIGHTS



EUROPEAN PRIVACY AND HUMAN RIGHTS

Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), are pleased to present the study "European Privacy and Human Rights (EPHR) 2010", funded by the European Commission's Special Programme "Fundamental Rights and Citizenship," 2007-2013.

TABLE OF CONTENTS

ABOUT EPHR	9
KEY FINDINGS.....	11
RESEARCH AND ANALYSIS.....	12
Summary of Country Developments	13
CRITERIA AND METRICS.....	42
METHODOLOGY	48
ACKNOWLEDGEMENTS.....	53
PRIVACY RESOURCES.....	61
 REPUBLIC OF AUSTRIA.....	 73
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	73
II. FOCUS AREAS.....	79
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	95
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION	96
 KINGDOM OF BELGIUM	 98
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	98
II. FOCUS AREAS.....	101
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	124
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	125
 REPUBLIC OF BULGARIA*	 126
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	126
II. FOCUS AREAS.....	132
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	147
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	148
 REPUBLIC OF CROATIA	 150
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	150
II. FOCUS AREAS.....	158
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	168
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	168
 REPUBLIC OF CYPRUS	 170
PRIVACY AND DATA PROTECTION FRAMEWORK.....	170
II. FOCUS AREAS.....	176

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	187
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	187
CZECH REPUBLIC	189
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	189
II. FOCUS AREAS.....	195
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	209
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	210
KINGDOM OF DENMARK	212
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	212
II. FOCUS AREAS.....	218
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	227
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	227
GREENLAND	229
REPUBLIC OF ESTONIA	230
I. STATE'S PRIVACY AND DATA PROTECTION FRAMEWORK	230
II. FOCUS AREAS.....	238
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	251
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	251
REPUBLIC OF FINLAND.....	253
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	253
II. FOCUS AREAS.....	259
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	277
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	277
FRENCH REPUBLIC	278
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	278
II. FOCUS AREAS.....	283
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	310
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	312
FEDERAL REPUBLIC OF GERMANY	313
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	313
II. FOCUS AREAS.....	318

Health & Genetic Privacy	332
III. Non-Governmental Organisations' Advocacy Work ON PRIVACY	334
IV. International Obligations & International Cooperation	336
HELLENIC REPUBLIC (GREECE)	338
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	338
II. FOCUS AREAS	343
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	354
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	354
REPUBLIC OF HUNGARY	356
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	356
II. FOCUS AREAS	362
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	376
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	377
REPUBLIC OF IRELAND	379
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	379
II. FOCUS AREAS	388
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	411
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	412
ITALIAN REPUBLIC*	413
I. PRIVACY AND DATA PROTECTION FRAMEWORK	413
II. FOCUS AREAS	422
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	438
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	439
REPUBLIC OF LATVIA	441
I. PRIVACY AND DATA PROTECTION FRAMEWORK	441
II. FOCUS AREAS	446
REPUBLIC OF LITHUANIA	460
I. PRIVACY AND DATA PROTECTION FRAMEWORK	460
II. FOCUS AREAS	472
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	488
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	489
GRAND DUCHY OF LUXEMBOURG	492

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	492
II. FOCUS AREAS.....	498
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	509
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	509
 REPUBLIC OF MACEDONIA	511
I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK	511
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	511
II. FOCUS AREAS.....	522
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	542
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	545
 KINGDOM OF THE NETHERLANDS	547
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	547
II. FOCUS AREAS.....	555
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	570
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	571
 KINGDOM OF NORWAY	573
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	573
II. FOCUS AREAS.....	579
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	601
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	601
 REPUBLIC OF POLAND	603
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	603
II. FOCUS AREAS.....	612
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	627
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	628
 REPUBLIC OF PORTUGAL.....	630
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	630
II. FOCUS AREAS.....	633
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	644
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	644
 ROMANIA.....	646
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	646
II. FOCUS AREAS.....	654

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	669
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	669
SLOVAK REPUBLIC	671
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	671
II. FOCUS AREAS.....	676
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	693
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	694
REPUBLIC OF SLOVENIA	696
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	696
II. FOCUS AREAS.....	702
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	711
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	711
KINGDOM OF SPAIN	712
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	712
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	712
II. FOCUS AREAS.....	720
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	735
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	735
KINGDOM OF SWEDEN	736
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	736
II. FOCUS AREAS.....	743
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY.....	762
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	762
SWISS CONFEDERATION (SWITZERLAND)	764
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	764
II. FOCUS AREAS.....	768
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	788
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	788
REPUBLIC OF TURKEY	790
I. PRIVACY AND DATA PROTECTION FRAMEWORK.....	790
II. FOCUS AREAS.....	794
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	802
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION ..	803

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND*	805
I. PRIVACY AND DATA PROTECTION FRAMEWORK	805
II. FOCUS AREAS	811
III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK	828
IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION	829
EUROPEAN UNION	830
I. PRIVACY AND DATA PROTECTION IN THE EU	830
KEY REGULATORY ACTORS	851

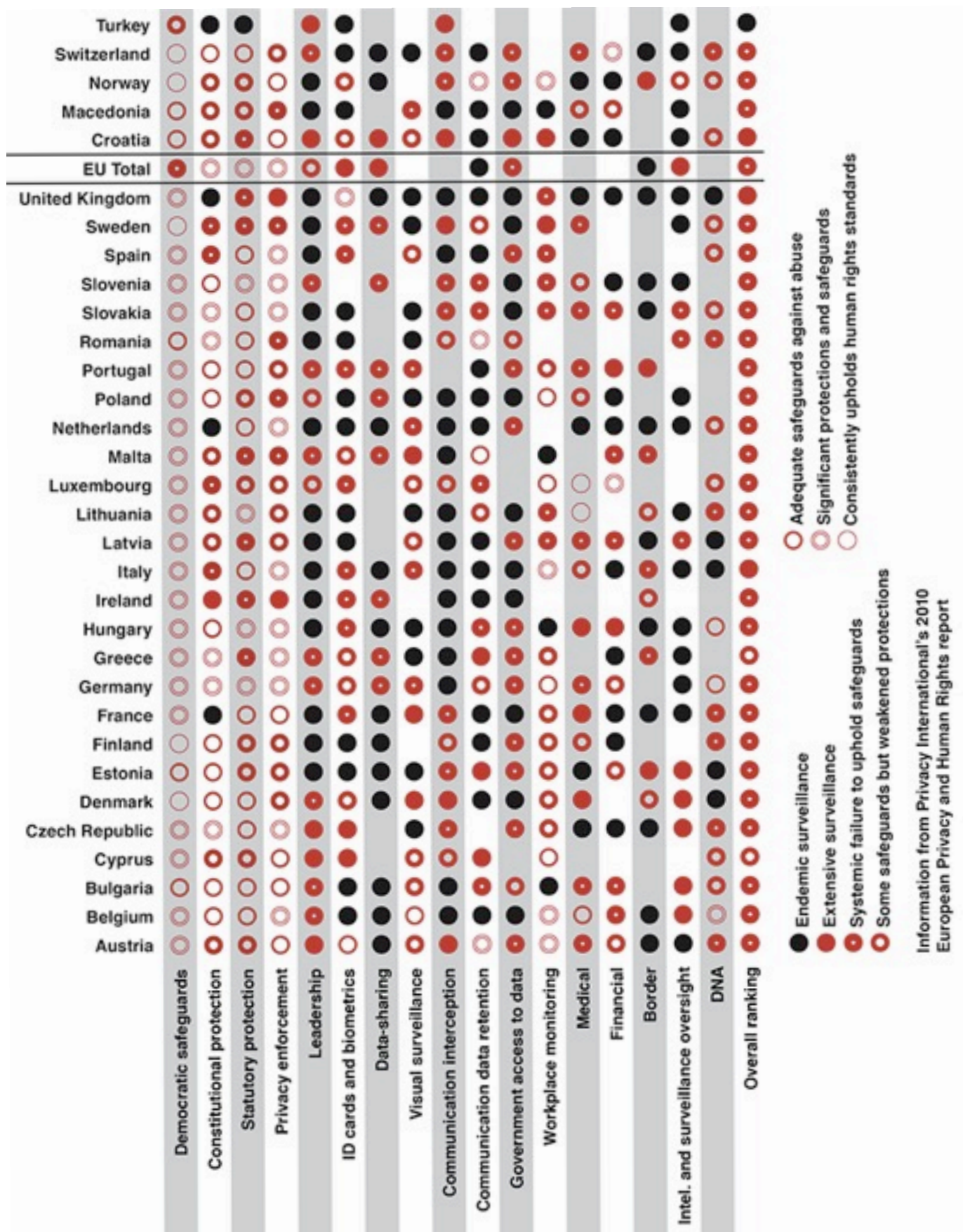
ABOUT EPHR

EPHR investigates the European landscape of national privacy/data protection laws and regulations as well as any other laws or recent factual developments with and impact on privacy. The study consists of 33 targeted reports, an overview presenting a comparative legal and policy analysis of main privacy topics and a privacy ratings for all the countries surveyed.

Privacy International has conducted an analysis of the country reports. Our research team has taken additional information from other sources to provide the summary information below for each country, noting the key developments and identifying the state of affairs.



This project was funded with the support of the Fundamental Rights and Citizenship Program of the European Commission.



KEY FINDINGS

Europe is the world's leader in privacy rights. But with leadership like this, we worry about the future. The Directive on Data Protection has been implemented across EU member states and beyond, but inconsistencies remain. Surveillance harmonisation that was once threatened is now in disarray. Yet there are so many loopholes and exemptions that it is increasingly challenging to get a full understanding of the privacy situations in European countries. The cloak of "national security" enshrouds many practices, minimises authorisation safeguards and prevents oversight.

The primary conclusion? The situation is mixed. And for a world leader, this is unconvincing and untenable.

Good

- European democracies are in generally good health, with the majority of countries having constitutional protections.
- Surveillance policies have faced obstacles across Europe, including political challenges, policy implementation problems, and resistance from regulators, civil society, the general public, and industry.
- European regulators are getting more and more complaints, which we take as a sign of increased awareness of privacy issues and awareness of the regulators' duties.
- Notification requirements for those placed under secret surveillance.
(Luxembourg, Switzerland, Czech Republic)

Heroic

- Greece: in 2007 there was a collective resignation from the regulator in protest against the government's insistence on repurposing the Olympics' surveillance system.
- Germany: groups mounted a campaign against communications data retention in which 34,000 people filed a case at the Constitutional Court appealing against the law.
- Netherlands: policy on mandatory smart meters had to be withdrawn after opposition.
- UK: NGOs mounted policy campaigns against the surveillance policies of the previous government, resulting in policy repeal on issues ranging from ID cards and biometric passports, to DNA practices, and large databases.

Awkward

- Many of the ambitious surveillance proposals have failed in implementation.
- Deployment of biometric passports and data retention is fragmented.
- Cutbacks have affected regulators' abilities to do their jobs, e.g. Latvia, Romania.

- Ministerial warrants still exist in too many countries, i.e., Ireland, Malta, UK.
- Access to financial data is on the rise, e.g. Belgium, Croatia, Czech Republic, France, Germany, Greece, Italy, Norway, Poland, Slovenia.
- Failed oversight mechanisms, e.g. Sweden's commissioner over covert surveillance powers resigned in protest.

Bad

- Inability to build safeguards into processes to gain access to information over new services, e.g. France, Germany, Switzerland seeking powers to conduct secret searches of computers, Ireland's ambiguous powers for unwarranted interception of VoIP; Italy building "backdoors" into systems; Bulgaria's "black boxes" at ISPs.
- France: Attempt to ignore constitutional amendment proposals to include an explicit constitutional right to privacy.
- eHealth systems with security faults and/or centralised registries (France, Germany, Italy, Netherlands).
- Biometric registries and databases emerging and with more coming (Estonia, Italy, Lithuania, Netherlands).
- Few protections and safeguards for government access to data (most countries).
- Illegal and warrantless surveillance still occurs.
- Journalists and dissident groups are under surveillance (Lithuania, FYRM, Poland, Romania, Slovakia, Turkey).

Ugly

- Direct access to information held by third parties without warrants or oversight, conducted by unaccountable bodies (e.g. Bulgaria, Croatia).
- Inability to audit and review the actions of security services. (e.g. Lithuania, Croatia, Estonia, Hungary, Sweden).
- Medical databases are emerging with centralised registries. (e.g. Croatia, Czech Republic, Denmark, Sweden, Norway, UK).

RESEARCH AND ANALYSIS

We conducted research on each country, relying for the most part on the country reports from our partners. We reviewed each country report and created a summary of the key developments as they were relevant to the ratings scheme. When information was missing we tried to supplement it with information from other sources.

Summary of Country Developments

Below is the list of countries and the summaries of our findings:

Austria	9
Belgium	11
Bulgaria	12
Croatia	13
Cyprus	13
Czech Republic	14
Denmark	15
Estonia	16
Finland	16
France	17
Germany	18
Greece	19
Hungary	20
Ireland	20
Italy	21
Latvia	22
Lithuania	22
Luxembourg	23
Former Yugoslav Republic Of Macedonia	24
Malta	24
Netherlands	25
Norway	26
Poland	27
Portugal	27
Romania	28
Slovakia	29
Slovenia	29
Spain	30
Sweden	30
Switzerland	31
Turkey	32
United Kingdom	32
EU	33

Austria

Assessment: Impressive that the Government has not implemented data retention, though there are some concerns about the extent of data sharing particularly for border surveillance.

- no explicit constitutional protection, though there is a federal law with a number of constitutional provisions including data protection as a fundamental right; constitutional amendment failed but protections are in existence nonetheless; adherence to ECHR in Constitutional Court decisions though Court dismissed a case on police access to data, but also ruled that access to data held by ISPs for copyright is not necessary
- substantial amendments were done to improve the previous data protection law, and has remedies for interferences; also include sectoral laws and laws applying to specific domains (communications, genetics, medical, financial)
- regulator can order controllers to respond appropriately to requests for information; includes judicial staff members; increase in number of cases; and can bring criminal charges; high rate of success in cases despite staffing shortages
- regulator still lacks independence despite being notified in 2005 of this problem by the European Commission
- centralisation of data on students has been regulated down from 60 years to 20 years retention with more limitations on access and use
- judicial warrants for interception of communications where a crime is punishable by one year or more of imprisonment - this is quite low threshold; dragnet investigations are possible for complex investigations into crimes punishable by more than ten years' imprisonment, and a sunset on this provision was repealed
- access to data laws were changed to increase availability, particularly in emergencies, and without court orders; Constitutional Court dismissed a case calling this practice into question
- government has been proposing the use of Trojans to gain access to computer systems, but plans are currently in stasis
- has not implemented the Data Retention Directive, as the issue is controversial in Austria
- extensive power for audio-surveillance collection though not used too often
- regulator has ruled in favour of medical privacy, e.g. preventing researchers from gaining access to medical data of drug-addicted convicts who underwent rehabilitation
- extended use of Schengen Information System, e.g. for issuance of driver's licences
- reports of plans for granting access to data by foreign government, i.e. granting US authorities access to DNA databases, fingerprint data, etc.
- growing use of CCTV, though some safeguards have been introduced including proportionality, emphasis on real-time rather than recording, deletion after 72 hours

- collects two fingerprints for biometric passports, but the data is stored only on the chip and minors under the age of 12 are not fingerprinted; has an e-card social security smart card; mandatory citizen card has been abandoned
- Supreme Court ruled in favour of workplace privacy re: restricting biometric time reading scanner on grounds of human dignity
- employers may not monitor private communications of employees, provided they are labelled as such; employers may not use CCTV except to monitor objects
- lower threshold of protections for medical information in information systems, with wide access provisions for authorised staff
- recent reduced protections on data sharing with other countries regarding financial accounts; though banks are regulated in how they can use personal information, including creditworthiness
- currently dealing with a proposed "Transparency Database", run by a private company, that will contain net income and social benefits per individual, though there are safeguards on who has access.
- DNA taken for only for those charged with serious crimes and from convicted, but retention is indefinite for convicts, suspects' information only removed upon acquittal and upon request; profile is retained even upon acquittal
- government boasts that it is amongst the leading countries in the world regarding DNA, also led the Prüm treaty for data sharing within Europe

Belgium

Assessment: Although legal situation is strong with an active civil society, technological surveillance measures are problematic, e.g. data retention regime, unique ID for travel.

- Belgian constitution recognises the right to privacy and private communications; courts have ruled on privacy cases, including on access to subscriber data, preventing disclosure
- specific laws apply to electronic communications, regulation of camera surveillance, medical privacy, consumer credit, social security, amongst others
- data protection legal regime has been criticised for not adhering to EU requirements; but Belgium has now fully implemented EU directives into law.
- DPA reports to Parliament; has greater capacities with 55 members of staff, though the numbers of complaints are relatively low; publishes a number of guidances and recommendations on data processing
- also have committees that oversee specific areas of activities, e.g. social security and health, national registry, etc.
- extensive regime of law for communications surveillance: access to communications is authorised by judiciary, though appears to be an investigatory

judicial authority; can demand the decryption of data and compelling network managers to comply with orders; significant numbers of interception orders and they are increasing

- law in 2001 banned anonymity for telecommunications subscribers, and can prohibit any services that hinders the application of wiretapping law;
- 1 year data retention up to 3 years, with police favouring three-year policy, though not fully in place; industry has opposed extensive surveillance
- in 2005 established a new agency for "threat analysis", by evaluating secret surveillance information held by other intelligence agencies, which the DPA argues is lacking in appropriate safeguards
- extensive plan for surveillance of all vehicles and movement in Belgium
- one of the first countries to implement RFID in passports
- one of the first countries to implement "smart IDs" for digital signatures, and a unique identifying number across government services; and the eID can now be used for purchasing train tickets despite privacy issues
- includes children's ID for use on the internet
- considerable debate followed introduction of RFID in Brussels public transportation system
- there are common rules for workplace surveillance, and guidance from the Commission
- eHealth platform, which is not mandatory, for sharing information within health care system, based on consent and in-built protections
- banking secrecy still applies, though there is a draft bill to give greater powers to financial investigators
- leadership: government has sponsored the creation of an Internet Rights Observatory
- an active NGO network raising issues
- has not ratified CoE convention on cybercrime
- DNA of those convicted of "serious offence", retention of 10 years for those convicted; sample is destroyed upon creation of profile

Bulgaria

Assessment: Very worrying developments particularly in secret surveillance and oversight.

- Constitution consists of detailed provisions for privacy, communications, and access to information.

- many changes to data protection law, sometimes contradictory directions; law includes fining powers
- extensive list of other laws that covers privacy
- Regulator is independent and elected by Parliament, and has order making powers
- awareness of the office is high, having received 45000 requests for information in 2009, though only 158 complaints
- national security argument is prevailing and lowering the obstacles to gaining access to information held by private sector organisations
- little oversight of national security services use of communications interception, and there is a history of abuses
- policy change is in progress to remedy this; with a Parliamentary sub-committee entrusted with oversight
- no official statistics available on the use of intercepts
- no consultation on the data retention policy, with government seeking direct access to databases of traffic data, resulting in significant criticism; later taken to court and Court ruled that data can only be accessed after a warrant has been issued
- two different governments have continued to try to gain direct access to data-stores
- significant clamp-down on anonymous use of the internet, e.g. website hosting companies
- ID contains biometric data
- collect DNA, and violations on the use of DNA have been identified by the regulator; collected from those indicted for a premeditated crime, deleted when no further reason based on the merits of the case (case-by-case basis);
- no clear framework of safeguards against workplace surveillance
- some safeguards are in place for medical privacy, including specific laws
- has not ratified CoE convention on cybercrime

Croatia

Assessment: A debate about privacy is emerging in the country, which is promising. Communications surveillance and oversight are worrying.

- Constitution protects both privacy and data protection
- data protection law includes the power to fine, though for small amounts, but imprisonment is an option; though power has never been used
- European Commission has stated that Data Protection Act still requires additional work to achieve full alignment for EU membership

- two additional regulations for data protection for record systems and special categories of personal data; but no sectoral protections
- regulator is an independent body and reports to Parliament; has order-making powers, and in 2008 dealt with 626 cases
- communications surveillance authorised by Supreme Court or investigatory judges but for a maximum of 7 months, and supervisory powers are weak as little oversight of intelligence agencies
- central authority claims the right to conduct interception on behalf of agencies, rather than having to contact service providers; and is an unsupervised body
- Communications data retention for twelve months for all data collected by service providers
- developing plans for mandatory SIM-registration policy for mobile phones
- growing use of CCTV, even in some schools but public opposition has arisen
- biometric passports have been proposed but not implemented
- trying to reduce the use of a single unique identifier
- workplace surveillance practices are growing, and there have been calls for a review and some regulatory guidance
- wide-scale data sharing of financial data is possible, and changes to the Bank Act have allowed for greater use of information
- centralised medical information system has a lack of safeguards and did not involve notice or consent of citizens
- Convention on cybercrime has been incorporated into national law
- DNA collected if identity is questionable in an investigation, retention of DNA from convicted individuals for twenty years

Cyprus

Assessment: Limited information so unable to make a full assessment, though some promising developments, e.g. workplace surveillance.

- Constitution protects privacy and communications
- data protection law was found to be not consistent with the EC Directive on the right of information, transfer to third countries, and some procedural mechanisms; we are unaware of whether this situation has been improved
- regulator is appointed by Council of Ministers, in consultation with Parliament, so is not entirely independent; head of the regulatory authority must have been a judge on the Supreme Court
- regulator may investigate complaints but may also conduct inquiries on his own initiative

- low level of complaints in the country, but runs public awareness initiatives
- regulates the collection of fingerprints in the workplace and reserves it only for exceptional cases
- communications surveillance requires a court order, though Attorney General may now authorise in order to save time; 2006 law also allowed police to monitor web logs, downloads and emails
- no strong legal protections regarding CCTV, regulator has intervened and requires a justification prior to installation
- workplace surveillance cases have included secret microphones being used
- workplace surveillance is regulated by the authority's Employment Order
- has ratified the CoE Convention on Cybercrime
- DNA: all convicted persons and suspects; removed when record is cleared; suspects' profiles are removed when they are acquitted or otherwise cleared

Czech Republic

Assessment: Good developments due to the hard work of civil society and the national regulator; though problematic legal regimes still exist despite some work, e.g. communications surveillance, CCTV, ID.

- Charter of rights and basic freedoms provides for the right to privacy and human dignity, protection of communications, and a data protection clause as well
- data protection law fully harmonised, and contains additional protections due to amendments, including recordings of communications
- regulator can impose fines of up to €820,000 and conduct audits
- number of complaints is rising, number of cases dismissed also quite high
- regulator has supervisory authority over the use of birth numbers, though over-use still continues
- regulator has conducted vast awareness-raising exercises
- Communications interception is authorised by a high court judge, even if done by intelligence agencies (though there are still concerns of abuses), and there is a notification requirement once the case is closed
- due to complaints about little oversight of communications surveillance, so new protections were introduced in 2009
- still attempts to expand intelligence agencies' powers
- 12 month data retention policy was changed to introduce graduated retention for various forms of data; and scope of use is expansive, and no oversight
- led initiative to sign agreements with US for the transfer of passenger data

- increasing use of CCTV, and regulator has insufficient power to regulate this activity, with some strong opposition from the public against these systems
- biometric passports include face and fingerprint data
- ID cards are increasingly being used in everyday life
- "anonymous" RFID cards are now available for travel in Prague
- a number of medical registries exist, with uncertain legal status; President had to veto a law that was to expand use of birth identification numbers, but this veto was overridden
- financial surveillance law introduced to limit lawyer-client privilege and solicitors must now report suspicious transactions
- strong civil society groups
- has not ratified CoE convention on cybercrime
- DNA: from all convicted persons, and profiles are kept for eighty years, and samples are retained for this period too

Denmark

Assessment: Communications surveillance regime in need of oversight. Use of unique identifier across society is worrying, as is the growth in CCTV use, DNA regime is likely to contravene ECHR.

- constitutional protection to privacy and, indirectly, data protection
- changes to data protection law allows for increased data sharing
- intelligence agencies are exempted from privacy laws
- sectoral laws provide protections for medical information, financial information, and marketing
- regulator is claimed to be an independent public body, but key staff are appointed by the Minister of Justice
- high level of complaints received; regulator gets involved in high profile cases (e.g. immigration system, Facebook)
- communications surveillance law allows for police to gain access to a list of all active mobile phones near a scene of a crime; government also considered idea of allowing wide-scale interception of communications in an area
- high levels of wiretapping requests and approvals to the courts
- 12 months data retention implemented by administrative order despite vocal opposition, though since then some changes to exclude smaller ISPs
- biometric passport includes facial recognition but no fingerprints as yet
- no ID card but a unique number is still used to identify on public registers

- cases emerging on workplace surveillance, and have led to small fine
- CCTV rules relaxed, and thus becoming more widespread
- eHealth portal with central register, but provides citizens' access to their own medical records, and uses authenticated access; world leader in centralised record-keeping
- DNA: collected from convicted persons and suspects charged for offence that could lead to more than 1.5 years in prison; retained for both suspects and convicts until two years after death; and samples retained

Estonia

Assessment: Legal framework is there, but policies and technologies are amongst the worst in Europe.

- Constitution applies to privacy, communications, and data protection; high courts have dealt with privacy cases though the results are mixed, but more recent jurisprudence shows some interest in expanding privacy
- data protection framework treats biometric and genetic data as "sensitive"
- regulator has fining powers, but fines are quite small; regulator was made independent in 2007, though operates under the Ministry of Justice; relatively small office, though activity is increasing
- surveillance is authorised by head of agencies
- communications surveillance, however, requires authority of investigation judge
- 12 month data retention law
- use of databases and data analysis powers by law enforcement and national security are problematic
- increasing use of CCTV, though there is a lack of official data on the matter; draft legislation on CCTV is in Parliament
- mandatory ID cards includes register of biometrics including iris, fingerprint, and face; card is multipurpose and holds additional information and identifiers
- few sectoral laws, though one on credit information
- workplace surveillance law exists but there is no regulation or case law as yet
- mandatory eHealth record system without opportunity to oppose the processing of information
- established an agreement with the U.S. for transfer of passenger data
- ratified CoE convention on cybercrime
- DNA: arrested or convicted for any "recordable offence"; kept for ten years after death for both suspects and convicts, and samples retained indefinitely

Finland

Assessment: Regulator is working hard on increasing awareness. Surveillance plans seem to be unabated by policy deliberations that have occurred elsewhere.

- constitutional right to privacy and communications; a number of cases have been decided
- comprehensive data protection law includes civil and criminal sanctions (imprisonment for up to 1 year)
- complaints to regulator increasing dramatically, indicating a stronger awareness of rights
- judicial orders for interception of communications
- retention of traffic data for 12 months
- access to income data is widespread, e.g. even in the calculation of traffic fines
- generalised surveillance is permitted in the workplace; though permitted to investigate loss of intellectual property
- multipurpose ID with information from various sources including medical insurance data is on the card
- DNA: taken from convicts serving 3 years or more, suspects charged of a crime punishable by 6 months or more; profiles kept for ten years after death, suspects profiles deleted within one year of dismissal; samples retained for same periods
- ratified CoE convention on Cybercrime

France

Assessment: Worryingly coming close to being crowned as Europe's leading Surveillance State. New databases and surveillance practices emerging continually; despite the hard work of regulator and civil society, some of the weakest safeguards in Europe.

- not explicitly named in the constitution but has been ruled to be implicit; though there have been recommendations to include within constitutional reform it has been ignored by the President
- comprehensive law, and sectoral laws for archives, video surveillance, employment, and consumer protection
- CNIL does much work around the world; has fining powers that not used extensively, and has limited powers over some areas of government activity
- level of legal activity is quite high
- new policing powers have been deployed with worrying implications, e.g. LOPPSI2 to remotely access, record, collect and transfer information held on IT systems
- police may gain access to logs without judicial orders in terrorism cases

- has law on the use of PNR
- 12 month retention law, and may be used for intellectual property rights cases; requires retention of identifying information of subscribers
- police and intelligence agencies have established a platform to grant themselves easy access to traffic data
- strong level of civil society and regulatory action, but unfortunately only small changes in government policy are attained
- many new databases and systems have been established to monitor various groups; some with very high error rates
- expansive use of CCTV
- biometrics collected for border management and for passports, though no sign of fingerprints in passports
- proposed expanded ID card project is still in suspension following protests and criticism
- workplace privacy rulings have allowed for reading of emails by employers, but abuse of internet activities is insufficient for termination of contract
- national ehealth records system, but with serious lack of data protection and many security breaches; the system is under revision but other problems prevail
- financial surveillance has twice breached ECHR according to the ECtHR
- DNA: taken from convicts or those charged with "serious offence"; convicts retained for 25 years, suspects' removed by motion of prosecutor; samples retained similarly

Germany

Assessment: Strong legal and regulatory framework, amongst the best in the world with highly competent regulators and civil society; but the actions of the Government and security services seriously degrade protections.

- constitutional protections for privacy of communications; though the Federal Constitutional Court in 1983 also created the right of informational self-determination; court rulings have been mostly privacy protective
- data protection law is amongst the strictest in Germany; amendments have added areas of regulation include video surveillance, smart cards, anonymisation, etc.
- additional legal protections were created in 2008 for employee privacy
- federal and state regulators are amongst the most meticulous and world-leading
- communications surveillance regime allows for warrantless automated wiretaps; vast use of communications surveillance powers, amongst highest in the world; studies have indicated that unlawful interception occurs

- government sought power to conduct secret searches of computers, was ruled unconstitutional by the Federal Constitutional Court, though they could be conducted with a judicial warrant
- subscriber information must be recorded even for pre-paid communications services
- 6 months data retention policy, but access is regulated by a judicial warrant for investigations on an enumerated list
- active civil society is an example to the world: 34,000 people filed a case at the Constitutional Court appealing against data retention
- expanding use of CCTV and visual surveillance techniques, though the courts and regulators have been active in opposing plans (including in one case a museum camera could see into the Chancellor's private flat)
- police may use GPS technologies to track suspects in cases of serious crimes, even without a judicial warrant
- increased plans for travel surveillance and road surveillance, and the removal of safeguards that were originally implemented when the systems went live
- biometric passports include fingerprints, but they are not stored on central or local databases
- ID cards are mandatory; though ID cards may incorporate fingerprints, on a voluntary basis, as the original mandatory plan faced considerable public opposition
- use of body scanners in Hamburg Airport, though it is optional
- genetic diagnostic law bans the use of genetic examinations for employment; biometrics may only be used in the workplace with approval of workers' council/ arbitration board
- rollout of ehealth ID suspended due to security concerns; now there are plans for a "secure patient data management system"
- no specific financial privacy law, but is customary law; though now have an automated means for authority to gain access to financial information
- has not ratified CoE convention on cybercrime, but was part of the Prüm convention process
- DNA: taken from convicts of a serious offence or repeatedly committing same minor offence, and from suspects charged of serious offence; removed when no longer necessary; samples retained similarly

Greece

Assessment: A rich and controversial history of privacy, with whole-scale abuse, and political upheaval. While many promising developments occurred in the mid 2000s, since

then the Government has repeatedly failed to implement necessary safeguards, and so surveillance continues.

- constitutional protections for privacy and communications, and through an amendment, a constitutional right to data protection through an independent authority
- comprehensive data protection law has been amended to update definitions of personal data and deal with transborder data flows, but also to exclude CCTV from the Act
- regulator is independent, run by a judge, and may issue administrative and penal sanctions, including mid-level financial fines; historically has played a significant role in policy debates, and has made a number of judgments
- in 2007 there was a collective resignation from the regulator in protest to the CCTV developments
- oversight bodies exist for communications surveillance; had fined Vodafone and Ericsson for abuses in interception of communications but this was overturned by the Constitutional Court
- following abuses, new law was introduced in 2008 to protect telecommunications privacy, requiring a security policy for each service provider, and require audits, and new penalties for abuses
- Government promised a new Security Plan to protect communications but no action has been taken by the Government
- while there is no retention law, there is extensive retention of communications data varying from 2-5 years
- repurposing of CCTV installed for the Olympics has been controversial; but now it is expanding even more so, including into schools and was exempted from law
- introduced law to require SIM-registration
- ID system administered by police includes collection of detailed information, though no longer collects religious information
- use of biometrics in workplace has been regulated to highly sensitive transactions
- regulator prevented the use of biometrics of Athens airport
- financial privacy is being eroded, for both taxation and credit reporting

Hungary

Assessment: Worrying developments in political process in Hungary have had serious implications for the privacy landscape. Weak oversight requires attention.

- constitutional protection for privacy and protection of personal data

- comprehensive data protection law was previously deemed "adequate" for trans-border data flows prior to joining the EU
- there are many sector-specific laws regarding addresses, identification codes, medical information, police information, etc. and even bio-banks, though the regulation is weak
- regulator can investigate complaints, and has order-making powers; though independent, the regulator often receives political pressure, and there are possibilities of weakening powers
- number of complaints and cases continue to rise; and a number of high profile cases
- established an agreement with the U.S. for transfer of passenger data
- growing use of CCTV, extended retention periods
- communications surveillance require a court order and is limited to crimes punishable by 5 years or more
- reports have emerged of the use of "black boxes" on service providers' networks to intercept communications without a warrant
- Constitutional Court has noted that there are serious oversight problems
- communications data retention in law in 2008, with a pending case calling for its annulment
- joined the Prüm convention to enable data sharing with other EU countries
- workplace surveillance cases include Vodafone monitoring the movements of their employees without notice; lack of regulation in this domain
- passports include fingerprints
- lack of regulations and promotion of data sharing in health and financial information
- active civil society
- ratified CoE convention
- DNA: taken from those convicted of specific crimes or suspects in investigations punishable by 5 years or more; convicts' data kept for 20 years, suspects are retained until proceeding is abandoned/acquittal; samples destroyed similarly

Ireland

Overall: Weaker regulatory enforcement and oversight process is problematic particularly for communications surveillance.

- no express right to privacy in the constitution, jurisprudence has indicated it is implied under the "personal rights" provisions
- comprehensive data protection regime has been amended to update its protections

- regulator is independent; and can serve enforcement notices; has been criticised for weak decisions on Google
- communications interception is authorised by Ministerial warrants, and overseen by a Judge of the High Court; law is drafted with a limited jurisdiction, possibly permitting warrantless interception of VOIP
- retention policy is amongst one of the worst, previously with extensive retention in an unregulated manner, then a 3-year retention scheme, now a 2 year scheme for telephone and 1 year for internet data
- no external approval is needed for access to traffic data

Italy

Assessment: Chaotic legislative environment leads to erratic protections. Lack of oversight in national security and law enforcement; but the privacy regulator and active civil society have played key roles in protecting privacy.

- no explicit protection of privacy in the constitution, though there are protections for communications and the home
- after two decades of debate, comprehensive data protection law enacted in 1996; updated in 2003 to incorporate new EU directives
- additional laws relating to video, workplace surveillance, statistical information, electronic files
- regulator has conducted investigations in variety of sectors and has been involved in high profile and highly influential cases
- halted biometric registration systems
- extensive legal framework for communications surveillance, and there are legislative plans to further regulate illegal wiretaps; yet pre-emptive interception occurs at the discretion of the Attorney General
- there have been cases of "backdoors" being built into services resulting in over-surveillance, including one case where the communications of 30,000 subscribers were violated
- interception rates are very high and it is unknown how many illegal interceptions take place
- signed on to Prüm and established a DNA database as a result; retention is for 40 years for the profiles, and 20 years for biological samples
- video surveillance is growing, though the regulator is quite active in this space
- biometric passports were to include fingerprints, but they were not to be stored in a central database; but no action has been taken

- attempted to implement ID system with centralised record store; but it was dismantled in 2009; a new system with a centrally recorded fingerprint has been delayed
- workplace surveillance rules bar the spying on employees web surfing habits
- ehealth initiatives involve centralised registers, though again the regulator is involved
- financial privacy was hampered by the dissemination on the internet of all tax returns
- active civil society
- ratified CoE convention on cybercrime

Latvia

Assessment: Some problematic limitation and oversight problems, particularly in communications surveillance and DNA. Modifications to data protection law to increase exemptions is problematic as well.

- constitutional protection covers privacy and communications
- comprehensive law, though amendments recently have included limitations on individuals' rights in state financial and insurance affairs, and again to permit processing of medial information
- laws exist for electronic communications and the DNA database
- regulator is under the jurisdiction of the Ministry of Justice; despite attempts to improve independence, plans have been postponed repeatedly
- regulator's office suffered staffing cutbacks in 2009
- communications surveillance is regulated to specific investigations
- supervising authority authorises surveillance, though this could be a prosecutor (in emergencies) or a judge
- tracking is only permissible with judicial authorisation
- cases of illegal interception have arisen
- law enforcement agencies can gain now access to information held by credit agencies in order to combat terrorism
- 18 month retention period
- CCTV is overseen by regulator
- biometric passports include fingerprints
- compulsory identity cards for all residents
- employers may monitor the communications of employees

- specific legal regime for medical privacy, even after death; though allows for medical research if de-identified
- ratified CoE Convention on cybercrime
- established an agreement with the U.S. for transfer of passenger data
- DNA: taken from those convicted or suspected of any "recordable offence"; retained for 75 years; and samples also retained

Lithuania

Assessment: This country is still learning the elements of privacy, but there are some promising developments particularly as the Supreme Court develops case law. The surveillance laws are open to abuse by government authorities, and stricter procedures are required.

- constitution protects privacy and communications, and the Supreme Court has reaffirmed the right to a private life is one of the most fundamental human rights
- significant upgrades to the data protection law in order to join the EU, completed in 2003/2004
- more recent changes include adding video surveillance to the law, restricting use of personal identification numbers, and more stringent protections on medical information, and independence of the regulator was strengthened
- low number of complaints reflects a lack of awareness levels in the country; though the numbers are rising
- judicial authorisation required for interception, though there isn't strict scrutiny, and the law has been criticised for being unclear, and the lack of clear procedures to prevent abuse by the State Security Department
- there are recent claims about the wiretapping of journalists
- retention law was implemented in 2009, for 6 months period unless the data is necessary for ongoing operations at which point it is retained for a further 6 months; though constitutional court decision of 2002 requires that this is restricted to data collected for normal business operations
- established an agreement with the U.S. for transfer of passenger data
- growing use of CCTV though regulator is working on the issue; though there are some cases of secret surveillance; and there has been much debate on the issue
- biometric passports include fingerprints, including the storage of biometrics on central register
- increasing use of surveillance techniques in workplaces and there is limited debate, and the courts tend to side with the employers
- ratified CoE Convention on Cybercrime

- DNA: taken from all convicts and suspects; all profiles retained for 100 years; samples must be destroyed upon creation of profile

Luxembourg

Assessment: limited resources for regulator but legal frameworks are in place. Financial privacy is strong. Some safeguards across society but we lack sufficient information on actions of security agencies.

- constitution guarantees the right to privacy and secrecy of correspondence
- comprehensive data protection law
- regulator has a small office; but can investigate on its own initiative, and issue financial penalties, and has order making powers and has dealt with some cases
- judicial warrants required for interception of communications, with some notification requirements
- 12 months retention of communications traffic, but requires a clear definition of the types of investigations where police can access the information
- regulations are in place for CCTV
- workplace monitoring is governed by law
- unique identity number of every resident, and widely used; fingerprint in passports, though removed from central register after 1 month
- strong laws on financial privacy
- party to the Prüm treaty
- DNA: taken from convicts from specific offences, and suspects of any recordable offence; convicts data retained for life plus ten years, suspects deleted upon acquittal; samples retained similarly

Former Yugoslav Republic Of Macedonia

Assessment: Despite strong frameworks of protections in place, abuses continue and poor surveillance practices persist without adequate remedies.

- constitutional protection for privacy, secrecy of communications, and data protection
- comprehensive data protection law in place, including recent amendments to strengthen the legal framework, including greater investigatory powers for the regulator
- regulator is independent and reports to Parliament (but has already faced political challenges), and will be relatively large in size; and has worked on public awareness programmes
- unique identifier in place

- despite legal regime, there are problems with communications surveillance regime, e.g. journalists are subjected to spying
- legal obligation on telcos to provide direct and uninhibited access to traffic and other data to the Ministry of Interior without notice or court order
- 24 month data retention regime
- growing number of CCTV, though it is supposed to be regulated
- passports use fingerprints; and national ID also uses biometrics
- no special protections for workplace privacy
- ratified cybercrime convention

Malta

Assessment: Privacy expertise and cases are emerging. Communications surveillance regime is problematic, as is surveillance oversight.

- constitution guarantees privacy protection, with some cases emerging
- comprehensive law in accordance with EC Directive
- regulator is independent, and works closely with other regulators in Malta and internationally
- small number of complaints received, but awareness building campaigns are being run
- worries about CCTV are high on the list of complaints
- warrants for interception of communications are issued by the Minister responsible for security services
- retention for 12 months for telephony data, six months retention for internet data, and some limitations on access
- passport biometrics are stored on the passport, but no plans to include on identity documents
- Government is considering full-body scanners, but no decision as yet
- no guidelines on workplace surveillance; although there are complaints to the regulator, none are actually formal complaints because employees are concerned about their position in the workplace
- guidelines are in place for financial privacy

Netherlands

Assessment: Strong tradition of civil liberties and privacy is being replaced with ambitious technological programmes and weak oversight. Strong regulator and civil society, and sometimes industry, work hard to draw attention to myriad of proposals and policies.

- constitutional guarantees to privacy and data protection; there were proposals to expand the data protection rights, and a new Commission has been appointed to review this
- comprehensive data protection, but there are plans to amend it particularly for third-country transfers, direct marketing
- additional laws regulate use of personal information by the police, in medical examinations and treatment, social security
- regulator is independent, though with limited fining powers; and has been given new powers in recent years, the latest promises from the Government have not yet been followed up on
- regulator is vocal in policy developments in the country, and is an international leader
- spread of road surveillance is increasing
- serious problems with jurisprudence on copyright infringement cases have reduced privacy of subscribers to internet service providers
- intelligence agencies do not require court order for communications surveillance
- several proposals to grant increased surveillance powers to law enforcement agencies
- police also monitoring social networking activities through a pilot
- Parliament rejected additional safeguards for data retention; retention period was set at 18 months, but reduced to 12 months
- Camera Surveillance Act allows images to be retained for four weeks
- notable victory for privacy protection by civil society pushing back against smart meters policy
- biometric passports to include fingerprints, and government wanted to store data on central database
- travel surveillance is expanding significantly, with data being retained for seven years
- plans for electronic patient file are being put in place with significant concerns raised
- use of identifier for financial transactions has drawn attention of regulator
- ratified cybercrime convention
- DNA: taken from anyone convicted or suspected of recordable offence; profiles kept until convict is 100 years old, suspects removed upon acquittal; samples retained similarly

Norway

Assessment: Increasing oversight over security agencies appears promising. Financial privacy problems continue despite widespread abuse. Regulatory plays a strong role, and there have been good signs of resistance to surveillance measures, e.g. body scanning, retention.

- constitution does not have a specific privacy clause, though has a search clause; Supreme Court ruled in 1952 to incorporate a legal protection of "personality" which incorporates privacy
- comprehensive law is generally considered strong, punishable by fines or imprisonment; and permitted to perform inspections in all databases include police systems
- regulator operates under the Ministry of Government Administration but is generally regarded as independent;
- regulator has played world-leading roles in awareness-raising campaigns
- communications interception authorised by court order in cases involving narcotics and national security, and some less serious offences
- new oversight body has been introduced for interception monitoring
- history of illegal wiretapping and political surveillance, so committee was established to monitor security services with an annual report to Parliament
- laws are now in place to make it easier for police to bug conversations of criminals; upon review a government commission found that the powers were being used in appropriate circumstances but was concerned about over-collection and lack of statistics
- no data retention law
- signed Prüm treaty
- issues fingerprint biometric passports since 2010; but no central database, and there is extensive debate regarding the security of the chip
- non-compulsory ID
- negative reaction to body scanner proposals lead to the cancellation of the plan
- fingerprinting in private sector is dissuaded particularly if other means of identification would be sufficient
- specific law applies to workplace surveillance, and requires negotiation with union representatives and requires regular evaluations
- medical privacy has been challenged through consolidation within the Government, leading to a high number of users who can access personal records; objections from regulator were ignored until appeal

- financial privacy degraded in 2009 by granting more agencies access to list of financial transfers in and out of Norway;
- publicly available tax returns is a long tradition, though in recent years it has become more controversial, leading to opposition parties proposing the banning of the process, particularly as there are now Facebook and iPhone applications to search the lists
- ratified CoE convention on cybercrime
- DNA: taken from all convicted with a prison sentence

Poland

Assessment: Courts and regulator are strong protectors of privacy but the Government pushes hard for vast surveillance schemes and limited oversight.

- constitutional protection for privacy, communications privacy, and data protection, and emerging jurisprudence
- comprehensive law's penalties seen as largely ineffective
- individuals are now given right to withdraw consent at any time
- sectoral laws apply to medical information, telecommunications, labour code and insurance
- regulator appointed by Parliament
- searches generally require warrants by court or public prosecutor; though most searches are carried out under claims of "urgency" without warrant
- interception of communications is conducted with limited oversight, and in large numbers (though official numbers are not published)
- a number of initiatives have been proposed to expand surveillance capabilities; police and anti-corruption authorities are gaining ever more powerful access to data
- 24 month communications data retention; originally called for 15-year retention period, and such proposals were rejected by a parliamentary commission
- access to data is restricted to police, national security agencies, and judicial authorities; though no legal threshold for gaining access
- recent scandal where 10 journalists were under surveillance by secret services to identify informants
- not ratified CoE convention
- increasing debate about CCTV, but there is no regulation of its use
- ID system is still largest collection of personal data; biometrics will be included this year

- previously no regulation of monitoring in the workplace, though courts have intervened
- medical records are protected under law, and particularly mental health records
- tax authorities have broad access to financial information

Portugal

Assessment: Insufficient information on policing and intelligence practices considering the history of abuse, but strong constitutional and legal measures are promising, and safeguards are emerging in surveillance schemes.

- constitutional protection to privacy, secrecy, and data protection
- comprehensive law applies broadly
- regulator is an independent agency that reports to Parliament; small number of complaints, though they are rising, as are fines
- regulator runs awareness raising programmes
- history of illegal political spying; too little information to assess communications surveillance
- 12 month data retention policy
- CCTV use must be registered with regulator, and now a law has been established, though use is expanding
- national ID has specific design and use policies to protect privacy; card can contain fingerprint biometric but can only be accessed with consent or as required by police and justice officials
- workplace surveillance is permitted; national monitoring of worker absenteeism during national strikes has caused some controversy; use of biometrics in the workplace is regulated by law
- safeguards have been implemented into national health reporting schemes
- has not ratified convention on Cybercrime

Romania

Assessment: Under-resourced regulator is supported by remarkable decisions from Constitutional Court. Some worrying developments in DNA surveillance, and the recent history of abuses shows that security services require greater oversight.

- constitution recognises privacy and confidentiality of communications; recent constitutional court cases have been remarkable in the defence of privacy
- comprehensive data protection law, with another law on communications privacy
- new changes in the civil code also protect privacy
- separate regime for audiovisual privacy

- regulator has suffered budget cuts and is thus unable to hire full team of staff and can not conduct investigations outside of Bucharest
- regulator has taken firm position in a number of cases
- communications surveillance regime requires authorisation of the President of the Court, and only authorises interception for 30 days, renewable only to 120 days
- intrusive surveillance permissible only if crime is punishable by 7 years in prison or more
- a number of cases have emerged with secret service spying on journalists and other public figures
- high level of wiretaps in previous years
- six month retention period for communications traffic was appealed to constitutional court which ruled it breached the Romanian Constitution
- CCTV use is growing as it is unregulated
- biometric passports involved collection of 10 fingerprints
- ratified convention on Cybercrime
- DNA: collected in enumerated cases, and only deleted by court decision or prosecutor's decision; samples are retained

Slovakia

Assessment: Some basic protections but worrying implementation of ID policy and unclear protections in some areas.

- constitutional protection for privacy, secrecy of communications and data protection
- comprehensive data protection law as well as some specific laws, though sometimes ambiguous, e.g. workplace surveillance
- regulator is independent, and is undertaking awareness raising activities with some success; has made some decisions that has been controversial with the government, particularly with respect to identity policy
- court order for communications interception for serious crimes; constitutional court case has required the Government to substantiate wiretapping warrants
- history of abuses against political and specific groups; and Roma homes are being entered without warrants
- six months data retention for internet communications data; and 12 months for other forms of communication data
- use of CCTV has been found to be in contravention with regulatory requirements
- biometric passport includes fingerprint

- mandatory ID card with additional information beyond basic profile characteristics; and is planning an e-ID card
- detailed procedures for workplace surveillance
- established an agreement with the U.S. for transfer of passenger data
- DNA: taken from anyone who receives more than a fine, and from all suspects; convicts profiles retained for ten years, suspects removed upon acquittal; samples destroyed as soon as possible

Slovenia

Assessment: Problematic surveillance practices, though the Commissioner's office plays a strong role in privacy protection.

- constitutional protection for privacy, communications, and data protection
- changes to data protection law incorporates coverage of video surveillance and biometrics
- also has laws on medical privacy, national statistics
- regulator continues to receive more and more complaint; and is highly credited with strengthening data protection in Slovenia
- interception requires judicial order; security services have more flexibility, and this is a position that was supported by the Constitutional Court
- communications traffic was originally retained for 24 months, but was recently amended and shortened to 14 months for telephone traffic and 8 months for internet traffic
- though Commissioner has drafted guidance for workplace surveillance, it has not been reviewed by Parliament as yet
- medical privacy in the Patients Rights Act; and abuses have led to fines from the Commissioner
- noted abuses in financial privacy where Tax Administration has been accessing the records of taxpayers unnecessarily
- ratified CoE Convention on Cybercrime

Spain

Assessment: Commendable regulator, but courts have not been overly helpful on privacy matters. Lack of adequate debate of technological surveillance .

- constitutional protection for privacy and data protection
- comprehensive protections are continually updated to increase protections
- regulator is world renown; strong decisions and guidance, as well as the ability to fine

- communications surveillance laws have been criticised for being vague, including key recovery, and warrantless interception
- 12 month retention of communications data, and ban on anonymity of prepaid mobile phones
- CCTV is regulated and sometimes reporting methods are required
- ID card debate has suffered from a one-sided promotion of the card rather than a critical analysis of its capabilities
- DNA is deleted upon acquittal
- ehealth record systems are emerging
- ratified Coe Convention on Cybercrime

Sweden

Assessment: Because of rise of controversy over interception law, some protections improved, but generally worrying developments across the board, and a significant need for oversight of security services.

- constitution serves as a foundation for privacy protection through enabling legislation; have been calls for a constitutional protection, and Swedish parliament voted in favour of proposition (though less far-reaching), banning "significant" intrusions
- data protection law has been amended because of concerns of it being "too restrictive", removing texts, sounds, images, and other "unstructured materials" from the DPA
- some sectoral protections have advanced privacy, e.g. privacy of credit information has been increased by a law in 2010
- regulator is a government agency but "carries out its functions independently"; has taken strong positions on a number of issues, e.g. objected to use of biometrics in schools even with consent; direct marketing and loyalty cards; though it is believed that its mandate is too limited
- in discussions re: the need for a "privacy" regulator, government instead created a commission to monitor and control use of covert surveillance by police and security services; first commissioner resigned following FRA case
- in principle a court order is required for communications interception, but the security services are given greater latitude; wiretapping has increased 500% since 1999
- FRA is permitted to use data mining software to search for keywords in all phone and email communications passing through the country's borders; was later amended because of privacy concerns, subjecting FRA to political scrutiny and permissions must be sought for every search

- despite pushing retention at the EU, Sweden has had a hard time implementing a law because of the FRA controversy
- statutory regulations on CCTV, though its liberalisation has led to a significant increase in CCTV use; and now even being used in schools
- biometric passport does not include fingerprints
- eID is a voluntary scheme that includes biometric data (facial)
- despite recommendations from a government-commissioned Committee, no rules on workplace privacy have emerged; though apparently surveillance is not prevalent
- proposal to centralise medical records ignored privacy concerns; regulator introduced rules on how information should be processed; legislative change put these on legal footing, but also enabled internet journals
- DNA: taken from convicts and suspects in offences that can be punished by 4 years or more; convicts' profiles kept for graduated periods depending on crime, and suspects' removed upon acquittal; samples retained similarly;
- has not ratified CoE convention on cybercrime

Switzerland

Assessment: Strong traditional protections but seriously being degraded in recent years, with ambitious spying, weak regulation of security services, including upcoming deliberations on communications surveillance expansion. Regulators are doing good work but are limited by resources.

- constitutional protection for privacy, communications and data protection, with some strong case law
- federal comprehensive law only requires registration of companies that use sensitive data or who transfer information abroad
- significant amendments were introduced to require adequate security, and to limited loopholes
- additional protections for health statistics, medical and legal data medical research
- regulator has sometimes limited possibilities for interventions; deals with significant volume of complaints despite limited resources; regulators in the cantons also have limited resources; but remarkable decisions are often made
- clamped down on legal interception of communications and restricted categories; now requires notification of interception; though expanded in 2007 communications surveillance by the secret services
- six month retention period; but government consulting on expanding to 12 months, and the installation of Trojan horses, worms, etc. for monitoring

encrypted communications; and identification is necessary for access to communications services, even in cafes or hotels;

- financial privacy is protected under 1934 law, but recently have been reducing these protections
- expanding use of CCTV, and even the use of drones
- changes to passport issuance means that all new passports will contain two fingerprints, and there is a fingerprint database
- have instituted "mobile" immigration controls
- new ID will include fingerprints
- plans to implement a mandatory health ID that will voluntarily include the storage of medical information
- growing DNA database for an expanded number of purposes (the enumerated list of crimes for which it could be taken has been deleted);
- DNA can be used for insurance purposes

Turkey

Assessment: Limited information on this country should be seen as a lack of progress in developing adequate structures and reporting mechanisms.

- constitutional protections for privacy and communications surveillance; proposals exist to add data protection
- data protection law has been pending since 2003, and nonetheless has some loopholes
- for now, privacy is regulated in the Civil Code, regulating the misuse of information; other sectoral applications consider privacy issues; but there is a lack of a comprehensive regulation, set of definitions
- reports state that human rights defenders are routinely placed under surveillance
- judicial warrants are required for interception of communications; and this has caused some concern for the national intelligence community
- plans for ID to include fingerprints but only on the card and not on a central database; though contains religious affiliation

United Kingdom

Overall: Over the past decade this country has become one of the worst examples for surveillance amongst democratic states, but there have been some noticeable and significant changes in the past year that may prove that it is possible to rise up from a surveillance state.

- no constitutional protection despite rich history of privacy

- Data Protection Act has been criticised for its weakness, though improvements have been made
- regulator receives many complaints, showing that public awareness is high; but decisions have indicated a timidity and often perceived as a "soft touch"
- regulator has been granted greater powers, and significant fining capacities
- extensive database and network surveillance programmes have been introduced over the past decade, though some are being dismantled
- most extensive use of visual surveillance, contemplated voice surveillance, and focused visual surveillance on specific populations
- weak regulatory regime over access to data, and there is extensive use of these powers
- interception of communications law only requires ministerial approval, with an under-resourced oversight mechanism through a "commissioner"
- proponents of health IT systems have avoided implementing adequate safeguards
- largest DNA database in the world, though lost a case at the ECtHR that may now lead to policy change (though the decision was in 2008 and the policy remains); taken from convicts of recordable offences, or anyone arrested for any recordable offence; indefinite retention of profiles; sample retained

EU

Assessment: Despite world-leading legal frameworks and great potential for innovation, the security agenda is over-riding some of the basic principles of the Union.

- Treaty obligations now include protection of human rights, and privacy as well as data protection rights; ECJ judgments in the area of privacy are weak and tend to ignore substantive issues
- extension of Directive into other areas of processing, i.e. traditional "third pillar" of justice and home affairs is a promising development
- EU's leadership role is impressive, but it is also setting a bad example
- concerted efforts to elevate the security agenda, i.e. Stockholm Programme
- data retention Directive was world-leading surveillance legislation
- passport standards created a mandate for fingerprinting nearly the entire population
- border information management and surveillance practices are increasing, as well as funding to research in this domain
- exemplary work from regulator and regulatory authorities

CRITERIA AND METRICS

We analysed each of the countries in accordance with the following criteria:

DEMOCRATIC SAFEGUARDS

The framework of participation, accountability, and rule of law enables a nation to nurture and protect rights. An open and democratic society is possibly the greatest protector of privacy. When a state is accountable to its citizens, it must justify its surveillance decisions, and it must change its practices when citizens appeal through a democracy's institutions including through open participation, media and public discourse, access to legislators and the courts, amongst other means. We used *The Economist's* recent ratings of the state of democracy around the world. We used *The Economist's* Democracy Index 2010 to gauge the strength of a democratic-nature of the state.

CONSTITUTIONAL PROTECTION

A constitution is the bedrock that stabilises the democratic framework but also provides the assurance of continued application of rights. The ability to appeal to the state's key foundation principles and show that a surveillance practice is incompatible with the interests of the government to interfere with the private lives of individuals. Many states have gone beyond merely stating the right to a private life, but also include specific clauses on the protection of communications. In a growing number of countries there is also a constitutional right to the protection of personal data. A key test of the strength of these principles is when a court rules on cases where the government has gone too far, and the emerging case law helps inform future action. A given country may not even have a distinct privacy right, but the courts could have interpreted the privacy right from "basic rights" or the "protection of dignity" principles in many constitutions

- Does a constitution exist and does it protect privacy, even "within the shadows" of other rights?
- Are there other protections, e.g. rights to data protection and private communications?
- Have the courts defended the right of privacy?
- Have there been recent cases?

STATUTORY PROTECTION

Laws are the expression of a government's commitment to its citizens rights and freedoms, and give life to the constitutional principles. These tend to come in the form of a Data Protection law, which in Europe is often is consistent with the EU Directive on Data Protection (95/46/EC), protecting privacy of information in both the public and private sectors. Often countries have additional laws that apply to specific types of information or sectors, e.g. medical information, employment law, etc. The most important characteristic of a law is that it enables individuals to seek redress.

- Are there laws protecting the right to privacy against governments and companies?
- Are there sectoral laws, e.g. medical privacy, workplace privacy, financial privacy?
- Are these laws useful in pursuing action?

PRIVACY ENFORCEMENT

For any protective law to be effective its enforcement must be unequivocal but fair. This is most often done in the form of a regulator who is given jurisdiction over a law, e.g. a data protection law, consumer law, etc., and can then assist individuals, conduct investigations, and penalise non-compliance. Not all regulators are equal, as some place energies into generating awareness of their function and thus reminding citizens of their rights. Others place an emphasis on working with government and industry to make them aware of their duties under the law. These regulators must have sufficient powers to investigate and penalise, must be independent of the government, must promote awareness of rights and responsibilities.

- Is there an independent and competent regulator?
- Is there a regulatory body with sufficient powers to investigate? Can this regulator act proactively?
- Does this regulator act in an effective way? Are the number of complaints significant? Have cases been taken through the administrative and legal systems?

LEADERSHIP

Some countries show positive leadership by promoting strong privacy protections around the world. Other governments act regressively by promoting bad policy and surveillance schemes.

- Has the government or regulator taken significant steps in privacy protection initiatives that has led other countries to consider doing so as well?
- Has the government signed and ratified problematic international treaties?

IDENTITY CARDS AND BIOMETRICS

State-imposed requirement for identity can form the basis of limitless invasions of human rights. The fusion of the individual with the machinery of the state through biometrics can irrevocably compound these violations. These systems are rarely designed carefully to protect civil liberties and instead have been historically linked with great infringements of human rights. Not all identity card systems are built equally: some are merely printed documents, others incorporate measures like smart chips or contactless technologies to enable the sharing and linking of information. More recently, some are taking on the use of biometrics, recording facial patterns, or fingerprints. The most dangerous of these systems combine all these techniques and then store the data in a centralised register, which in turn enables even greater data-sharing.

- Is there a national identity scheme, and does it include biometrics?
- Are they implemented in privacy protecting ways or in surveillance-enhancing ways?
- Is there adequate debate about the nature of biometrics or is there a blind faith in the technology and international obligations?

DATA-SHARING

Privacy is best protected when information can be confined to individually accountable purposes. Keeping information in separate silos ensures that the government never has dominion over the lives of individuals. Traditionally information held by governments has been held in separate registers: e.g. a tax file is kept separate from a medical file. Increasingly governments are keen to find new ways of bringing together information from across government departments. They may do so for different functions, e.g. combining healthcare provision with immigration status checking. Privacy is best protected when there are strong barriers between these sources of information, as they were collected for one purpose and must not be used for another.

- Are there laws protecting against use of information for secondary purposes?
- Has the government set forth on plans to diminish existing protections?

VISUAL SURVEILLANCE

Electronic visual surveillance is becoming ubiquitous in our living environment. Fusion with communications and software systems presents substantial opportunities for tracking, profiling, and discrimination. The growth and spread of visual surveillance in recent years has been remarkable. Previously, visual surveillance was deployed sparingly; now visual surveillance is being used in more locations, with fewer restrictions. Yet much of the criminological research shows that existing systems have little effect on crime, and are also open for abuse.

- To what extent are there visual surveillance systems in the public and private sectors?
- Are these regulated and are their limitations in place?
- What is the nature of the policy debate?

COMMUNICATION INTERCEPTION

Interception is generally considered amongst the most intrusive forms of surveillance. Countries that understand this will implement it under extremely strict conditions of law and will apply stringent controls. Interception must be done sparingly once other methods of investigation have been tried, and failed; and authorised by an independent judge, with regular oversight of the activities of the state agencies. Increasingly, governments are resorting to unwarranted surveillance.

- Are there adequate laws protecting against abuse?
- When can police intercept? e.g. only when investigating specific types of crimes, "serious crimes", etc.

- Do state security agencies have to follow similar rules?
- Who authorises? a judge? a politician? ["Judicial warrants" does not mean the same in all countries, where sometimes judges have investigatory powers, but we do our best to note this]

COMMUNICATIONS DATA RETENTION

One of Europe's most pernicious policies, the retention of communications traffic data on a population scale, means that telecommunications and Internet service providers are required to retain logs on with whom you communicate and what you do online for up to two years, in the event you become of interest to the state.

- Is there a retention law? If so, for how long must communications data be kept?
- Has there been any consideration of the different types of information and how retention periods may have to differ?
- Has there been any detailed deliberation on the policy? e.g. consultations, industry engagement, court cases

GOVERNMENT ACCESS TO DATA

Governments empower themselves to gain access to data held by companies and individuals. Too often they do so without requiring police and security agencies to gain authorisation from a judge, and never tell the individual that his or her personal data was accessed by the state.

- What powers do various agencies have to gain access to files?
- Are there safeguards on how law enforcement agencies get access to data on databases in the private sector?

WORKPLACE MONITORING

The evolution of management and insurance practices have motivated employers to institute saturation surveillance in their workplaces. Employment contracts allow employers to establish comprehensive and continuous surveillance over employees. Employers often try to gain access to background information on employees and potential employees, often peering into the most intimate details. Increasingly, employers are also monitoring activities at work, using audio and video surveillance, intercepting communications, and monitoring online interactions. Some are looking to collect biometric details. States often have legal protections against workplace surveillance, and some have gone so far as to ban specific forms of technologies and data collection, as they recognise that employees face a power imbalance against an employer and traditional forms of "consent" may not apply to this relationship.

- Are there laws protecting against abuse?
- Are there legal cases and methods for employees to object to these practices?
- Are there guidelines issued by the regulator or some other institution to inform employers and employees?

MEDICAL

People are more concerned about the privacy of their health information more than any other aspect of their lives. Yet governments are increasingly exploiting their citizens' health data. What was once confidential health information is now a resource to be collected, analysed, and shared. Some states have laws that protect information collected in the provision of healthcare. Other states have laws that compel the sharing of this information. Increasingly, states are seeking to develop electronic systems that will collect, process, and centrally store all this most sensitive information.

- Do patients have control over their medical information?
- Are there safeguards and protections against the secondary and other uses?
- Are there plans to develop a centralised patient register?
- Are there safeguards on how the information will be collected and used?

FINANCIAL

In recent years, the financial profile of people has become an open resource for governments and companies. Audit trails of financial behaviour are routinely shared across governments and the corporate sector with little or no distinction between the two. Monitoring bank accounts, international transfers, and the state of one's finances is of interest to both the state and industry. Both want to know about habits and purchases, while the state also wants to require the disclosure of this information to identify money laundering, but also to identify possible sources fraud, or even tax revenue. Sometimes, states require the systematic disclosure of financial information, such as through the publication of tax returns, or the collection of all suspicious transactions.

- Are there protections around government access to financial information?
- Are there safeguards around other uses of financial information by the private sector?

BORDER

Borders are now becoming constitution-free zones where governments can do as they please. States are introducing measures to collect vast amounts of information on all travellers, both citizens and visitors, with "securing" the border as the justification. Now states are introducing measures, inspired by the Bush Administration, to collect fingerprints of all travellers, as well as intelligence information from their airline reservation records in order to profile passengers.

- Has the government implemented profiling at borders or begun collecting passenger travel data?
- Is the government collecting biometrics at borders?
- Has the government initiated agreements with other governments to share information?

INTELLIGENCE AND SURVEILLANCE OVERSIGHT

Many governments are allowing their security services to circumvent constitutional and statutory protections and safeguards. The trump card of "national security" is now being used as commonly as "terrorism" to justify further encroachments on due process and the rule of law. History has shown that secret surveillance by security services has caused great harm and led to abuses. Many governments are returning to these practices and allowing their security services to circumvent constitutional and statutory protections and safeguards, avoiding warrant requirements, preventing oversight, and exempting these agencies from the law.

- Are national security agencies exempted from privacy laws?
- Are there appropriate reporting and oversight mechanisms for secret surveillance?
- Have there been cases of abuse and if so, has there been sufficient safeguards put in place?

DNA

Many countries now compel the collection of DNA samples and the generation of DNA profiles from innocent people who have not even been charged or for minor investigations, and then retain their profiles and samples for extended periods of time, sometimes indefinitely. Even though the European Court of Human Rights has ruled against this practice, many countries intentionally ignore the need for safeguards and protections. We consulted with the Council for Responsible Genetics to develop this index.

- Are there limitations under which circumstances collection of DNA may occur? e.g. limited to convicted persons and serious offences?
- When is data removed? Is there any data sharing?
- What happens to the DNA samples once the profiles have been generated?

RESULTS

Privacy International
European Privacy Ratings - Country Reviews

Country	Democratic safeguards	Coordinated protection	Privacy protection	Privacy enforcement	Law enforcement	Health, Social and Security	Data sharing	Legal safeguards	Global information	Online data retention	Government Access to Data	Workplace monitoring	Research	Provision	Records	Overweight of balancing and national security legislation	Notes	Score
ALBANIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
ARMENIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
AUSTRIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
BELARUS	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
BELGIUM	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
BULGARIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
CYPRUS	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
CZECH REP.	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
DEUTSCHLAND	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
DENMARK	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
ESTONIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
FINLAND	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
FRANCE	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
GERMANY	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
GREECE	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
HUNGARY	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
IRELAND	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
ITALY	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
LITHUANIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
LUXEMBOURG	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
NETHERLANDS	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
POLAND	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
PORTUGAL	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
ROMANIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
RUSSIA	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
SEYCHELLES	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
SPAIN	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
SWEDEN	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
SWITZERLAND	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
UNITED KINGDOM	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
UNITED STATES	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00

This data is also available in CSV format.

METHODOLOGY

ABOUT OUR ANALYTICAL APPROACH

The methodology for our analysis and ratings of countries is based on a qualitative review of research data resulting mostly from the country reports from EPHR 2010. EPHR 2010 consisted of over 600 pages of reporting from experts from across Europe. These experts are legal, technological, and academic experts who were asked to help update the existing text from previous years' reports, and to add information under a specific number of categories. These categories then informed the criteria for the ratings.

The research was complemented by Privacy International's own research monitoring privacy developments around the world. We also have a network of advisory board members and colleagues in countries across Europe, as well as relationships with a number of regulatory officials who could guide us when we encountered information-gathering challenges.

We were also able to identify other research studies that have looked at cross-country issues relating to privacy and human rights. Most notably, we used:

- *The Economist* Intelligence Unit's "Democracy Index 2010", published in December 2010, as this was a strong gauge on the democratic accountability of each of the states included in our own study. As a result we used *The Economist's* study as the primary source for our category "Democratic safeguards". There were

two challenges arising from relying on *The Economist's* study: (1) *The Economist's* study was based on a score out of 10, whereas our own studies were previously based on scores out of 5. (2) *The Economist's* study included as part of its own criteria the category of "civil liberties", so there was some risk of double counting on this issue.

- The Council for Responsible Genetics released a report in December 2010 summarising their initial research on policy DNA databases around the world. We have a close working relationship with CRG and trust the integrity of their research process. Additionally, we cross-checked their findings with our own EPHR country reports and found a strong level of synergy in the results when we had data on DNA databases in our study's countries. We did notice one case where our results were more up-to-date on recent developments, and similarly, found a couple of cases where our country reports were not as recently informed as CRG's own study.
- We also relied upon a number of research studies commissioned by the European Commission on the divergence of laws on privacy and the work of the regulators to raise awareness of privacy. These helped inform our thinking on the criteria.

CHANGES TO OUR APPROACH

This is the third time we are conducting a cross-country comparison/analysis of privacy protections. Each time we develop more sophisticated methods for analysing and assessing privacy and surveillance. We consult with experts and advisors from around the world on a regular basis in order to develop and improve upon our methodology.

The first shift in our approach, and perhaps the most significant, is that this study only looks at European countries. This was not intentional -- the nature of the funding we received was such that we only had the resources to look at European countries. One side-effect of this shift is that these countries all have a very similar regime of laws and so we needed to find a more nuanced method of identifying the differences between countries.

Another significant change in this study is that we have moved away from a five-point scheme to a more complicated schema. Though it was helpful that this matched *The Economist's* study, this was not the primary purpose of the shift. Rather, we had also conducted a literature review of cross-country comparisons conducted on human rights issues and identified a number of criticisms.

In previous years the reasoning behind our assessments were somewhat opaque. This is a common criticism of such studies in that it is hard to explain why a group of experts would assess one country as having x type of protections but another country as having y . This was a criticism of many of the other studies in this space.

As a result, rather than only relying upon multiple experts' assessments of the merits of a given country's system, as informed by the Country Reports from EPHR, we decided to be more granular in our assessments. Introducing granularity would also let us capture

more nuance within a given category, and even cater for contradictions within policy domains.

For instance, under "constitutional protections", a given country may not actually have an explicit statement of privacy within the constitution and so previously we may have marked this country down. A country may not have the right terms in a constitution but regardless cases may yet be raised to the Constitutional Court and measured on a right to privacy. So the Courts may have established a right to privacy within other basic rights. And then even in countries with constitutional statements on privacy, the Courts may come out against privacy protections. So we needed to move to a measurement system that could cater for these dynamics: given that the constitution didn't mention privacy it may have made it more challenging for the judiciary to speak of privacy, and yet they may speak favourably nonetheless, and perhaps more so than in other countries with explicit protections.

To cater for these dynamics, which are practically inherent in all the categories, we developed a series of questions applying to each category and a scoring system. We would judge the country against the various subquestions in the category and the country would be marked:

- 0 - no safeguards or protections
- 1 - some safeguards
- 2 - advanced protections

This system has two risks of bias. First, it has a positive bias in that a country may not be "punished" for a particularly poor score but would rather receive just nominal points so long as we could not "delete" points from the results of the other questions that we scored. We felt that having a bias in favour of governments was worth pursuing. In fact, we compounded this bias to allow for a special mark of 2* or 3 points for countries with particularly strong protections in one subdomain that we felt should be noted even though it did not necessarily affect the other questions within the category.

The second possible bias is that a country for which we had more limited information would be judged more harshly than one for which we had more information. To mitigate the risks of misjudging countries, we were more willing to apply no judgment to a country within a category if too little information was available. We also would average out the answers within a category based on the quality of the information.

Therefore, all categories were measured out of 10 points. Again, multiple experts reviewed this process, and many of the decisions are explained within the "analysis" section of this report.

RANKINGS V. RATINGS

We have also abandoned the idea of "rankings", where one country is awarded the "worst" mark. We believe that there is some merit to this practice, but we felt that we would find the results more interesting if we could see classifications rather than the

number figures. That is, if country A had an average of 4.2 and country B had an average of 4.5, we are unsure if it would be fair to say that country A was "worst" out of this list. Similarly, we would be cautious about saying that country B was "best". Rather, it is more valuable to see the gradations in each category and the similarities and disparities between countries when they are categorised by both criteria and average results. As such, we felt that a "ratings" scheme would be more appropriate.

NORMATIVE APPROACH

The obvious challenge of devising questions and criteria for the measurements in each category is that it requires us to be more explicit as to what we think are "good" answers to the questions. This meant that we had to decide what it is that is considered a set of acceptable practices for a democratic state. We are therefore pushed to make both subjective and normative judgements.

We make use of objective indicators to the largest extent possible (e.g. existence of laws, number of cases, powers and extent of data collection and access). Inevitably, we then have to apply a level of subjectivity based on our experts' and analysts' perceptions of whether this is good practice or merely an acceptable practice (this makes up the "2" within the scheme). This critique applies to any such study, however: even the chosen "objects" are in fact merely subjectively chosen indicators, and chosen for the purpose of appearing objective when in fact they may not always be indicative of the state of affairs.

The great challenge for a privacy advocacy organisation in conducting this rating, and perhaps for any advocacy group in any field attempting something similar is that if the criteria are fair, and if there is a positive bias, then we have to be willing to be explicit about what we find "acceptable", or perhaps even "desirable". It is easy to condemn a practice, and thus grant a "0"; but how do we measure something within a surveillance scheme as a "1", "2", or even "2*"? We could never give out a positive mark towards any surveillance scheme because, by definition it is conducting surveillance. Of course we could also diminish our expectations and just celebrate whenever something within a surveillance scheme is "less worse" than in another country's scheme.

Rather, the solution lies in being honest in our goals: we do not aim to see a world in which surveillance is entirely absent. Instead, we would like to see a world where surveillance is minimised, conducted under law, only when it is necessary in a democratic society, and proportionate, with appropriate inbuilt safeguards, and rights of recourse. So a country can have a communications data retention scheme and still get positive marks; just as many positive marks as a country without a communications data retention scheme; and possibly even more as in some countries there may not be a law but the practice is widespread nonetheless.

Importantly, privacy advocates see not only the state of laws as the ultimate goal, but rather we believe that the protection of privacy is strongest in countries where the debate about privacy is alive and well. That is, a country's framework is perhaps stronger when the protections in words and laws is strong, but also where the debate is strong. Sure, we

can count the laws, but if people are unaware of their rights and organisations unaware of their duties, then nothing has been accomplished. The challenge then becomes one of measuring the policy discourse around privacy, and we sometimes do so objectively by looking at the numbers of complaints to regulators; and sometimes by looking a little more subjectively at the types of media coverage in a country, the strength of its civil society, and the willingness of a citizenry to question a practice both publicly and, when necessary, legally, and the extent to which a nation supports these types of action through allocation of resources.

As advocates and academics, we believe that the key challenge to all methodologies is for the researcher to know what he or she is hoping to achieve.

SOME REFERENCES

- "Democracy index 2010: Democracy in retreat", *Economist* Intelligence Unit, December 2010.
- UNDP and Global Integrity, "A User's Guide to Measuring Corruption", UNDP and Global Integrity, 2008.
- "Evaluating the Evaluators: Media Freedom Indexes and What They Measure", Centre for International Media Assistance of the National Endowment for Democracy and the Center for Global Communications Studies at the Annenberg School for Communication, 2010.

ACKNOWLEDGEMENTS

Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), are pleased to present the study "European Privacy and Human Rights (EPHR) 2010," funded by the European Commission's Special Programme "Fundamental Rights and Citizenship," 2007-2013.

EPHR investigates the European landscape of national privacy/data protection laws and regulations as well as any other laws or recent factual developments with and impact on privacy. Research field specifically encompasses jurisdictions of all 27 EU Member States, two EFTA countries (Norway and Switzerland) and three EU candidate countries (Croatia, Macedonia, and Turkey). EU as a jurisdiction is taken in to consideration as well. The study consists of 33 targeted reports, an overview presenting a comparative legal and policy analysis of main privacy topics, and a privacy rating for all the countries surveyed. Depending on the selected report, the information provided is updated as of May-October 2010.

To gather information for EPHR, knowledgeable individuals from academia, public institutions, law firms, human rights groups, and other fields were asked to submit reports and relevant information. Their information was supplemented with additional research carried out by the EPHR research team. The analysis of the country reports and the ratings for each country are a result of the work of the EPHR team. EPHR builds on the legacy of EPIC's and Privacy International's publication "Privacy & Human Rights: An International Survey of Privacy Laws and Developments," which is the most authoritative reference among global and comparative surveys on privacy regulations and developments worldwide. Thus, we would like to thank the following country report contributors:

National Experts Who Took Part in EPHR 2010 by Updating Country Reports and Providing Additional Information

Republic of Austria

Stefan Mayr, Johannes Kepler University of Linz, Austria.

Kingdom of Belgium

Fanny Coudert, Brendan Van Alsenoy, Danny De Cock, Els Kindt and Jos Dumortier, Interdisciplinary Centre for Law and ICT (ICRI) – K.U. Leuven, Belgium; Alexandre Dulaunoy, Association Electronique Libre, Belgium; Nichole Rustin-Paschal, Electronic Privacy Information Center, USA, and Cédric Laurant, Center for Media and Communication Studies, Central European University, Hungary.

Republic of Bulgaria

Alexander Kashumov, Fani Davidova and Gergana Jouleva, Access to Information Programme, Bulgaria; Plamen M. Borissov, Borissov & Partners, Bulgaria.

Republic of Croatia

Ivan Gjurgjan, Gjurgjan & Šribar Radic, Croatia; Jan Klasinc, Institute for Public Administration - iDEMO (Institute for Democracy), Croatia.

Republic of Cyprus

Nicholas Ktenas and Chrystalla Neophytou, Neocleous & Co LLC, Cyprus.

Czech Republic

Richard Otevřel, Havel & Holásek, Czech Republic.

Kingdom of Denmark

Christoffer Badse, Danish Institute for Human Rights, Denmark; Michael Hopp, Plesner Law Firm, Denmark.

Republic of Estonia

Kaupo Lepasepp and Mihkel Miidla, Sorainen AS, Estonia; Viive Näslund, Lepik & Luhaäär Lawin, Estonia.

European Union

Gloria González Fuster, Law, Science, Technology & Society (LSTS) at Vrije Universiteit Brussel, Belgium; Maria Grazia Porcedda, European University Institute, Italy; Matteo E. Bonfanti, Center for Media and Communication Studies, Central European University, Hungary.

Republic of Finland

Ilona Teräkivi, LMR Attorneys Ltd, Finland; Eija Warma, Castrén & Snellman Ltd, Estonia.

France Republic

Pascale Gelly and Caroline Doulcet, Cabinet Gelly, France.

Germany

Werner Hülsmann, Deutsche Vereinigung für Datenschutz & FIF, Germany, Kristina Irion, CEU CMCS.

Greece

Vagelis Papakonstantinou, PKpartners, Greece; Elena Spiropoulou, Spiropoulou Law Firm, Greece.

Republic of Hungary

Ivan Szekely, Open Society Archives at Central European University, Hungary; Máté SzaBó, Office of the Commissioner for Educational Rights at Ministry of Education, Hungary; Endre Győző Szabó, Department of Judicial Cooperation and Private International Law of the Ministry of Public Administration and Justice, Hungary.

Republic of Ireland

Rossa McMahon, Patrick G. McMahon Solicitors, Ireland; Thomas McIntyre, University College Dublin, Ireland.

Italian Republic

Marco Calamari, Progetto Winston Smith, Italy; Michele Iaselli, Associazione Nazionale per la Difesa della Privacy, Italy; Ugo Pagallo, Università degli Studi di Torino, Italy; Guido Scorza, Istituto per le Politiche dell'Innovazione, Italy.

Republic of Latvia

Raivo Raudzeps, Sorainen, Latvia; Arturs Kuks, Department of International and European Law, University of Latvia, Latvia.

Republic of Lithuania

Henrikas Mickevičius, Human Rights Monitoring Institute, Lithuania; Mindaugas Kiskis, Mykolas Romeris University, Lithuania; Paulius Galubickas, Sorainen, Lithuania.

Luxembourg

Olivier Reisch, Linklaters, Belgium; Jan Dhont and Thomas Daenens, Lorenz, Belgium.

Macedonia

Bardhyl Jashari, Filip Stojanovski, Vesna Paunkovska, Nade Naumovska, Elena Stojanovska and Zoran Gligorov, Metamorphosis Foundation, Macedonia.

Malta

Ian Gauci, Gatt Tufigno Gauci Advocates, Malta; Andrew J. Zammit, Zammit & Associates, Malta; Jackie Scerri, Zammit & Associates, Malta.

The Netherlands

eLaw@Leiden, Center for Law in the Information Society, Leiden University, The Netherlands; Wolter Pieters, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, The Netherlands; David Riphagen, The Netherlands.

Kingdom of Norway

Christine Hafskjold, The Norwegian Board of Technology, Norway; Lee A. Bygrave, Tobias Mahler and Thomas Olsen, Norwegian Research Center for Computers and Law, University of Oslo, Norway.

Poland

Andrzej Adamski and Arkadiusz Lach, Nicolas Copernicus University, Poland; Arwid Mednis

Wierzbowski & Wspolnicy, Poland; Katarzyna Szymielewicz, Panoptykon Foundation, Poland.

Republic of Portugal

João Luís Traça, Miranda Correia Amendoeira & Associados, Portugal.

Romania

Ioana Avadani, Centrul pentru Jurnalism Independent, Romania; Bogdan Manolea, Association for Technology and Internet - APTI, Romania.

Slovak Republic

Marian Lauko and Michal Marhefka, Weinhold Legal, Slovak Republic.

Republic of Slovenia

Matej Kovačič, University of Ljubljana, Slovenia; Andrej Tomsic, Office of the Information Commissioner, Slovenia.

Kingdom of Spain

Antoni Farriols Sola, Comisión de Libertades e Informática, Spain; Ferran Adell, Universitat Autònoma de Barcelona, Spain; Javier Sempere, Agencia de Protección de Datos de la Comunidad de Madrid, Spain.

Kingdom of Sweden

Ola Svenonius, Södertörn University, Sweden.

Switzerland

Christian Thommen, Grundrechte.ch, Switzerland; Christoph Mueller, University of Zurich, Switzerland; Heinrich Busch, Switzerland.

Republic of Turkey

Emre Berk, Bener Law Office, Turkey.

United Kingdom

Anna Mazzola, Hickman & Rose, United Kingdom; Daniel Cooper, Mark Young, Shamma Iqbal and Philip Christofides, Covington & Burling, United Kingdom; Ross Anderson, Computer Laboratory, Cambridge University, United Kingdom.

National Experts Who Took Part in Former Editions of "Privacy & Human Rights:an International Survey of Privacy Laws and Developments"

(Countries Relevant For EPHR Study)

Republic of Austria

Axel Horns, FITUG e.V. (Förderverein Informationstechnik und Gesellschaft); Albert Koellner, Andreas Krisch, Peter Kuhm, VIBE!AT (Verein für Internet-Benutzer Österreichs); Dieter Kronegger, Arge Daten; Georg Lechner, Österreichische Datenschutzkommission; Erich Moechel, Quintessenz; Astrid Paisner, Freshfields Bruckhaus Deringer; Bettina Stomper, Quintessenz.

Kingdom of Belgium

Jacques Berleur, Facultés Universitaires Notre-Dame de la Paix; Alexandre Dulaunoy, Association Electronique Libre; Jos Dumortier, Interdisciplinary Centre for Law & ICT

(ICRI), Katholieke Universiteit Leuven; Bénédicte Havelange, Anne-Christine Lacoste, An Machtens and Hugues Parasie, Commission de la protection de la vie privée/ Commissie voor de Bescherming van de persoonlijke levenssfeer; Pierre-Emmanuel Laurant, Elsewhere Entertainment; Yves Pouillet and Karen Rosier, Centre de Recherches Informatique et Droit.

Republic of Bulgaria

Fany Davidova, Marina Karakonova and Alexander Kashumov, Access to Information Programme; Veni Markovski and Dragoslava Pefeva, Internet Society Bulgaria; Nelly Ognyanova, Bulgarian Institute for Legal Development.

Republic of Cyprus

Michalis Kitromilides, Office of the Personal Data Protection Commissioner.

Czech Republic

Pavel Cerny, Environmental Law Service (EPS); Karel Neuwirt, Ivan Procházka and Hana Stepankova, Office for Personal Data Protection; Helena Svatosova, Iuridicum Remedium; Ondrej Veis, Charles University.

Kingdom of Denmark

Christoffer Badse, Danish Institute for Human Rights; Mads Bryde Andersen, University of Copenhagen; Kira Kolby Christensen and Charlotte Edholm Petersen, Datatilsynet; Bo Elkjaer; Tina Fugl, Danish Data Protection Agency; Rikke Frank Joergensen and Per Helge Sørensen, Digital Rights Denmark.

Republic of Estonia

Triinu Jaaksoo and Maarja Kirss, Data Protection Inspectorate; Kaidi Oone, Estonian State Chancellery, Department of State Information Systems; Toivo Übi, Andmekaitse Inspektsioon.

European Union

Kristina Irion, Center for Media and Communication Studies, Central European University.

Republic of Finland

Reijo Aarnio and Maija Kleemola, Office of Data Protection Ombudsman; Joel Jaakkola; Jorma Kuopus, Office of the Parliamentary Ombudsman; Ville Oksanen and Mikko Valimäki, Electronic Frontier Finland.

France Republic

Anne Carblanc, Organization for Economic Cooperation and Development; Maria Farrell, International Chamber of Commerce; Marie Georges, Commission Nationale Informatique et Libertés (CNIL); Jean-Marc Manach, Journalist; Meryem Marzouki, Imaginons un Réseau Internet Solidaire; Jérôme Thorel, Advisory Board, Privacy International.

Germany

Ralf Bendrath, Universität Bremen; Herbert Burkert, GMD; Ulrich Dammann, Bundesbeauftragte für den Datenschutz; Alexander Dix, Commissioner for Data Protection and Access to Information (Brandenburg); Helmut Heil, Bundesbeauftragte für den Datenschutz; Gerrit Hornung, Projektgruppe verfassungsverträgliche Technikgestaltung, University of Kassel; Kristina Irion, Electronic Privacy Information Center; Detlef Nogala, Max-Planck-Institut; Fereniki Panagopoulou, Humboldt University; Jan Schallaböck, Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD), Independent Centre for Privacy Protection Schleswig-Holstein (ICPP); Christian Schröder, Freshfields Bruckhaus Deringer; Christoph Sobotta, University of Frankfurt.

Greece

Panageas Christos, City College; Amalia Logiaki, Greek Data Protection Authority; Nikolaos K. Papadopoulos, Technological Educational Institute of Serres; Vagelis Papakonstantinou, PK Partners.

Republic of Hungary

Zsolt György Balogh, University of Pécs; Bela Csiszer, Budapest University of Technology and Economics; Ádám Földes, Hungarian Civil Liberties Union; Gabor Freidler and Nóra Horváth, Office of the Parliamentary Commissioner for Data Protection and Freedom of Information; Zoltan Galantai, Budapest University of Technology and Economics; László Majtényi, Hungarian Information and Privacy Commissioner; Attila Péterfalvi, Commissioner for Data Protection and Freedom of Information; Máté Dániel Szabó, Eötvös Károly Policy Institute; Iván Székely, OSA Archivum and Budapest University of Technology and Economics.

Republic of Ireland

Ronnie Downes, Irish Data Protection Agency; Aileen Harrington and Joe Meade, Office of the Data Protection Commissioner; TJ McIntyre, University College Dublin, Digital Rights Ireland; Mícheál O Dowd; Antoin O'Lachtnain, Digital Rights Ireland; Elizabeth Jane Walsh, University College Cork.

Italian Republic

Marco Calamari, Progetto Winston Smith; Andrea Glorioso; Alessandro Monteleone; Andrea Monti, Studio Legale Monti.

Republic of Latvia

Linda Austere, Center for Public Policy "PROVIDUS"; Aiga Balode, Data State Inspection; Anita Kovalevska, Latvian National Human Rights Office; Signe Plumina, State Data Inspection.

Republic of Lithuania

Ona Jakstaite, Barbara Jurgeleviciene, Neringa Kaktavičiūtė and Vaida Linartaite, State Data Protection Inspectorate; Mindaugas Kiskis, Law University of Lithuania; Asta Radvilaite and Jolanta Samuolyte, Human Rights Monitoring Institute; Simonas Toliu, Law University of Lithuania; Laura Sukelyte, EU Phare Programme Twinning Project on Personal Data Protection.

Luxembourg

Bruno Nowak, Investlife.

Macedonia

Dance Danailovska, Open Society Institute; Bardhyl Jashari and Filip Stojanovski, Foundation Metamorphosis; Neda Korunovska, Foundation Open Society Institute; Marijana Marushic, Zoran Pandev, Vesna Paunkoska and Biljana Volceska, Directorate for Personal Data Protection.

Malta

Ian Deguara, Data Protection Commissioner's Office.

The Netherlands

S. Artz and Diana Alonso Blas and Anne-Marije Fontein, College Bescherming Persoonsgegevens; Jan Holvast, Holvast & Partners; Sjoera Nas, Bits of Freedom; Maurice Wessling, Bits of Freedom and European Digital Rights.

Kingdom of Norway

Lee Bygrave, Institutt for rettsinformatikk (Norwegian Research Centre for Computers and Law) and Faculty of Law, University of Oslo; Gunnel Helmers, Data Inspectorate of Norway.

Poland

Andrzej Adamski, Nicolas Copernicus University; Sybilla Graczyk, Association of Polish Consumers; Igor Kowalewski, Dorota Rowicka, Justyna Seweryoska and Alina Szymczak, The Bureau of the Inspector General for Personal Data Protection; Ewa Kulesza, Inspector General for Personal Data Protection; Arwid Mednis, partner Wierzbowski Eversheds.

Republic of Portugal

Clara Guerra, National Data Protection Commission; João Miguel Neves.

Romania

Virgil Cristian Cristea, Institution of the Romanian People's Advocate; Valeriu Guguianu, Ministry of Public Information; Bogdan Manolea, Association for Technology and Internet (APTI); Ioan Muraru, Avocatul Poporului.

Slovak Republic

Zuzana Babicová and Daniel Valentovic, Office for Personal Data Protection; Andrej D. Bartosiewicz, Association for Support of Local Democracy; Pavol Husar, Commissioner

for the Protection of Personal Data in Information Systems; Natalia Krajcovicova, Inspection Unit for the Protection of Personal Data; Vladimir Pirošik, Environmental Lobbying Facility; Peter Wilfling, Citizen and Democracy Association.

Republic of Slovenia

Joze Bogataj, Data Protection Inspectorate; Sonja Bien Karlovšek and Andrej Tomšič, Information Commissioner; Matej Kovacic and Vasja Vehovar, University of Ljubljana.

Kingdom of Spain

Rafael Fernández Calvo, Commission for Liberties and Informatics; David Casacuberta, Computer Professionals for Social Responsibility-Spain (CPSR-Spain); Pedro Dubie, AEDIP; Emilio Aced Félez, Agencia de Protección de Datos; Miguel Angel Garcia, MAG (Estudios de Consumo); Eva Sanchez Guerrero, Open University of Catalonia; Beatriz Iglesias, Computer Professionals for Social Responsibility-Perú(CPSR-Perú); Yasha Maccanico, Statewatch; Piñar-Mañas and Mercedes Ortuño, Agencia Española de Protección de Datos; Arturo Quirantes, University of Granada and Computer Professionals for Social Responsibility-Spain.

Kingdom of Sweden

Alberto Escudero-Pascual, Royal Institute of Technology; Elisabeth Wallin, The Data Inspection Board.

Switzerland

Heiner Busch; Christoph Mueller, University of Zurich; Felix Rauch, Swiss Internet User Group; Dag Wiese Schartum, Eliane Schmid, Federal Data Protection Commissioner's Office; Kosmas Tsiraktsopoulos, Swiss Data Protection Commission.

Republic of Turkey

Nilgün Basalp and Nurcan Kaya, Istanbul Bilgi University.

United Kingdom

Yaman Akdeniz, (previously from) University of Leeds; David Banisar, Article 19; Ian Brown, Oxford Internet Institute; David Clancy, Information Commissioner's Office; Maurice Frankel, Campaign for Freedom of Information; Alex Hamilton, Liberty; Eduardo Ustarán, Berwin Leighton Paisner.

This project was funded with the support of the Fundamental Rights and Citizenship Program of the European Commission.

EUROPEAN PRIVACY AND HUMAN RIGHTS TEAM

Privacy International, London.

- Simon Davies, Director
- Gus Hosein, Deputy Director
- Alexander Hanff, Communications Project Leader

- Eric King
- George Morgan
- Wendy M. Grossman

Center for Media and Communication Studies, Central European University (CEU), Budapest.

- Kristina Irion, Research Director
- Matteo E. Bonfanti, Research Fellow
- Cédric Laurant, Senior Research Fellow
- Sarah Pipes, summer intern

Electronic Privacy Information Center, Washington D.C.

- Marc Rotenberg, Executive Director and President

PRIVACY RESOURCES

PRIVACY NEWS

Privacy News and Reports

- BNA Privacy & Security Law Report <http://www.bna.com/products/corplaw/pvln.htm>.
- BNA Privacy Law Watch <http://www.bna.com/products/ip/pwdm.htm>.
- Privacy Law & Business <http://www.privacylaws.com>.
- EDRI-Gram <http://www.edri.org/edriagram>
- Privacy and Information Security Blog Law (Hunton & Williams). This blog will help you to find the primary source of the news. <http://www.huntonprivacyblog.com/>
- Baker McKenzie, Privacy Law Resources <http://www.bmck.com/ecommerce/home-privacy.htm>
- Baker McKenzie, Security Law Resources <http://www.bmck.com/ecommerce/home-security.htm>
- Privacy Exchange <http://www.privacyexchange.org/>
- Panopticon <http://www.panopticonblog.com/2011/01/05/scottish-government-issued-privacy-guidance/>

Newsletters

- BNA newsletter: <http://ecommercecenter.bna.com>;
- Baker & McKenzie newsletter: <http://www.bmck.com/elaw/register.asp>;
- EDRI newsletter (mostly covers European countries): <http://www.edri.org/>
- EDPS Newsletter <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Newsletters>

INSTITUTIONAL RESOURCES

European Privacy Commissioners

- Austria: Büro der Datenschutzkommission und des Datenschutzrates
<http://www.dsk.gv.at>
- Belgium: Commission de la Protection de la vie privée
<http://www.privacy.fgov.be/>
- Bulgaria: Commission for Personal Data Protection
<http://www.cdpd.bg>.
- Croatia
<http://www.azop.hr/default.asp>
- Cyprus http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_gr/index_gr?OpenDocument
- Czech Republic
<http://www.uoou.cz/uoou.aspx>
- Denmark
<http://www.datatilsynet.dk/>
- Estonia
<http://www.aki.ee/est/>
- Finland
<http://www.tietosuoja.fi/>
- Former Yugoslav Republic of Macedonia
e-mail: info@dzlp.gov.mk
- France
<http://www.cnil.fr/>
- Germany
http://www.bfdi.bund.de/cln_136/Vorschaltseite_DE_node.html
- Greece
http://www.dpa.gr/home_eng.htm
- Hungary
<http://abiweb.obh.hu/abi/>
- Iceland
<http://www.personuvernd.is/>
- Ireland
<http://www.dataprivacy.ie/>
- Italy
<http://www.garanteprivacy.it/garante/navig/jsp/index.jsp>
- Latvia
<http://www.dvi.gov.lv/>
- Liechtenstein
<http://www.dss.llv.li/>
- Lithuania
<http://www.ada.lt/>

- Luxembourg
<http://www.cnpd.public.lu/fr/index.html>
- Malta
<http://www.dataprotection.gov.mt/>
- Netherlands
<http://www.dutchdpa.nl/>
- Norway
<http://www.datatilsynet.no/>
- Poland
<http://www.giodo.gov.pl/168/j/pl/>
- Portugal
<http://www.cnpd.pt/index.asp>
- Romania
<http://www.dataprotection.ro/>
- Slovak Republic
http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=92
- Slovenia
<http://www.ip-rs.si/>
- Spain
<https://www.agpd.es/portalwebAGPD/index-ides-idphp.php>
- Sweden
<http://www.datainspektionen.se/>
- Switzerland
<http://www.edoeb.admin.ch/>
- United Kingdom
<http://www.ico.gov.uk/>
- Central and Eastern Europe Data Protection Authorities <http://www.ceecprivacy.org>

Intergovernmental organisations and international cooperation

EU

- European Commission, DG Justice, Data Protection http://ec.europa.eu/justice_home/fsj/privacy/
- The European Data Protection Supervisor <http://www.edps.europa.eu/EDPSWEB/>
- Article 29 Working Party on Data Protection http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.
- European Network and Information Security Agency <http://www.enisa.eu.int/>
- European Union Agency for Fundamental Rights, Charter of fundamental rights of the European Union, artt. 7 and 8, http://infoportal.fra.europa.eu/InfoPortal/infobaseShowContent.do?btnCat_202&btnCountryBread_169

Council of Europe

- Data protection <http://www.coe.int/dataprotection>

OECD

- Information and Communication Technologies (general) http://www.oecd.org/topic/0,3373,en_2649_37441_1_1_1_1_37441,00.html
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
- Guidelines for the Security of Information Systems: http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

APEC

- Electronic Commerce Steering Group http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html

United Nations

- Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly Resolution 45/95 of 14 December 1990 <http://www.unhchr.ch/html/menu3/b/71.htm>
- Human Rights Committee <http://www2.ohchr.org/english/bodies/hrc/index.htm>
- Human Rights Committee, General Comment n. 16, [http://www.unhchr.ch/tbs/doc.nsf/\(Symbol\)/23378a8724595410c12563ed004aeecd?OpenDocument](http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?OpenDocument)
- UNCTAD, Information Economy Report Series <http://www.unctad.org/templates/Page.asp?intItemID=3594&lang=1>

World Trade Organization

- http://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm
- http://www.wto.org/english/tratop_e/serv_e/_derived/sourcecontrol_gats_factfiction10_e.htm

International Chamber of Commerce

- E-Business, IT and Telecoms <http://www.iccwbo.org/policy/ebitt/>

International Working Group on Data Protection in Telecommunications

<http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>

Non-governmental organisations

- EPIC <http://epic.org/>
- Virtual Privacy Office <http://www.datenschutz.de/>
- Association for Progressive Communications' European Civil Society Internet Rights Project <http://europe.rights.apc.org/>

Human rights reports

- Human Rights Watch, Annual World Report <http://www.hrw.org/en/publications/reports>.
- Amnesty International Annual Report, <http://www.amnesty.org/>.
- US State Department, Country Reports on Human Rights, section (f) on Arbitrary Interference with Privacy, Family, Home, or Correspondence <http://www.state.gov/g/drl/rls/hrrpt/index.htm>

Country-specific additional privacy resources

Austria

Austrian Association for Internet Users (NGO)
<http://www.vibe.at>

Austrian Society for Privacy and Data Protection (NGO)
http://www2.argedaten.at/php/cms_monitor.php?q=AD-NEWS-LAST

Quintessenz
<http://www.quintessenz.org/>

Arge Daten
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15048tpb

Belgium

Droit-Technologie (online portal of legal information: news, legislation, case law, law review articles and theses)
<http://www.droit-technologie.org/>

Research Center for Computer and Law (Centre de Recherche Informatique et Droit)
<http://www.fundp.ac.be/droit/crid/>

The Interdisciplinary Centre for Law and ICT (ICRI) – K.U.Leuven
www.icri.be

Net Users' Rights Protection Association
<http://www.nurpa.be/>

Bulgaria

Access to Information Programme (NGO)

http://www.aip-bg.org/index_eng.htm

Internet Rights Bulgaria Foundation (NGO)

<http://www.irbf.ngo-bg.org/en>

Internet Society Bulgaria

http://www.isoc.bg/index_en.html

Croatia

CEEC: Data Protection in the Republic of Croatia

<http://www.ceecprivacy.org/main.php?s=2&k=croatia>

Czech Republic

Czech News Agency (CTK)

<http://www.ctk.eu/>

Prague Post

<http://www.praguepost.cz/>

Iuridicum Remedium

<http://www.iure.org/>

Big Brother Awards CR

<http://www.bigbrotherawards.cz/en/english/home-eng>

Denmark

Privacy Forum, arising from Danish Industry's Privacy Task Force

<http://www.privacyforum.dk/>

Digital Rights

<http://www.digitalrights.dk/>

IT-Political Association

<http://www.itpol.dk/>

Estonia

Estonian Informatics Centre

<http://www.ria.ee/atp/eng/index.html?id=712>

Estonian National ID Cards

<http://support.sk.ee/>

CEEC: Data Protection in the Republic of Estonia

<http://www.ceecprivacy.org/main.php?s=2&k=estonia>

Finland

Protection of Privacy in Working Life, Ministry of Labour (Jan 2010)

http://www.mol.fi/mol/en/03_labourlegislation/03_privacy/index.jsp

Electronic Frontier Finland (NGO)

<http://www.effi.org/index.en.html?tmplang=en>

FINLEX (English translations of Finnish acts)

<http://www.finlex.fi/en/>

France

Juriscom.net (online portal of legal news)

<http://www.juriscom.net>

Legalis.net (online portal of legal news)

<http://www.legalis.net/>

Droit-Tic

<http://www.droit-ntic.com/>

IRIS (NGO)

<http://www.iris.sgdg.org/>

Germany

Virtual Privacy Office (online portal)

<http://www.datenschutz.de/privo/>

Chaos Computer Club

<http://ccc.de/> (in German)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (Forum for Peace and Social Responsibility),
<http://www.fiff.de/>

FoeBuD
<http://www.foebud.org/>

Friends of Information Technology and Society
<http://www.fitug.de/>

Independent Centre for Privacy Protection (in German)
<http://www.datenschutzzentrum.de>

Greece

The Hellenic Authority for Communication Security and Privacy (ADAE) <http://www.adae.gr/portal/index.php?id=1&L=1>

Hungary

Hungarian Civil Liberties Union (NGO)
<http://tasz.hu/>

Eötvös Károly Policy Institute
http://www.ekint.org/ekint/ekint_angol.head.page?nodeid=27

Parliamentary Commissioner's Office of Hungary
<http://www.obh.hu/>

CEEC: Report on Data Protection Commissioner – Hungary
<http://www.ceecprivacy.org/main.php?s=2&k=hungary>

Ireland

Irish Internet Association (industry organization)
<http://www.iiia.ie/>

Irish Council for Civil Liberties
<http://www.iccl.ie/>

Italy

Associazione Nazionale per la Difesa della Privacy
<http://difesaprivacy.blogspot.com/>

Electronic Frontiers Italy (NGO)
<http://www.alcei.it/>

Privacy.it
<http://www.privacy.it/>

Anopticon
<http://tramaci.org/anopticon/>

Digital Thoughts (blog addressing ICT law with emphasis on Italy)
<http://blog.andreamonti.eu/>

Latvia

CEEC: Data Protection in the Republic of Latvia
<http://www.ceecprivacy.org/main.php?s=2&k=latvia>

Human Rights in Latvia
<http://www.humanrights.lv/>

Lithuania

Human Rights Monitoring Institute -Lithuania
<http://www.hrmi.lt/>

Luxembourg

Internet Society Luxembourg
<http://www.isoc.lu/>

Macedonia

Metamorphosis Foundation
www.metamorphosis.org.mk/

CEEC: The Office for Personal Data Protection
<http://www.ceecprivacy.org/main.php?s=2&k=macedonia>

Malta

Chetcuti Cauchi Advocates (law firm data protection unit)

<http://www.cc-advocates.com/data-protection/unit.htm>

Netherlands

Bits of Freedom (NGO)

http://www.bof.nl/index_uk.html

Privacy.pagina.nl (online portal)

<http://privacy.pagina.nl/>

Norway

Electronic Frontier Norway

<http://efn.no/>

The Norwegian Board of Technology

<http://www.teknologiradet.no/FullStory.aspx?m=5>

Poland

CEEC: Data Protection in Poland

<http://www.ceecprivacy.org/main.php?s=2&k=poland>

Inspector General for the Protection of Personal Data

<http://www.giodo.gov.pl/138/j/en/>

Privacy Protection in Data Communication Systems (government produced guide)

<http://techinfo.giodo.gov.pl/index-en.html>

Panopticon Foundation <http://www.panoptikon.org/>

Romania

Association for the Defence of Human Rights in Romania (NGO)

<http://www.apador.org/indexe.htm>

Romanian People's Advocate Institution Ombudsman

<http://www.avp.ro/indexen.html>

Centrul pentru Jurnalism Independent

<http://www.cji.ro/>

Slovakia

CEEC: Data Protection in the Slovak Republic

<http://www.ceecprivacy.org/main.php?s=2&k=slovakia>

Slovenia

Slovenian Human Rights Ombudsman

<http://www.varuh-rs.si/cgi/teksti-eng.cgi/Index?vsebina=/cgi/teksti-eng.cgi%3Fpozdrav>

Spain

Revista Datos Personales <http://www.datospersonales.org>

Sweden

Matthias Klang, Country Report—Sweden, APC European Internet Rights Project

http://europe.rights.apc.org/c_rpt/sweden.html

Switzerland

Directory of compiled Federal laws and regulations (decrees)

<http://www.admin.ch/ch/d/sr/sr.html> (in German, French and Italian)

Directory of decisions of the Swiss Federal Court (Bundesgericht)

<http://www.polyreg.ch/##>

Swiss "Big Brother Awards"

<http://www.bigbrotherawards.ch>

Swiss Federal Government and Administration

<http://www.admin.ch>

Turkey

Publications of Dr. Yaman Akdeniz

<http://www.cyber-rights.org/yamancv.htm>

United Kingdom

Campaign for Freedom of Information (NGO)

<http://www.cfoi.org.uk/>

Foundation for Information Policy (NGO)

<http://www.fipr.org/>

Privacy International (NGO)

<http://www.privacyinternational.org>

Privacy Laws and Business (NGO)

<http://www.privacylaws.co.uk/>

Statewatch (NGO)

<http://www.statewatch.org>

REPUBLIC OF AUSTRIA

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Austrian Federal Constitutional Law (*Bundes-Verfassungsgesetz* or B-VG¹) neither explicitly recognises the right to privacy nor contains a clear competence clause, which is why legislative power is split between the federal level and the nine states (*Bundesländer*). The federal Act concerning the protection of personal data (*Datenschutzgesetz* 2000 or DSG²) contains a number of constitutional provisions³, among them a fundamental right to data protection.⁴ Also, the European Convention on Human Rights (ECHR) forms part of the Austrian Constitution, and the Constitutional Court often relies on Art. 8 ECHR in privacy cases. An amendment to the constitutional framework, including *inter alia* a single competence clause (in favour of federal legislation) as well as a more clearly worded version of the fundamental right to data protection failed to obtain the necessary qualified majority in 2009.⁵

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The DSG came into force in January 2000⁶, transposing the EU Data Protection Directive 1995/46/EC while at the same time replacing a 1978 law of the same name.⁷ The DSG has been amended substantially as of January 2010.⁸ The basic framework, however, has by and large remained unaltered.

It regulates the use of data and – under the heading "Fundamental Right to Data Protection" – contains four different rights: a right to secrecy, a right to obtain information (who processes what data, for which purposes they are used, etc.), a right to

¹ Federal Law Gazette (BGBl. Nr.) 1/1930 as amended, available in English at <http://www.ris.bka.gv.at/Englische-Rv/>.

² BGBl. I Nr. 165/1999 as amended, available in English at <http://www.ris.bka.gv.at/Englische-Rv/>.

³ Austrian law allows for "constitutional provisions" (*Verfassungsbestimmungen*) within regular statutes. These provisions are part of the Constitution, the core of which is the B-VG.

⁴ Art 1 Section 1 DSG.

⁵ The non-constitutional parts of the amendment, however, have largely entered into force as of 1 January 2010. Whether the Government will try again to pass the proposed constitutional amendment is not yet foreseeable.

⁶ For an overview of other relevant laws and regulations see <http://oesterreich.gv.at/site/5809/default.aspx>.

⁷ BGBl. Nr. 565/1978.

⁸ BGBl. I Nr. 133/2009.

rectification of incorrect data, and a right to erasure of illegally processed data.⁹ Whereas the latter three rights cover data destined for automated or manual processing (e.g. in filing systems), the right to secrecy comprises any personal data (e.g. contained in paper files) concerning the data subject, insofar as s/he has an interest deserving such protection.¹⁰ Moreover, prevailing opinion and case law acknowledge a right to keep data confidential.¹¹ It is noteworthy that any natural or legal person or group of natural persons (e.g. companies, associations, religious or political organisations, etc.) can be data subjects, enjoying the fundamental right to data protection as outlined above.¹²

Restrictions to the right to secrecy are only permitted in the following cases.¹³ Either personal data is used in the vital interest of the data subject or with his/her consent or a restriction is necessary to safeguard overriding legitimate interests of others. Restrictions by public authorities have to be based on laws and to be necessary in a democratic society for at least one of the aims stated in Art. 8 paragraph 2 ECHR. A law restricting the right to secrecy concerning sensitive data¹⁴ additionally has to further substantial public interests and provide suitable extra safeguards. Section 48a DSG, which was introduced in 2005 following the tsunami disaster, deals with the use of data in case of a catastrophe and can serve as an adequate example. Still, even in the case of permitted restrictions any interference with the fundamental right has to be limited to the least intrusive of all effective means. These conditions also apply to restrictions of the rights laid out in Art. 1 Section 3.

Another peculiarity, influencing the choice of legal remedies, is the "direct third-party effect" (*unmittelbare Drittwirkung*) of the fundamental right to data protection. Apart from the right to information, this fundamental right can be asserted before the civil courts against organisations that are established according to private law, as long as they are not playing an enforcement role.¹⁵

Since 2004 the Austrian Civil Code contains a legal basis¹⁶ for damages caused by illegal privacy intrusions. Grave violations may also justify compensation for pain and suffering.

⁹ Art. 1 Section 1 (1) and (3) DSG.

¹⁰ *Id.*

¹¹ VfSlg 12.228, Decision of the Constitutional Court, 30 November 1989, G 245-250/89, G 268-275/89, available via <http://www.ris.bka.gv.at/Vfgh/>.

¹² Section 4 item 3 DSG.

¹³ Art. 1 Section 2 DSG.

¹⁴ Section 4 item 2 DSG.

¹⁵ Art. 1 Section 5 DSG.

¹⁶ Section 1328a Civil Code.

The provision protects natural persons, with an exception for public figures.¹⁷ Additionally, the Enforcement Act (*Exekutionsordnung*) provides for injunctions whenever an applicant's right to privacy is at stake.¹⁸

Sector-based laws

Several sector-based laws contain privacy-relevant provisions. Chapter 12 of the Telecommunications Act (*Telekommunikationsgesetz* or TKG¹⁹) includes *inter alia* a guarantee of the confidentiality of communications as well as a provision on data protection, taking into account the specificities of the technical preconditions. Generally, the legitimate use of certain data for marketing purposes or the provision of value-added services depends on the user's (i.e. a natural person, using a publicly available communications service for business or private purposes) consent.²⁰ Furthermore, the TKG contains special data protection provisions concerning subscriber directories, call tracing, unsolicited communications, and calling line identification.²¹

The Genetic Engineering Act (*Gentechnikgesetz* or GTG²²) requires confidentiality of personal data gathered through genetic analysis and gives the person examined a right to access as well as a right to information. Many other statutes deal with single aspects of the use of medical and health data. The *Gesundheitstelematikgesetz* (GTelG²³) regulates the use of telematics in the health service sector, including data security and information management.

The Banking Act (*Bankwesengesetz* or BWG²⁴) deals with special requirements and restrictions concerning the use of client data.

Part Four of the Security Police Act (*Sicherheitspolizeigesetz* or SPG²⁵) regulates the use of personal data by security authorities, generally referring to the DSG and underlining the (self-evident) principle of proportionality.²⁶ It allows the use of personal data

¹⁷ Decision of the Supreme Court, 23 September 2008, 4 Ob 150/08 z, available via <http://www.ris.bka.gv.at/Jus>

¹⁸ Section 382g EO, which entered into force as of 1 July 2006: BGBl. I Nr. 56/2006. The materials show clearly, that the lawmaker had privacy infringements by individuals (especially in the form of stalking) in mind.

¹⁹ BGBl. I Nr. 70/2003 as amended, available in English at <http://www.ris.bka.gv.at/Englische-Rv/>.

²⁰ Section 96 TKG.

²¹ Sections 92-107 TKG.

²² BGBl. Nr. 510/1994 as amended; see Section 71 GTG.

²³ BGBl. I Nr. 179/2004 as amended.

²⁴ BGBl. Nr. 532/1993 as amended.

²⁵ BGBl. Nr. 566/1991 as amended.

²⁶ Section 51 SPG.

whenever it relates to the authorities' tasks and a cause exists which justifies the processing of such data. Section 56 SPG deals with the transmission of data and states that the DSG-regime²⁷ is not applicable here. To a certain extent the means of gathering personal data overlap with the provisions set out in the Code of Criminal Procedure (*Strafprozessordnung* or StPO²⁸) requiring a court or prosecutor's order. The line between crime or danger prevention and ordinary investigations cannot always be drawn easily.

In January 2003 the Law on the Documentation of Education (*Bildungsdokumentationsgesetz*²⁹) came into force, regulating the use of pupils' and students' data for purposes of long-term documentation. Schools, universities, and other professional academies have to collect a large set of data including social security numbers, religious affiliation, need for special educational assistance, grades, and degrees, and transmit that information to the competent ministries and the Austrian Agency for Statistics, where the data will be stored and can be identified with the help of social security numbers. According to Section 8, the personal link has to be erased 20 years after the last data have been added.

As mentioned before, the legislative competence for data protection issues is split between federal level and states. That is why in 2000 the states adopted various laws relating to data protection. Some of the states have introduced rules regarding the notification of suspicions of neglect, maltreatment and sexual abuse of children.

DATA PROTECTION AUTHORITY

The Data Protection Commission (*Datenschutzkommission* or DSK) handles the vast majority of alleged violations of the rights granted by the DSG and is in charge of the Data Processing Register (*Datenverarbeitungsregister* or DVR), ensuring the publicity of data applications.³⁰

When the DSG was drafted, it was criticised for maintaining the cumbersome structure of the original 1978 Act.³¹ The 2010 amendment substantially simplifies the registration procedure for data applications, in order to decrease the Commission's workload in this regard. Unless specific exceptions apply³², notifications will only be examined

²⁷ Sections 8, 9 DSG.

²⁸ BGBl. Nr. 631/1975 as amended, e.g. Sections 134-140 StPO.

²⁹ BGBl. I Nr. 12/2002.

³⁰ Sections 16 – 25 DSG.

³¹ See Viktor Mayer-Schönberger & Ernst Brandl, *Datenschutzgesetz 2000* (Line Publishing Vienna 1999).

³² Section 18 (2) DSG. The specific exceptions are : an application is carried out in the form of a joint information system or involves sensitive data, certain criminally relevant data or data whose purpose is to give information on the data subject's creditworthiness.

automatically as to completeness and plausibility. However, the DSK has the authority to examine notifications *ex officio* at any time.³³

The amendment also introduces changes to the legal remedies, especially with regard to enhancing procedural efficiency. On the one hand, formal requirements are newly introduced, giving the DSK an opportunity to dismiss complaints on formal grounds.³⁴ On the other hand, a new provision precludes parallel control (ombudsman) and complaint proceedings.³⁵ In addition, it has been clarified that the DSK's decisions, which are by and large publicly available³⁶, have a binding declaratory character. Nevertheless it can order private sector controllers to respond appropriately to requests for information.³⁷ No regular remedy at law is permitted against the rulings of the DSK; however, the parties have the right to bring a case before the Administrative Court (*Verwaltungsgerichtshof*) or the Constitutional Court (*Verfassungsgerichtshof*).³⁸

Persons or groups of persons can file complaints with the DSK. Regardless of the status of the controller, the right to information has to be asserted before the DSK. Additionally, the Commission is competent to render decisions on complaints lodged against public sector controllers³⁹ for alleged violations of the rights to secrecy, rectification, and erasure of data.⁴⁰ The Commission has the power to exercise its functions *vis-à-vis* the highest executive authorities (enumerated in Art. 19 B-VG)⁴¹, but it has no such power with regard to acts of Parliament or judicial decisions.⁴² Additionally, the DSK acts as an ombudsman institution, routinely grants legal advice (by e-mail or telephone), and administers the cross-border transmission and committal of data. Finally it acts as the sourcePIN Register Authority.⁴³

³³ Section 22a (1) DSG.

³⁴ Sections 31 (3), (4) DSG.

³⁵ Section 31 (6) DSG.

³⁶ See <http://www.ris.bka.gv.at/dsk/>. This database contains selected decisions since 2000.

³⁷ Section 31 (7) DSG.

³⁸ Section 40 DSG. Since the 2010 amendment, public sector controllers are in principle excluded from the right to bring a case before the Administrative Court.

³⁹ According to Section 5 DSG these also include controllers who despite having been incorporated according to private law, execute laws.

⁴⁰ Section 1 (5) DSG.

⁴¹ Constitutional provision in Section 35 (2) DSG.

⁴² Section 1 (5) DSG. In this context it is noteworthy that the Austrian Court of Audit ("Rechnungshof") as well as the Ombudsman ("Volksanwaltschaft") are technically parliamentary institutions.

⁴³ *E-Government-Gesetz* or E-GovG (E-Government Act), BGBl. I Nr. 10/2004 as amended, Section 7. Cf. "E-Government & Privacy", *infra*.

The DSK consists of six members and six deputies (one of each group being a judge) on a part-time basis⁴⁴ and a total of 20 established posts. More than half of the complaints lodged with the Commission concern alleged violations of the right to information, another third the right to secrecy. The number of ombudsman cases, 90 percent of which arise from the private sector, has been increasing constantly in recent years (around 300 in 2009). These cases vary widely in terms of complexity. Among other means, the Commission can issue recommendations, setting an appropriate period for compliance. But it can also bring a criminal charge or, in case of severe transgression by a private sector controller, file a lawsuit before the competent civil court. In case of transgression by an organ of a territorial corporate body (*Gebietskörperschaft*), the DSK gets the highest competent authority involved. Within a period not exceeding 12 weeks, this authority is supposed to ensure compliance with the DSK's recommendation or inform the Commission why the recommendation is not complied with. It is remarkable that this informal remedy has an outstandingly high rate of success; however, due to staff shortage the duration of these proceedings goes up.⁴⁵

The licensing function concerning cross-border transmission and storing data leads to a relatively small amount of caseload. Exchanging data with recipients in European Economic Area countries is not subject to any restrictions, unless it concerns public sector controllers in fields that are not subject to the law of the European Union. No authorisation is needed for data exchange with recipients in third countries with an adequate level of data protection.⁴⁶

Claims against private sector controllers have to be asserted before the civil courts. As the claimant bears a considerable financial risk concerning the litigation costs, the number of cases is moderate.⁴⁷ The claimant has a right to interlocutory injunctions, can bring an action for a permanent injunction, or can sue controller or processor for damages.⁴⁸ All rights granted by the DSG are subject to a limitation period of one year after knowledge of a potential violation and an absolute limitation period of three years.⁴⁹

A second institution established by the DSG is the Data Protection Council (*Datenschutzrat*), which is a political advisory body. Members of the DSK can at the same time be members of the Council.⁵⁰

⁴⁴ Section 36 (3a) DSG.

⁴⁵ Section 30 (6) DSG. See *Datenschutzbericht 2009*, (Official Bi-Annual Data Protection Report 2009), at 3, 15 – 22, available in German at <http://www.dsk.gv.at/DocView.axd?CobId=40344>.

⁴⁶ Section 12 DSG. An ordinance of the Federal Chancellor contains list of these countries.

⁴⁷ See *Datenschutzbericht 2009*, *supra* at 18.

⁴⁸ Section 32 DSG.

⁴⁹ Section 34 (1) DSG.

⁵⁰ Sections 41 – 44 DSG.

In 2005 the European Commission initiated infringement proceedings against Austria and Germany for not creating fully independent Data Protection Authorities. The DSK is integrated into the Federal Chancellery and its executive member is a senior official of the Chancellery.⁵¹ In a 2009 *avis motivé* the European Commission restated its concerns in terms of lacking independence, which were not resolved by the 2010 amendment either. Further steps have yet to be taken.⁵²

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The relevant Austrian case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

A 2002 amendment to the statute regulating military competences (*Militärbefugnisgesetz* or MBG⁵³) allows the Austrian military intelligence service to request the name, address, and identification number of potentially every telecommunications user from Internet service providers (ISPs) or other telecommunications service providers.⁵⁴ The draft was strongly opposed by Austrian privacy organisations since the obligation is merely based on the assertion that a certain piece of information is needed for intelligence purposes.⁵⁵

The Code of Criminal Procedure (StPO⁵⁶) regulates practices such as wiretapping, electronic eavesdropping (*Lauschangriff*, audio as well as optical surveillance), or

⁵¹ "EC: Data Protection Inadequate in Austria and Germany" EDRIgram newsletter No. 3.17, 24 August 2005, available at <http://www.edri.org/edriagram/number3.17/DPA>.

⁵² Nicolas Raschauer, "Art. 8 der Grundrechtecharta (Grundrecht auf Datenschutz) und die Überwachung durch eine unabhängige Kontrollstelle" ("Art. 8 GRC and the Supervision by an Independent Supervisory Body"), 8 September 2010, available at http://www.springerrecht.at/art-8-der-grundrechtecharta-grundrecht-auf-datenschutz-und-die-uberwachung-durch-eine-unabhangige-kontrollstelle_nicolas-raschauer/.

⁵³ BGBl. I Nr. 86/2000 as amended.

⁵⁴ Section 22 (2a) MBG.

⁵⁵ ARGE DATEN, "Militärs – Lauschgeil durchs Land" (Military – Eavesdropping through the Country), 17 June 2002, available in German at http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=95162atc; VIBE, "Willkürlicher militärischer Zugriff auf Benutzerdaten" (Arbitrary Military Access to User Data), 18 June 2002, available in German at http://web.archive.org/web/20080426021608/http://www.vibe.at/aktionen/200206/mil_18jun2002.html.

⁵⁶ On 1 January 2008 a comprehensive amendment to the StPO entered into force.

dragnet investigations (*Rasterfahndung*, cross-referencing of government and – in certain circumstances – private databases).⁵⁷

Wiretapping can comprise master data, access data, location data, or the content of a telecommunications or other information society service.⁵⁸ Getting access to the content is subject to stricter requirements, however the basic structure is the same: the intervention can be permitted by a judge if the wiretapping is deemed necessary for investigations into a wilfully (*vorsätzlich*) committed criminal offence punishable by more than one year of imprisonment.⁵⁹ The lawfulness of electronic eavesdropping and dragnet investigations is subject to complex rules. Generally they can be judicially permitted if necessary for investigations into criminal or terrorist organisations or into crimes punishable by more than 10 years of imprisonment.⁶⁰ When the latter two means of investigation were introduced they contained sunset clauses, which – despite their dubious rate of success – were repealed in 2001.⁶¹

A 2005 amendment to the Security Police Act (SPG) authorises the police to keep public places under audio/video surveillance and store the data collected for up to 48 hours or longer if necessary for the investigation of criminal offences committed.⁶² The annual Security Report (*Sicherheitsbericht*)⁶³ contains statistics on wiretapping as well as electronic eavesdropping. In 2008 two audio/optical surveillance operations were carried out and 4,073 wiretaps judicially authorised.⁶⁴

A most contentious issue concerning wiretapping was who had to bear the costs of the surveillance measures. The Constitutional Court declared an ordinance imposing the major part of the costs upon the telecommunications operators unconstitutional.⁶⁵ Still, the 2003 Telecommunications Act requires telecommunications providers to furnish the necessary surveillance equipment, specified by an ordinance by the Federal Minister of

⁵⁷ Sections 134 – 148 StPO. Dragnet investigations were introduced by a 1997 amendment, but have never been carried out according to official sources.

⁵⁸ Section 1 (1) item 2 of the *Notifikationsgesetz* (Notification Act) contains a rather complex definition of these services. What is roughly meant are services normally provided in return for consideration electronically by distance selling at the individual retrieval of the recipient.

⁵⁹ Sections 134, 135 StPO.

⁶⁰ Sections 136, 141 StPO.

⁶¹ Brigitte Zarzer, "Österreich übernimmt Lauschangriff und Rasterfahndung ins Dauerrecht" ("Temporary Rules on Electronic Eavesdropping and Dragnet Investigations Become Permanent"), *Telepolis*, 13 October 2001, available at <http://www.heise.de/tp/r4/artikel/9/9806/1.html>.

⁶² Section 54 (6) SPG, introduced by amendment BGBl. I Nr. 151/2004, which entered into force in January 2005.

⁶³ Sicherheitsbericht 2008 at http://www.bmi.gv.at/cms/bmi_service/start.aspx#t_download.

⁶⁴ *Id.*, at 456 and 582.

⁶⁵ See http://www.epic.org/privacy/intl/austrian_vfgh-022703.html.

Transport, Innovation, and Technology.⁶⁶ A second ordinance regulates the providers' reimbursement, which is based on a case-to-case evaluation of their assistance. The reimbursement contains personnel costs as well as installation, maintenance, and monitoring of the surveillance equipment.⁶⁷

Another most controversial amendment to the SPG⁶⁸, which was motivated by a decision of the DSK⁶⁹, finding police authorities guilty of a violation of the right to secrecy, entered into force in January 2008. It obliges telecommunications service providers and providers of services under Section 3 item 2 E-Commerce Act (*E-Commerce-Gesetz* or ECG) to grant police authorities access to user data like names, addresses, or IP addresses.⁷⁰ Moreover, in case of present danger for person's life and limb, police authorities now have the right to immediately access location data and the user's International Mobile Subscriber Identity (IMSI), as well as the right to use IMSI catchers.⁷¹ A court order is not required in any of these cases. In 2009 the Constitutional Court dismissed a case brought by a telecommunications service provider challenging these novelties.⁷²

Technological development has raised yet another issue. Online searches, especially with the use of remote forensic software (commonly referred to as *Trojaner*) have been controversial since the Federal Ministers of Justice and the Interior came – in principle – to an understanding in October 2007.⁷³ A working group reconsidering the legal framework as well as technical questions came to the result that some online surveillance measures are covered by the existing rules outlined above⁷⁴, however, by and large

⁶⁶ *Überwachungsverordnung* (Ordinance on Surveillance of Telecommunications) BGBl. II Nr. 418/2001 as amended.

⁶⁷ *Überwachungskostenverordnung* (Ordinance on Reimbursement for Surveillance Costs) BGBl. II Nr. 322/2004 as amended.

⁶⁸ Amendment BGBl. I Nr. 114/2007.

⁶⁹ DSK, 20 July 2007 K121.279/0017-DSK/2007. Police had tracked down a man (suspect of having abused and now offering his nine-year-old daughter for sexual abuse in a chat-room) by contacting the operator of the website (identifying the IP address with the help of the nickname) and the Internet access provider (identifying the user) not having obtained a judicial order. Available via <http://www.ris.bka.gv.at/Dsk/>.

⁷⁰ Section 53 (3a) SPG; a major point of criticism are the very vague preconditions which need to be satisfied in order to justify such an interference.

⁷¹ Section 53 (3b) SPG.

⁷² Decision of the Constitutional Court, 1 July 2009, G 31/08-13, available in German at http://www.vfgh.gv.at/cms/vfgh-site/attachments/7/8/0/CH0006/CMS1247635915839/spg_g31-08.pdf.

⁷³ Sebastian Fischer, "*Wiener Koalition erlaubt Online-Durchsuchungen*" ("Vienna Coalition Allows Online-Search"), *Spiegel online*, 19 October 2007, at, <http://www.spiegel.de/politik/deutschland/0,1518,512432,00.html>.

⁷⁴ E.g. when related to messages or communications data (e-mail, voice over IP etc.); optical surveillance; see Sections 135, 136 StPO.

necessary authorising provisions are lacking.⁷⁵ The government programme 2008-2013 includes the aim of introducing online searches, but no action has been taken yet.⁷⁶

In a groundbreaking 2009 decision⁷⁷ the Supreme Court (*Oberster Gerichtshof* or OGH) held that – in the current legal framework – Internet access providers are not obliged to pass on the names and addresses of file-sharers to copyright holders. The relevant provision in the Copyright Act (*Urheberrechtsgesetz* or UrhG⁷⁸) would require Internet providers to process traffic data (i.e. dynamic IP addresses) and link them with the time of a (copyright-infringing) download. However, the TKG⁷⁹, consonant with EU Directive 2002/58/EC⁸⁰, states that except for cases (explicitly) regulated by law, traffic data must not be stored and shall be erased or made anonymous after termination of the connection. Also, as a general principle, the Data Protection Act (DSG) requires the use of data to be strictly earmarked. The TKG, which is interpreted in the light of the Directive, contains exceptions, which allow the processing (and thereby storing) of traffic data for specific purposes. With regard to the principle of legal certainty, the OGH was not convinced that an implicit legal basis for an exception could be deduced from the copyright provision. As data must not be stored for the purpose in question, a civil obligation to disclosure cannot exist.

In 2005 the Data Protection Commission (DSK) rejected a research centre's application for permission to use personal data of drug-addicted convicts who underwent rehabilitation instead of serving their sentence.⁸¹ The researchers intended to use these records to evaluate this new penal approach. With a view to proportionality, the DSK found that the centre had to obtain the convicts' consent before using their personal records.⁸²

National security legislation

No specific information has been provided under this section.

⁷⁵ Daniel AJ Sokolov, "Österreich: Arbeitsgruppe Online-Durchsuchung legt Bericht vor" ("Austria: Working Group Online-Search Presents Report"), *Heise online*, 9 April 2008, at <http://www.heise.de/newsticker/meldung/oesterreich-Arbeitsgruppe-Online-Durchsuchung-legt-Bericht-vor-198121.html>.

⁷⁶ *Regierungsprogramm 2008-2013 "Gemeinsam für Österreich"*, at <http://www.bka.gv.at/DocView.axd?CobId=32965> "><http://www.bka.gv.at/DocView.axd?CobId=32965> . See the Chapter on Justice, the Interior and Defence, sub-chapter Inner Security, A.2,

⁷⁷ OGH, 14 July 2009, 4 Ob 41/09 x, available via <http://www.ris.bka.gv.at/Jus/>.

⁷⁸ BGBl. Nr. 111/1936 as amended. See Section 87b (3) UrhG.

⁷⁹ Section 99 TKG.

⁸⁰ Directive on Privacy and Electronic Communications, see Art. 6 Section 1.

⁸¹ *Suchtmittelgesetz* (Act on Dependence Causing Substances), Section 39.

⁸² DSK, 16 December 2005, K202.042-DSK/2005, available via <http://www.ris.bka.gv.at/Dsk>.

Data retention&&

So far, Austria has not transposed the EU Directive 2006/24/EC on data retention and therefore has been found guilty of a failure to fulfil its obligations by the European Court of Justice (ECJ), which refused to consider any (belated) fundamental rights objections.⁸³ Data retention is largely perceived as a threat in Austria. Presumably legislative action will be deferred until after the European Commission's re-evaluation of the Directive (due in autumn 2010) or even the ECJ's ruling on the preliminary reference by the Irish High Court, challenging the fundamental rights conformity of data retention.⁸⁴

National databases for law enforcement and security purposes

The Austrian Federal Ministry of Interior (*Bundesministerium für Inneres*) operates the national part of the Schengen Information System (N.SIS).⁸⁵ The System contains data on certain wanted/controlled persons and objects. The N.SIS will allow the competent authorities and bodies access, through an automated search, to alerts regarding wanted/controlled persons or objects and persons with refusal of entry in order to fulfil their specific tasks in the field of border control, issuing of visas, residence permits, driver's licenses, customs regime, police and judicial activities, and also to guarantee public order and national and European security. The N.SIS receives additional data from the authorities of other Schengen countries through the SIS-Center in Strasbourg (C.SIS) which is relevant for entry into the Schengen area.⁸⁶

National and international data disclosure agreements

In December 2006 Germany and Austria became the first countries to harmonise their DNA databases under the new "Prüm Treaty".⁸⁷ National contact points are granted access to the reference data in the DNA analysis files and can conduct automated searches by comparing DNA profiles. In case of a hit the searching contact point receives an automated notification. By mutual consent the contracting parties can also compare unidentifiable DNA profiles with all DNA profiles from other national DNA analysis files' reference data. Similar rules apply to fingerprinting and vehicle registration data. Any excessive supply of available personal data is governed by the rules on mutual legal

⁸³ ECJ, 29 July 2010, C-189/09.

⁸⁴ <http://www.digitalrights.ie/2010/05/05/high-court-decision-on-our-data-retention-challenge/>.

⁸⁵ More information on the SIS are available at http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133020_en.htm.

⁸⁶ DSK, Information about Data in the Schengen Information System, available at <https://www.dsk.gv.at/site/6286/default.aspx>.

⁸⁷ The German-Austrian Police and Justice Treaty (*Deutsch-Österreichischer Polizei- und Justizvertrag*) was signed in 2003 and entered into force on 1 December 2005. It was succeeded by the "Prüm Convention" or "Prüm Treaty" which came into force on 23 November 2006 between Austria and Germany. See Art 4 "Prüm Treaty", available at <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf>.

assistance.⁸⁸ Even though the European Data Protection Supervisor considered the privacy elements of the Prüm Treaty were incomplete⁸⁹, the Council decided to integrate the Treaty into EU legislation.⁹⁰

The Austrian DNA database contains more than 132,000 DNA profiles.⁹¹ Officials in the Ministry of the Interior boasts that in terms of DNA database development and use, Austria is among the leading countries in the world.⁹²

Newspapers report that Austria plans to grant the USA access to DNA databases, fingerprint data, and consequently identities of suspects and/or convicts. Allegedly the USA threatened to strike Austria off the Visa Waiver Programme if it did not cooperate sufficiently.⁹³

Cybercrime

No specific information has been provided under this section.

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

The Trade and Commerce Act (*Gewerbeordnung* 1994 or GewO⁹⁴) contains the prototype of direct marketing regulation in Austria. The use of sensitive data⁹⁵ by direct marketing ventures and list brokers in principle depends on the data subject's consent. The data subject can demand the erasure or barring of data stored for marketing purposes free of charge. Also, persons can enrol in a so-called "Robinson-list", administered by a sub-

⁸⁸ Art. 4 – 6 Prüm Convention.

⁸⁹ "European DNA-Data Interchanges Raise Privacy Concern," BJHC & IM Newsletter February 2007 (quoting EDPS Peter Hustinx), <http://www.bjhcim.co.uk/news/1/2007/n702002.htm>.

⁹⁰ Press Release, 12 June 2007, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803>. See Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008, OJ L 210, 6 August 2008, at 1–11.

⁹¹ By 1 April 2010. See http://gerichtsmedizin.at/assets/files/projekte/interpol/gmi_interpol_pressekonferenz20100526_BMI.pdf.

⁹² *Id.*

⁹³ "Österreich gewährt USA Zugriff auf Polizeicomputer" ("Austria granted U.S. Access to Police Computers"), *derStandard.at*, 01 October 2010, <http://derstandard.at/1285199791984/Oesterreich-gewaehrt-USA-Zugriff-auf-Polizeicomputer>.

⁹⁴ BGBl. Nr. 194/1994 as amended. See Section 151 GewO.

⁹⁵ Section 4 item 2 DSG.

division of the Austrian Economic Chamber (*Wirtschaftskammer Österreich*), which bars them from receiving advertising material and prevents their data from being used.

The Telecommunications Act⁹⁶ and the E-commerce Act (*E-Commerce-Gesetz* or ECG⁹⁷) contain rules on unsolicited commercial communications. Calls and facsimile transmissions for marketing purposes are not permitted without prior consent of the subscriber or a person authorised to use his line. The sending of electronic mail – including SMS messages – to customers for purposes of direct marketing or addressed to more than 50 recipients is in principle not permitted without the recipients' prior consent. Exceptions exist where the sender has received the contact details in the context of a sale or service to his customers, as long as they had the opportunity to object, free of charge and in an easy manner, to the use of these contact details and are not registered with a list according to section 7 ECG.

If the identity of the sender on whose behalf the communication is transmitted is disguised or concealed or if there is no valid address to which the recipient may send a request that such communications cease, the sending of electronic communications is prohibited.

Any person violating the rules outlined above commits an administrative offence punishable by a fine of up to €37,000.⁹⁸ The 2007 Supervision of Securities Act (*Wertpapieraufsichtsgesetz* or WAG⁹⁹) extends the TKG-regime to the unsolicited advertising of financial instruments and investments.

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section

Online youth safety

No specific information has been provided under this section.

⁹⁶ Section 107 TKG, setting rules for calls and facsimile transmissions on the one hand and electronic mail, including SMS messages on the other hand.

⁹⁷ BGBl. I Nr. 152/2001. Sections 6 – 8 ECG, covering electronic mail.

⁹⁸ Section 109 (3) items 19 – 21 TKG.

⁹⁹ BGBl. I Nr. 60/2007. See Section 62.

TERRITORIAL PRIVACY

Video surveillance

In 2006 a Viennese lawyer expressed concern that more than 100,000 illegal monitoring systems with recording functions existed in Austria.¹⁰⁰ As most of these systems were used illegally, i.e. without prior permission of the Data Protection Commission (DSK), enforcement of the legal restrictions was hardly possible. The first-ever permission had provisionally been granted to Vienna's public transport system, *Wiener Linien*, to see whether such a system could help to prevent vandalism. However, at that time, police stations, banks, traffic monitoring, etc. used video surveillance legally.¹⁰¹

Before the amendment to the Data Protection Act (DSG) entered into force on 1 January 2010, video surveillance was covered by the general provisions of the DSG¹⁰², which were designed with a view to "classical" data protection challenges, increasingly leading to difficulties in their application to video surveillance issues. The newly introduced Chapter 9a, comprising Sections 50a – 50e, sets out a general framework for video surveillance, while sector-based specificities remain. Audio surveillance ("private eavesdropping") is not included.

Video surveillance is defined with a special emphasis on the aspect of systematic (especially continuous) monitoring.¹⁰³ The rules on the legitimate use of data as well as the principle of proportionality apply. Furthermore video surveillance is only admissible if it is the least intrusive means. Notably, real-time surveillance is a less intrusive means than recording.

Section 50a (3) and (4) DSG contains *leges speciales* on the question of which interests in secrecy deserve protection. Video surveillance by the police is regulated in sector-based laws, especially the Security Police Act (SPG¹⁰⁴). Subsection 4, requiring a balancing of interests, is relevant only for the private sector. Justifiable encroachments are concrete threats regarding objects or persons under surveillance, legal norms that prescribe exercising due care and real-time surveillance limited to rendition. The resulting interferences are then not considered violations of interests in secrecy deserving protection.¹⁰⁵ However, even surveillance that is admissible under the rules outlined

¹⁰⁰ EDRI-gram, "Illegal Video Surveillance in Austria," 25 October 2006, at <http://www.edri.org/edriagram/number4.20/Austria>.

¹⁰¹ *Id.*

¹⁰² Especially the following sections of the DSG: 6 – 9 (legitimate use), 17 *et seq.* (notification and registration), 24 (duty to provide information), and 26 (right to information).

¹⁰³ Section 50a (1) DSG.

¹⁰⁴ See section 54 (4), (5) SPG.

¹⁰⁵ Section 50a (4) items 1 – 3 DSG

above may not capture intimate locations like private apartments, lavatories, or changing rooms.¹⁰⁶

A controller can lawfully transmit random recordings (captured beyond the purpose and admissibility of a video surveillance measure) to the competent authorities when there is a reasonable suspicion that a criminal act has been committed. A controller cannot refuse delivery of recordings to courts or administrative authorities that are then solely responsible for the lawfulness of such requests.

Recordings have to be logged and erased after 72 hours.¹⁰⁷ The installation of video surveillance is regularly subject to notification and to prior checking by the DSK.¹⁰⁸ Moreover, the controller has an obligation to indicate areas under video surveillance in order to enable potential data subjects to avoid being recorded.¹⁰⁹ As far as real-time video surveillance is concerned, there is no right to information. In all other cases the person seeking information is entitled to a copy of the recordings that relate to him/her. Third-party interests in secrecy etc. can conflict with the right to obtain a copy of the recordings. In such a case the right to information can be satisfied by a detailed, written description. Additional information such as origin, recipients, legal basis etc. can always be provided in writing or – with the data subject's consent – orally.¹¹⁰

In spring 2010 the DSK temporarily banned Google Street View after it became public that W-LANs had been sniffed and even unencrypted content data had been recorded during the systematic photographing of street views.¹¹¹ According to Google, only bits and pieces were recorded. However, the DSK could not rule out that, contrary to the registration, additional informative data had been recorded and therefore temporarily banned the data application Google Street View while the case is pending with the Commission.¹¹²

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this section

¹⁰⁶ Section 50a (5). See also the Explanatory Report, in German at http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_00472/fname_172230.pdf.

¹⁰⁷ Section 50b DSG.

¹⁰⁸ Section 50c DSG.

¹⁰⁹ Section 50c DSG.

¹¹⁰ Section 50e DSG.

¹¹¹ *ARGE DATEN "Österreichische Datenschutzkommission verbietet Googles Street View"* ("DSK bans Google Street View"), at http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=63497usw.

¹¹² DSK, "Google Street View", in German at http://www.dsk.gv.at/site/cob__39654/6733/default.aspx.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

Since 2006 passports are equipped with RFID chips containing data such as the name, a photograph and – since March 2009 – two fingerprints, usually taken from the index fingers.¹¹³ Local or district authorities that issue the passport scan the fingerprints and then store the data only on the RFID chip.¹¹⁴ Minors under the age of 12 are exempt from fingerprinting.¹¹⁵

National ID & smart cards

In 2005 Austria introduced the "e-card", a social security smart card, which plays a fundamental role in the social security online administrative system ("ELSY"). The e-card, which has to be produced upon any consumption of health services, has replaced health insurance certificates throughout the European Economic Area (EEA) and grants access to a platform for many other e-health services. It is designed as a key card, containing name, date of birth, sex, and social security number.¹¹⁶ Upon the explicit request of the cardholder, emergency data can be stored on the e-card.¹¹⁷ With the consent of the cardholder, the e-card grants access to further personal data. To that end physicians etc. have a key-card authorising their access to the relevant data.¹¹⁸

Additionally the e-card can include the function of a citizen card (*Bürgerkarte*¹¹⁹). The idea of a mandatory citizen card including tax number and other data has been abandoned. Today many privately issued smart cards (e.g. bank cards, member cards) with certain technical specificities can be equipped with an electronic authentication function. The Austrian Computer Society issued the first examples of these citizen cards in December 2002, which were valid until 2005.¹²⁰

RFID tags

No specific information has been provided under this section

¹¹³ (Passgesetz or PassG (Passport Act), BGBl. Nr. 839/1992 as amended, Section 3 (5). *See also* the Executive Order of the Minister of the Interior, BGBl. II Nr. 223/2006 as amended.

¹¹⁴ Ministry of the Interior, "Der neue Sicherheitspass" ("The New Secure Passport"), available at http://www.bmi.gv.at/cms/BMI_Service/reisepass/files/FlyerZickZack.pdf.

¹¹⁵ Section 8 (5) PassG.

¹¹⁶ *Allgemeines Sozialversicherungsgesetz* or ASVG (General Act on Social Security), Section 31a (3).

¹¹⁷ Section 31a (5) ASVG.

¹¹⁸ See http://www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?action=2&p_menuid=51906&p_tabid=4.

¹¹⁹ See "E-Government", *infra*.

¹²⁰ See <http://members.ocg.at/>.

BODILY PRIVACY

No specific information has been provided under this section

Workplace privacy

In 2006 the Supreme Court issued an injunction proscribing the use of a biometric time reading system using fingerprint scanners in a hospital. The Court held that even the use of templates (and not the biometric raw data), created a connection with specific employees and fell within the ambit of human dignity. As measures touching upon human dignity can only be introduced by an employer/works council agreement. The decision virtually put an end to the use of biometric time recording systems.¹²¹

Another issue is the use of the Internet for private purposes at work. Even though employers can prohibit the private use of the Internet, introducing a permanent control system constitutes a measure interfering; upon human dignity and therefore requires an employers/works council (or contractual) agreement. Whether a total prohibition of private use would be enforceable (justifying a dismissal etc.) is more than doubtful.

A far more delicate problem concerns employers' control of the content of employees' private e-mails. In principle, under no circumstances is the employer authorised to read private communications, not even if the private use of the Internet is entirely forbidden. However, the employer has a right to exercise (a certain amount of) control over professional communications, hence private e-mails – in order not to be read – must be clearly labelled as such. With a view to the fact that evidence gathered illegally can be produced in court, even the labelling does not reliably grant privacy.¹²² E-mails with critical content should therefore not be sent via an employer's server.

The 2010 amendment to the Data Protection Act (DSG) explicitly prohibits purposeful monitoring of employees by video surveillance at their workplace.¹²³ The surveillance of objects at the workplace for reasons other than efficiency control is not covered by this prohibition.

¹²¹ OGH, 20 December 2006, 9 ObA 109/06 d. See *Arbeitsverfassungsgesetz* or ArbVG (Labour Constitution Act) Section 96 (1) item 3. See also *ARGE DATEN*, "OGH hat entschieden – AUS für biometrische Stempeluhr" (Supreme Court Decides: No Biometric Time Recording Systems) 12 February 2007, at http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=09391war.

¹²² Christine Kary, "'Big Brother' am Arbeitsplatz" ("Big Brother' at Workplace"), *Die Presse*, 28 March 2007, at <http://diepresse.com/home/wirtschaft/economist/293711/index.do> ; see also Thomas Angermaier "Surfen und private E-mails am Arbeitsplatz" ("Surfing and Personal E-mails at Work"), PRVAnews, October 2008, at http://www.dbj.co.at/phps/start.php?noie=1&lang=de&content=publikationen_show.php&navi=publikationen&publikation_nr=513.

¹²³ Section 50a (5) DSG.

HEALTH & GENETIC PRIVACY

Medical records

Like most other countries, Austria has laws requiring that carriers of certain dangerous infections be reported to health authorities.¹²⁴ Exceptions to the general rule of medical confidentiality can be found where serious injuries have obviously been caused by criminal activity or in cases of child abuse. Another challenge results from the exchange of health data through electronic systems. The *Gesundheitstelematikgesetz* (GTelG¹²⁵) regulates the use of telematics in the health service sector, including data security and information management. It deviates from the DSG insofar as only direct personal data fall within the scope of this law. The DSG in particular requires identity and legitimate authority of the data recipient to be sufficiently established. In contrast, the GTelG establishes minimum identity requirements as well as mechanisms trying to prevent misuse.

Since first steps to implement the Health Reform Act 2005 (*Gesundheitsreformgesetz* 2005¹²⁶) were taken in 2006, the Electronic Health File (*Elektronische Gesundheitsakte* or ELGA) has been a most controversial issue. Proponents describe ELGA as a key instrument in Austrian e-health ambitions that electronically administers all relevant health data while sufficiently protecting patients' rights, especially with a view to data protection.¹²⁷ It enables authorised persons to access all available health data regardless of time or location of treatment. Opponents fear the abolishment of medical confidentiality and criticise the imprecise definition of health care service providers who are granted access to ELGA. Patients have no access to the health care service provider index.¹²⁸ Finally, the term "health data" is defined extremely broadly, comprising personal data on the physical and psychological well-being as well as data gathered in the course of determining that status, including accounting for health services and patients' health-related habits and environmental influences.¹²⁹ ELGA is about to be introduced and implemented by the "ELGA limited" (ELGA GmbH), which was founded in 2009 and took over the agenda of "Arge ELGA" as of 1 January 2010.¹³⁰

¹²⁴ *Epidemiegesetz* (Law on Epidemics) 1950, *Tuberkulosegesetz* (Law on Tuberculosis) 1968, *AIDS-Gesetz* (Law on HIV) 1993, *Geschlechtskrankheitengesetz* (Law on Venereal Diseases) 1945. A complete list of all relevant infections can be obtained at <http://www.infektionsnetz.at/>.

¹²⁵ See *supra*.

¹²⁶ BGBl. I Nr. 179/2004, available at http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2004_I_179/BGBLA_2004_I_179.pdf.

¹²⁷ See <http://www.elga.gv.at/> (in German).

¹²⁸ *ARGE DATEN*, "AMS, ELGA und das verlorene Ärztegeheimnis" ("ELGA and the Lost Secret of Doctors"), 16 February 2007, at http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=08596tae.

¹²⁹ Section 2 item 1 GTelG, regulating the use of telematics in the health sector.

¹³⁰ See <http://www.elga.gv.at/index.php?id=3>.

Genetic identification

The Genetic Engineering Act (*Gentechnikgesetz* or GTG¹³¹) requires confidentiality of personal data gathered through genetic analysis and gives the person examined a right to access as well as a right to information. The use of non-anonymous data for any other than the original purpose requires the written consent of the data subject. The GTG also contains an explicit prohibition on the use of genetic data by employers and insurance companies.¹³² The DSG includes specific provisions on scientific research.¹³³ Apart from that it deals with medical data in a very general way, considering it "sensitive data", consequently benefitting from a more rigid protection.

Financial privacy

The Banking Act (*Bankwesengesetz* or BWG¹³⁴) deals with special requirements and restrictions concerning the use of client data. The central provision concerning privacy, Section 38, which has quasi-constitutional status, guarantees bank client confidentiality. Section 38 contains a set of exceptions, covering court orders in criminal proceedings or administrative proceedings for certain fiscal offences. Austria has adopted a new anti money laundering law according to the standards of the Organisation for Economic Cooperation and Development (OECD). Banks now have to establish the identity of customers wishing to open an account or of non-customers wishing to conduct financial transactions exceeding the limit of €15, 000.¹³⁵ Due to critics' claims that Austria was creating a tax haven a 2009 law loosened the requirements for interstate cooperation.¹³⁶ Banking institutions are now obliged to transmit all foreseeably relevant data (via the Austrian Ministry of Finance) upon a foreign public authority's request proving at least a reasonable suspicion of tax evasion.¹³⁷ Banking institutions must also comply with the DSG. They are not allowed to use personal data obtained through client accounts for other purposes. Section 18 DSG requires the prior registration of data applications whose purpose is to give information on the data subject's creditworthiness.¹³⁸

¹³¹ BGBl. Nr. 510/1994 as amended; see Section 71 GTG.

¹³² Section 67 GTG.

¹³³ Sections 46, 47 DSG.

¹³⁴ See *supra*.

¹³⁵ § 40 BWG.

¹³⁶ *Amtshilfe-Durchführungsgesetz* (Assistance Implementation Law) BGBl. I Nr. 102/2009.

¹³⁷ Explanatory Report, German version available at http://www.parlament.gv.at/PAKT/VHG/XXIV/A/A_00681/imfname_161425.pdf.

¹³⁸ A large part of complaints with the Data Protection Commission concerns databases on creditworthiness. See *Datenschutzbericht* 2009, *supra* at 35.

As a rule, creditworthiness ratings by private agencies are data applications open to inspection by the public.¹³⁹ The service provider (i.e. the controller) has a duty to inform the data subject about the purposes for which the data is collected and the name and address of the controller. However, violating the principle of fair and lawful use¹⁴⁰, this duty is often ignored, which makes the entry unlawful¹⁴¹ and is in itself sufficient to have the data erased.¹⁴² Once per year a data subject has the right – free of charge – to ask for information about the processed data, its origin, recipients, transmissions, purpose, and legal basis. If law does not mandate the inclusion of data in a data application open to inspection by the public, such as a creditworthiness database, the data subject can object at any time and without any need to give reasons. As a consequence the data must be erased within eight weeks.¹⁴³ According to the Supreme Court (OGH) data subjects also have the option to object partially and demand corresponding erasure.¹⁴⁴ Erasure means the physical (not just logical) erasure. Reorganising data is not sufficient for controllers to comply with their duty.¹⁴⁵

The Consumer Credit Act 2010 (*Verbraucherkreditgesetz* or VKrG¹⁴⁶) introduces an exception to the right to objection for joint information systems of crediting institutions registered with the Data Protection Commission (DSK), such as the "Consumer Credit Evidence" or the banking institutions' "Warning List". In these cases erasure of data is subject to considerably stricter requirements.¹⁴⁷

E-GOVERNMENT

The Federal Government's online platform "Digital Austria" offers comprehensive information about e-government applications in Austria, prioritising "the integration of all citizens, data protection management, and customer orientation".¹⁴⁸

¹³⁹ Section 4 item 7 DSG. Openness to public inspection is not excluded if the service requires pay for use. Supreme Court (OGH), 1 October 2008, 6 Ob 195/08 g.

¹⁴⁰ Section 6 (1) item 1 DSG.

¹⁴¹ OGH, 15 December 2005, 6 Ob 275/05 t.

¹⁴² *ARGE DATEN*, "Löschungsanspruch gegenüber Wirtschaftsauskunftsdiensten & Banken" ("Right to Erasure vis-à-vis Creditor Protection Agencies and Banks"), available at http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=30575bvj.

¹⁴³ Section 28 (2) DSG.

¹⁴⁴ OGH, 1 October 2008, 6 Ob 195/08 g.

¹⁴⁵ OGH, 15 April 2010, 6 Ob 41/10 p.

¹⁴⁶ BGBl. I Nr. 28/2010, which entered into force in June 2010. See Section 7 (5) VKrG.

¹⁴⁷ Sections 24, 27 and 28 (1) DSG. *ARGE DATEN*, "Löschungsanspruch gegenüber Wirtschaftsauskunftsdiensten & Banken," *supra*.

¹⁴⁸ See <http://www.digitales.oesterreich.gv.at/DesktopDefault.aspx?alias=egov&init>.

The central element of e-government in Austria is the citizen card (*Bürgerkarte*), an electronic identification concept (and not a physical object), which uniquely identifies a person by digital means and can *inter alia* be used to deal with administrative authorities securely or functions as an online ID as well as a secure and qualified online signature.¹⁴⁹ The unique identification of a natural person – the only kind of person entitled to hold a citizen card – is effected by an identity link established with the help of a particular source identification number (*Stammzahl* or sourcePIN).¹⁵⁰ The sourcePIN is usually derived from that person's registration number in the Central Register of Residents and secured by using strong cryptography.¹⁵¹ The Data Protection Commission (DSK) acts as the sourcePIN register.¹⁵² For security reasons, the sourcePIN is stored permanently only in the citizen card; however, it can be regenerated by the sourcePIN register whenever required. In a next step the sector-specific ssPIN (*bereichsspezifisches Personenkennzeichen* or bPK) is derived from the sourcePIN of a natural person. The ssPIN's use is then limited to a specific sector of State activity.¹⁵³

Austrian privacy organisations have strongly criticised the DSK's role, for it acts as its own supervisory body and no independent mechanism of control has been established at the heart of this national identification system.

Electronic delivery can be chosen as an additional service, which is carried out by (private) electronic delivery services. The providers have to prove their reliability, especially with respect to data protection, and are subsequently licensed by the Federal Chancellery.¹⁵⁴

In 2007, the reform of the electoral law extended the franchise by lowering the age limit to 16 years and introduced voting by mail from within the country.¹⁵⁵ As a reaction to a decision by the Constitutional Court (VfGH), absentee voting had been introduced in 1990, allowing Austrians living abroad to exercise their franchise by mail.¹⁵⁶ E-voting and the extension of voting by mail have been subject to lively discussions ever since. As of 2007, voting by mail no longer requires a witness to prove the personal exercise of the right to vote. Instead, the voter signs a statutory declaration on the outside of the envelope (*Wahlkarte*). Sealing the envelope also covers the signature. Later the perforated

¹⁴⁹ See *Signaturgesetz* (Electronic Signature Act) BGBl. I Nr. 190/1999 as amended, Section 2 item 3a and Section 4.

¹⁵⁰ Section 4 (1) and (2), E-GovG.

¹⁵¹ Section 6 (2) E-GovG.

¹⁵² Section 7 E-GovG.

¹⁵³ Section 9 (1) E-GovG.

¹⁵⁴ *Zustellgesetz* (Service of Documents Act) BGBl. Nr. 200/1982 as amended, Section 30 (1); *Zustelldienstverordnung* (Delivery Service Regulation) BGBl. II Nr. 233/2005 as amended, Section 3.

¹⁵⁵ Cf. Art 26 sections 1 and 6 B-VG for national parliamentary elections.

¹⁵⁶ VfSlg. 12.023, Decision of the Constitutional Court, 16 March 1989, G 218/88.

seal can be opened in a way that allows identifying the voter without at the same time disclosing the ballot, which is sealed in a second envelope.

However, there is no constitutional basis for e-voting. Neither voting through the Internet nor the use of electronic voting machines at the polling station is admissible in national, regional, or local elections. The first elections offering an e-voting option were the Austrian Student Union (*Österreichische Hochschülerschaft*) elections in 2009. A turnout of 0.9 percent of online voters led the Ministry of Science to temporarily abandon its support for the e-voting experiment. Moreover, certain malfunctions led to successful challenges of the elections at the universities of Vienna and Salzburg.¹⁵⁷ Hence, the 2011 elections will go back to the traditional ballot.

Finally it has to be mentioned that before the reform of the electoral law in 2007, the Austrian Constitution allowed the States (*Bundesländer*) to introduce compulsory voting in State elections.¹⁵⁸

This "Transparency Database" has been a matter of political dispute for more than a year; however, it's only recently that the government agreed in principle on the features of this database. The draft law¹⁵⁹ is now subject to expert opinions. It will establish a database which will be run by the BRZ limited (*Bundesrechenzentrum GmbH*) for the federal government. It will contain net income and social benefits for individuals and state aid, subsidies, and tax benefits (e.g. resulting from group taxation) for companies, and state aid as well as subsidies for agriculturists. The database will be accessible for the data subject only and the granting of further benefits will require forwarding an electronic copy, which – in exceptional cases – will contain information on the applicant's entire household. The government can authorise aggregated and anonymous analyses by the BRZ limited.

OPEN GOVERNMENT

The Freedom of Information Act (*Auskunftspflichtgesetz*¹⁶⁰) compels federal authorities to provide information concerning their areas of responsibility insofar as there is no conflicting obligation to maintain confidentiality. However, no right to access documents is granted and the duty to provide information is limited in scope, as other tasks of the administration should not be seriously affected. Similar laws exist in the nine states (*Bundesländer*).

¹⁵⁷ Daniel AJ Sokolov, "Vorläufiges aus für E-Voting in Österreich" ("Temporarily No further E-Voting in Austria"), 03 April 2010, at <http://www.heise.de/newsticker/meldung/Vorlaeufiges-Aus-fuer-E-Voting-in-Oesterreich-969992.html>.

¹⁵⁸ Cf. Art 60 (1) B-VG in the relevant version before 1 July 2007.

¹⁵⁹ *Transparenzdatenbankgesetz* (TDBG), available at https://www.bmf.gv.at/steuern/fachinformation/neuegesetze/transparenzdatenban_11344/tdbg_01092010-entwurf.pdf?q=transparenzdatenbank.

¹⁶⁰ BGBl. Nr. 287/1987 as amended.

The Security of Information Act (*Informationssicherheitsgesetz* or InfoSiG¹⁶¹) aims at implementing obligations under international law concerning the secure use of classified information. Persons (e.g. civil servants etc.) disclosing classified information which they gained access to based on this law and which could impair Austria's public security, national defence, or foreign relations, commit a criminal offence. The penalty ranges from a fine to imprisonment up to six months, in special cases up to one year. Sanctions against journalists etc. who spread such information are not stipulated in the law. When the law was drafted it was criticised for being poorly formulated and there were concerns that it might adversely affect the free flow of information. The fact that any official¹⁶² could classify his/her files raised fears that this tool could be used to restrict public scrutiny.¹⁶³ When the law was finally adopted those fears had been widely put aside.

Today, "industrial security" is a most important field of application of the InfoSiG. A commission in the Federal Chancellery issues "Facility Security Clearances" for companies or research centres who make bids on international tenders that involve classified official information.¹⁶⁴

Other recent factual developments (with an impact on privacy)

Due to an amendment to the Austrian Broadcasting Corporation Act (*ORF-Gesetz*) the public broadcaster ORF (*Österreichischer Rundfunk*) had to shut down its "special interest" online platform "Futurezone" as of 1 October 2010.¹⁶⁵ Futurezone, which had been dealing with net politics, data protection, and civil rights for 11 years, was among the most renowned German-language institutions in the field.¹⁶⁶ According to the ORF, the archives will be maintained and at some point publicly available.¹⁶⁷

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Among the organisations that actively advocate data protection and privacy in Austria, there is "ARGE DATEN", a non-profit, non-governmental organisation, which is examining the interaction between usage of computer science, information law, and society. Its aim is the human and socially responsible use of information technology and

¹⁶¹ BGBl. I Nr. 23/2002 as amended.

¹⁶² The author or originator; see *Informationssicherheitsverordnung* (Ordinance on Security of Information), BGBl. II Nr. 548/2003, section 3 (2).

¹⁶³ ARGE DATEN, "Das Informationsverhinderungsgesetz...", 19 November 2001, http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=03985nja.

¹⁶⁴ Sections 11 *et seq.* InfoSiG.

¹⁶⁵ The Vienna newspaper *Kurier* runs a new platform under futurezone.at, which has no editorial link to the former futurezone.orf.at. <http://news.orf.at/stories/2017383/>.

¹⁶⁶ Cf. e.g. "ORF soll Qualität sparen, nicht Geld" ((ORF Cuts Down on Quality, not on Costs) *Zeit online*, at <http://www.zeit.de/digital/internet/2010-06/orf-futurezone?page=2>.

¹⁶⁷ According to an e-mail by online@orf.at (13 October 2010) a link has not yet been established.

telecommunications.¹⁶⁸ Another organisation is "*Quintessenz*," a platform whose mission is the restoration of civil rights that have been abolished by technical means during the first stage of the information revolution.¹⁶⁹ "VIBE!AT" is an association promoting the responsible and self-determined use of the Internet. It actively tries to create public awareness of attempts to overly limit this freedom.¹⁷⁰

The initiative "Open Government Data Austria", which was newly formed in 2010, is campaigning for free and better access to public, non-personal data (e.g. census data, environmental data, traffic data, etc) through mash-ups, new user interfaces, and a standardised format (Linked Open Data or LOD). The initiative, which is supported by researchers and universities, aims at cooperating with public authorities and their e-government ambitions to the benefit of citizens, economy, and administration.¹⁷¹

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Austria has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and its First Optional Protocol, which establishes an individual complaint mechanism.¹⁷²

Austria is a member of the Council of Europe and the ECHR forms part of the Austrian Constitution.¹⁷³ Austria has signed and ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data¹⁷⁴ as well as the Additional Protocol regarding supervisory authorities and cross border data flows.¹⁷⁵ It has also signed but not yet ratified the Convention on Cybercrime ("Budapest Convention").¹⁷⁶

¹⁶⁸ Cf. http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15048tpb.

¹⁶⁹ See generally <http://www.quintessenz.at/cgi-bin/index?funktion=about>.

¹⁷⁰ See generally <https://www.vibe.at/verein>.

¹⁷¹ See generally <http://gov.opendata.at/site/about>.

¹⁷² Austria has signed the ICCPR on 10 December 1973 and ratified it on 10 September 1978. It has signed the First Optional Protocol to ICCPR on 10 December 1973 and ratified it on 10 December 1987. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁷³ Cf. Constitutional Privacy Framework, *supra*. See also ETS No. 005, signature 13 December 1957, ratification and entry into force 3 September 1958, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=26/10/2010&CL=ENG>.

¹⁷⁴ ETS No. 108, signature 28 January 1981, ratification 30 March 1988, entry into force 1 July 1988, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

¹⁷⁵ ETS No. 181, signature 8 November 2001, ratification 4 April 2008, entry into force 1 August 2008, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

¹⁷⁶ ETS No. 185, signature 23 November 2001, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

As a member of the OECD, Austria also cooperates with this organisation. Finally, Austria has bi- and multilateral treaty obligations with ramifications on privacy and data protection.¹⁷⁷

As a member of the European Union Austria has a duty to transpose the content of EU privacy and data protection legal instruments (e.g. the Data Protection Directive (1995/46/EC), the Directive on Privacy and Electronic Communications (2002/58/EC), the E-Commerce Directive (2000/31/EC)) into its national legal order. Relevant Austrian institutions also have a general duty to interpret national law in conformity with EU law.

¹⁷⁷ Cf. e.g. the "Prüm Treaty" "International Data Disclosure Agreements," *supra*.

KINGDOM OF BELGIUM

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Belgian Constitution recognises the right of privacy and private communications¹ Article 22 prohibits government infringement on the private life of individuals by stating that, "Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by law..."²

The Constitution protects the confidentiality of letters (Article 29). This article does not, however, apply to electronic communications. The secrecy of electronic communications is explicitly protected under the Electronic Communication Act.³

The Constitution also contains a provision protecting the freedom of the press. Article 25 states that "The press is free; censorship can never be established; a surety bond from authors, publishers, or printers cannot be demanded."

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Law on Protection of Personal Data of 1992 (or 'Data Protection Act') governs the processing and use of personal information in Belgium. Amending legislation to update the 1992 Act and make it consistent with the European Union (EU) Data Protection Directive was approved by the Parliament in December 1998.⁴ It received a royal decree (*Arrêté royal*) and was adopted in February 2001; it entered into force in September of the same year, further implementing the Data Protection Act.⁵ The royal decree specifies the conditions under which personal data can be further processed for historical, statistical, or scientific purposes; sets additional requirements for the processing of sensitive data and the processing of data not collected directly from the individual;

¹ Constitution of Belgium, available at http://www.fed-parl.be/constitution_uk.html.

² Article 22 was added to the Belgian Constitution in 1994. Prior to this constitutional amendment, the Supreme Court (*Cour de cassation*) had already held that Article 8 of the European Convention of Human Rights found direct application in the Belgian legal system. *Cour de cassation*, 26 September 1978.

³ Act of 13 June 2005 on Electronic Communications, *Moniteur belge* (Belgian State Gazette), 20 June 2005, at 28.070.

⁴ Act concerning the Protection of Privacy with regard to the Treatment of Personal Data Files, December 8, 1992 (*Loi relative à la protection des données à caractère personnel du 8 décembre 1992*) as amended by the Act of 11 December 1998 transposing EU Directive 95/46/EC of 24 October 1995, available at <http://www.law.kuleuven.ac.be/icri/itl/12privacylaw.php>.

⁵ Royal Decree of 13 February 2001, *Moniteur belge* (Belgian State Gazette), 13 March 2001, at 7839-7919.

specifies the modalities of individuals' rights (access, rectification, deletion); and further explains notification obligations. The royal decree also sets out penalties ranging from fines (Articles 37-39), publication of a judgment in a newspaper after conviction (Article 40), confiscation of filing systems, and orders to erase data (Article 41).

Sector-based laws

See below under the relevant thematic sections.

DATA PROTECTION AUTHORITY

The Commission for the Protection of Privacy (*Commission de la protection de la vie privée*, or Commission) oversees the application of the Data Protection Act and reports directly to the Parliament.⁶ The Commission investigates complaints, issues opinions, and maintains the registry of personal files.⁷ In 2008, the Commission answered 363 complaints and 2,096 requests for information.⁸ Complaints give way to a mediation by the Commission. In 2008, 44 percent of mediations have focused on consumer credit contracts and the related registration in the central credit database (*Centrale des crédits aux particuliers*) held by the National Bank. Requests for information have mainly concerned video surveillance (14 percent), marketing software for financial and commercial actors (12 percent), public authorities and privacy (12 percent), data protection in work relationships (11 percent), and credit files (9 percent). The number of public requests for information also increased from about 6,200 in 1999 to about 7,400 in 2001, and 2,096 in 2008⁹. As of June 2010, there are 55 permanent members of staff,¹⁰ compared to 34 in 2004, 19 in 2001, and 28 in 2000.¹¹

Sector committees have been established within the Commission by Belgian law, either the general Privacy Act or sector-specific acts. Each Committee is charged with overseeing privacy practices in a specific sector and is made up of Commission members and experts familiar with the sector in question. There are currently six sector committees, one for each of: the National Registry; the Social Security and Health; the Federal Authorities; the Crossroads Bank of Enterprises ("*Banque-Carrefour des Entreprises*"), the central database that contains all relevant information about

⁶ Privacy Commission (*Commission de la protection de la vie privée*) homepage <http://www.privacycommission.be/>.

⁷ As of 30 June 2004, there were 23,883 records in the Commission's registry. Email from An Machtens, Conseiller POMIS, Commission de la protection de la vie privée, to Cédric Laurant, Policy Counsel, Electronic Privacy Information Center (EPIC), 12 July 2004 (on file with EPIC).

⁸ Privacy Commission (*Commission de la protection de la vie privée*), Annual Report for 2008, available at <http://www.privacycommission.be/fr/static/pdf/annual-reports/rapport-annuel-2008.pdf>.

⁹ *Id.*

¹⁰ Email from An Machtens, *supra*.

¹¹ Emails from Hannelore Dekeyser and Anne-Christine Lacoste, *supra*.

enterprises); the Phenix Sector Oversight Committee, which supervises privacy in the judiciary; and the Statistical Oversight Committee.

The Commission has issued a number of recommendations¹² relating *inter alia* to workplace privacy (Opinion n° 10/2000), video surveillance (Opinions n° 34/99, n° 3/2000, n° 4/2004, n° 10/2005, n° 31/2006, n° 22/2007), the compatibility of the census survey (conducted every ten years) with Belgian privacy regulations (Opinion n° 37/2001), the protection of privacy in the context of electronic commerce (Opinion n° 34/2000), the regulation of direct marketing under the data protection legal framework (Recommendation n° 4/2009),¹³ the recording by banks of their customers' telephone communications (Recommendation n° 01/2002), the use of electronic communications for electoral advertising purposes (Opinion n° 7/2003), the project of royal decree regarding the model contract on matrimonial brokerage, publication of facial images (particularly in a school context) (Opinion no 33/2007), user and access management in e-government (Recommendation n° 1/2008), the processing of biometric data (Opinion n° 17/2008), information collected from candidates for house rentals (Recommendation n° 1/2009), draft legislation relating to the use of biological material (Opinions n° 10/2009, n° 16/2009 and n° 17/2009), and e-ticketing (Recommendation n° 1/2010), etc.¹⁴

In 2009, the Commission began releasing recommendations for rules regarding the secondary use of information gathered for different public purposes. For example, a sociologist completing a study of gender and class in the criminal justice system will only be able to make use of a public database that collects the names of individuals working in the criminal justice system for the purpose of maintaining employee records if the researcher follows the Commission's recommendations.¹⁵

Major privacy & data protection case law

In March 2009, Yahoo! was fined by a Belgian court for not disclosing the personal data of people involved in a cybercrime investigation.¹⁶ Yahoo! argued that investigators could not legally make this request and that Belgian authorities should have contacted the US government first, as required by a treaty between both countries. In late 2010, an appeals

¹² All opinions of the Commission are available in Dutch and French at <http://www.privacycommission.be>. In this report we refer to the number of the advice and the year so you can easily retrieve the document from the Web site.

¹³ See also *SPF Economie*, "Le spamming en 24 questions et réponses", http://economie.fgov.be/fr/binaries/spamming_brochure_fr_tcm326-31741.pdf.

¹⁴ These recommendations and opinions can be found at the Web site of the Privacy Commission (in French and Dutch) at <http://www.privacycommission.be/nl/decisions/>.

¹⁵ "La Commission de la protection de la vie privée formule des recommandations dans le cadre de traitements ultérieurs", available at http://www.privacycommission.be/fr/decisions/commission/processing_recommendations.

¹⁶ EDRI-gram, No. 7.5, "Yahoo Penalised in Belgium for not Disclosing Personal Data," 11 March 2009 <http://www.edri.org/edri-gram/number7.5/belgium-decision>.

court overturned the decision, holding that the US email service provider could not be compelled under law to provide users' data to Belgian law enforcement authorities.¹⁷

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Surveillance of communications is regulated under the Law of 30 June 1994.¹⁸ Prior to its enactment, there was no specific law on this subject. The law requires permission of a *juge d'instruction* before wiretapping can take place. Orders are limited to a period of one month. There were 114 orders issued in 1996,¹⁹ and reportedly around 1,000 in 2002.²⁰ The law was amended in 1997 to remove restrictions on the use of encryption.²¹ The Parliament also amended the law in 1998²² to force telecommunications carriers to provide greater assistance and to give the *juge d'instruction* and the Attorney General (*Procureur du Roi*) more powers. The *juge d'instruction* now has the authority to request the cooperation of experts or network managers to help decrypt telecommunications messages that have been intercepted. The experts, network managers, etc., risk criminal sanctions if they attempt to refuse to cooperate.

¹⁷ "Gand: Yahoo! acquitté en appel de ne pas avoir transmis des données à la justice", *Le Vif L'Express*, 30 June 2010, available at <http://levif.rnews.be/fr/news/belga-generique/gand-yahoo-acquitte-en-appel-de-ne-pas-avoir-transmis-des-donnees-a-la-justice/article-1194765233838.htm>.

¹⁸ Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, available at http://www.cass.be/cgi_loi/legislation.pl.

¹⁹ "Écoutes: une pratique décevante et flamande ! Le résultat judiciaire des écoutes téléphoniques est médiocre. La Chambre va modifier la donne", *Le Soir*, 12 December 1997, available at <http://www.lesoir.be>.

²⁰ The increase in wiretaps is partly due to the higher number of types of communications that the police are now able to intercept, from regular landline telephones, to mobile phones, SMS messages, facsimiles, satellite communications, emails, chat sessions, etc. Filip Verhoest, "'Meest geavanceerde' telefoontapkamer van Europa in gebruik genomen. Boeven af luisteren in stereo," 13 May 2003, *De Standaard*; see also Ricardo Gutiérrez, "La Belgique se dote de grandes oreilles," *Le Soir*, 12 May 2003, available at http://www.lesoir.be/articles/a_03E4C3.asp.

²¹ Chapitre 17, Loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, 19 December 1997, available at http://www.cass.be/cgi_loi/legislation.pl.

²² Loi du 10 juin 1998 (adding Art. 88bis, 90ter et seq. to the Code of Criminal Procedure (Code d'instruction criminelle)), modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, 10 June 1998, available at http://www.cass.be/cgi_loi/legislation.pl ; see "Le GSM en toute sécurité ? Pas sûr", *Le Soir*, 20 February 1998, available at <http://www.lesoir.be>.

Almost unnoticed, a law enacted in December 2001 bans anonymity for subscribers and users of telecommunications network operators and service providers, although the application of the law is subject to a proportionality requirement. A royal decree may prohibit the exploitation of telecommunications services if they render it impossible to identify the caller or make it otherwise difficult to track, monitor, wiretap, or record communications. With this new rule, the government can now prohibit any telecommunications service that hinders the application of wiretapping laws.²³

In 2003, a new royal decree was enacted to implement the 10 June 1998 Law to provide more details about the practical and technical measures that telecommunications network and service providers have to comply with in order to cooperate with law enforcement authorities.²⁴

The Electronic Communications Act also requires telecommunications network operators and service providers to record and store traffic and identification data of their end users for various law enforcement purposes.²⁵ A recent Act covering the data-gathering methods of intelligence services²⁶ has enabled those services to access and use this data for carrying out their mission (Art. 126 of the Electronic Communications Act). The data should be stored for a minimum period of 12 months and a maximum of 36 months.. The

²³ The wording of the law is so vague that a decree might prohibit any kind of anonymisation software and the use of proxies by ISPs, since they all make the identification or tracking of communications "difficult," Etienne Wéry, "Surfer anonymement devient illégal en Belgique", 18 March 2002 <http://www.droit-technologie.org/actuality-527/surfer-anonymement-devient-illegal-en-belgique.html>.

²⁴ Arrêté royal du 9 janvier 2003 portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du Code d'instruction criminelle ainsi que de l'article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, available at http://www.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=2003-02-10&numac=2003009111. For more information, see generally Patrick Van Eecke & Jos Dumortier, *Elektronische Handel* (Die Keure, Brugge 2003).

²⁵ Such as the pursuit and repression of criminal offences, criminal investigations, the fight against malevolent calls to emergency services, and investigations carried out by the Telecommunication Mediation Service in cases related to malevolent uses of electronic communication networks or services.

²⁶ Act of 4 February 2010 (Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité), *Moniteur belge* (Belgian State Gazette), 10 March 2010.

Belgian police are officially in favour of a three-year general retention policy.²⁷ However, the implementing royal decree has not been approved yet, despite the obligation for Belgium to transpose the Data Retention Directive by June 2009. First, the Commission issued a negative opinion on the text. The text was then modified accordingly by the government, after which the Commission issued a second, favourable, opinion (Advice n° 20/2009). The approval of the Commission is, however, subject to the introduction of additional safeguards such as limiting the maximum retention period to 12 months, deleting the data at the expiration of the retention period, and defining the concept of "exceptional circumstances". The government has modified the text again but the decree is still pending approval.

In 2009, the number of legal wiretapping increased by 20 percent (from 4,386 to 5,265 requests granted) compared to the previous year as reported by the Ministry of Justice.²⁸

National security legislation

In 2005, the Commission issued an opinion about a draft bill (*avant-projet de loi*) regarding "Threat Analysis" (Opinion n° 8/2005). The purpose of the bill is to improve the gathering, use, and analysis of information useful for assessing terrorist and extremist threats likely to harm national security, Belgian assets, or the safety of Belgian citizens abroad. To this end, the bill creates a new institution, the Coordination Agency for the Analysis of Threat (*Organe de coordination pour l'analyse de la menace*, or OCAM). Its job is to coordinate the collection of that information from various security and intelligence government agencies, and evaluate it. The Commission emphasises that this new type of data collection and analysis by law enforcement is highly sensitive due to the grounds on which it is justified (likelihood and probability) and because it operates unbeknownst to the persons concerned. Although it welcomes the government's project because it provides at least a legal basis for this new data processing, the Commission has reservations about the project's compliance with the provisions of the Law on Protection of Personal Data. In this regard, the Commission recommends that the language of the

²⁷ The European Commission made strong critiques of the law before its enactment. However, most of its critiques were not addressed, and most of them rejected without adequate motivation. Some of the European Commission's critiques mentioned that the law was too vague and could not be considered a "law" pursuant to current case law of the European Court of Human Rights (ECHR). The European institution also specified that the law, by not restricting the strictures within which the government has to implement data retention measures, is too vague and gives the government carte blanche to act in a discretionary fashion. According to the European Commission, the data retention provision of the Belgian law is also disproportionate with respect to the Court of Justice of the European Community's case law. One has to note that, even though the new EU Directive on Privacy and Electronic Communications allows EU Member States to allow data retention for a reasonable period, the Belgian law, as it is now written, could be considered in violation of current ECHR's case law. For more information, see European Commission, Opinion regarding Belgian bill on computer crime ("Notification 2000/151/B – Projet de loi relatif à la criminalité informatique – Emission d'un avis circonstancié au sens de l'article 9, paragraphe 2 de la Directive 98/34/CE du 22 juin 1998 – Emission d'observations au sens de l'article 8, paragraphe 2 de la directive 98/34/CE"), June 2000, appended to the Parliamentary report of the Justice Commission, Chamber of Representatives of the Belgian Parliament, 19 October 2000, DOC 50 0213/011.

²⁸ "Les écoutes téléphoniques en hausse de 20%", *La Libre*, 11 May 2010, available at <http://www.lalibre.be/actu/belgique/article/582071/les-ecoutes-telephoniques-en-hausse-de-20.html>.

bill be modified so that it specifies more detail (rather than only for "threat analysis") about the purposes for which personal data will be transferred between partner security and police agencies and the OCAM; the bill should determine the criteria to be used to decide whether to proceed with this transfer and better implement the security safeguards surrounding the processing of data; and the bill should also establish guarantees to protect international data transfers among foreign authorities.²⁹ The bill became law in July 2006³⁰ and entered into force on 1st December 2006.

Data retention

The Electronic Communications Act currently mandates that telecommunications network operators and service providers store traffic and identification data of their end users for various law enforcement purposes for between 12 and 36 months, including allowing intelligence services to access and gather that type of data in order to carry out their mission.³¹ The implementing royal decree has not been approved yet, despite the June 2009 deadline by which Belgium was required to transpose the EU Data Retention Directive. The Commission made approval of the Decree subject to the introduction of additional safeguards such as limiting the maximum retention period to 12 months, deleting the data at the end of that period, defining the concept of "exceptional circumstances", and Parliament's completing its assessment of the draft bill and draft royal decree.³² The Belgium ISP Association stated that a period of six months would be enough and asked the government to support the costs for a longer period, saying that failing to do so would raise subscription costs for their customers.³³ The Decree³⁴ is still awaiting approval.³⁵

²⁹ *Id.*

³⁰ Act of 10 July 2006 concerning threat analysis, *Moniteur belge* (Belgian State Gazette), 20 July 2006. The Act has been completed by a royal decree approved on 28 November 2006, *Moniteur belge* (Belgian State Gazette), 1st December 2006.

³¹ Act of 4 February 2010 (Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité), *Moniteur belge* (Belgian State Gazette), 10 March 2010.

³² The Commission also claimed that a public report needs to be made public each year, in order to assess if data retention is necessary and in what conditions it had been used, and commented on the text itself to clarify the "exceptional circumstances" when the data can be kept more than 24 months. See Opinion n° 20/2009 of 1st July 2009, demande d'avis relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012), available in French at http://www.privacycommission.be/fr/docs/Commission/2009/avis_20_2009.pdf.

³³ EDRi-gram, "Belgium: Minister of Justice Wants 2 Years of Data Retention", 26 August 2009 <http://www.edri.org/edri-gram/number7.16/belgium-data-retention>.

³⁴ Draft Law on Data Retention of 27 August 2009, available in French and Flemish at http://bewaarjeprievacy.be/sites/bewaarjeprievacy.be/files/20090827_MvT__Voorontwerp_van_Wet.pdf.

³⁵ Maartje De Schutter, "Update on the Belgian Transposition of the Data Retention Directive", EDRi-gram, No. 8.3, 10 February 2010, <http://www.edri.org/edri-gram/number8.3/belgium-data-retention-draft-law>.

National databases for law enforcement and security purposes

In the last few years, several cities and municipalities have authorised private companies to collect parking fines for vehicles parked in the street. Before then, only the police had the authority to collect those fines. In order to identify vehicle owners, the private companies required access to a central database that matches licence plates with car owners, access that the courts have considered illegal in several cases. The Constitutional Court voided an attempt by the federal legislator to provide a valid legal basis, after which the Flemish legislator introduced new draft legislation.³⁶

A new law dated 19 May 2010 created a reference database for vehicles³⁷ that indicates which organisation maintains the vehicles' data. The new legislation guarantees the traceability of vehicles on Belgian territory. Its stated objectives include: the development of a mobility plan; the investigation, prosecution, and execution of criminal penalties; the imposition of taxes and indemnities relating both to the registration and to the use, parking, and seizure of vehicles, technical control, and emergency help. In all, 29 reasons are listed.

National and international data disclosure agreements

Alerted by a complaint filed by Privacy International alleging the secret disclosure of millions of records of European citizens undertaken without regard to legal process under data protection law, the Commission began an investigation into the SWIFT case.³⁸ SWIFT is a multinational service provider in the financial sector and its headquarters are established in La Hulpe, Belgium.³⁹ At the request of the US Department of the Treasury, SWIFT systematically transmitted information concerning the financial transactions of millions of European bank clients. It appeared that the US Department of the Treasury periodically addressed warrants to SWIFT in the US. In its opinion of 27 September 2006, the Commission expressed astonishment about the export of information about Belgian citizens to the US and its revelation to the US authorities each time an individual performs an international payment transaction.⁴⁰ The Commission stated that these practices violate basic provisions of Belgian and European data protection legislation.

³⁶ See Constitutional Court n° 59/2010, 27 May 2010. See also Opinion n° 37/2008 of 29 November 2008 relating to the previous draft legislation of the Privacy Commission.

³⁷ Law of 19 May 2010 establishing a reference database for vehicles, *Moniteur belge* (Belgian State Gazette), 28 June 2010 (2nd ed.).

³⁸ Privacy International, "PI Launches Campaign to Suspend Unlawful Activities of Finance Giant", 28 June 2006 [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-538985](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-538985).

³⁹ <http://www.swift.com>.

⁴⁰ Decision Nr. 37/2006, available in French and Dutch at www.privacycommission.be. See also Privacy International, "Belgian Prime Minister Condemns SWIFT Data Transfers to US as 'Illegal'", 28 September 2006 <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-543789>.

This opinion was later confirmed by an opinion of the Article 29 Working Party.⁴¹ This incident also led the European Parliament to encourage the European Central Bank (ECB) to state its plans for protecting the privacy of wire transfers. In reply, the ECB said that it was not governed by EU law on the protection of personal data (94/46/EC), but by Regulation (EC) No. 45/2001 on the processing of personal data inside EU entities.⁴²

In November 2006, the Commission received a letter from the Belgian Prime Minister requesting advice about a possible agreement with the US covering the transfer of SWIFT data to the US Department of the Treasury. In its second opinion (n° 47/2006), the Commission reminded the Belgian government of the essential principles with regard to transfers of personal data between Europe and the US and suggested a series of possible actions. In June 2007, the Council of Europe and the US reached an agreement on the transfer of personal financial information from SWIFT to the US.⁴³ The agreement stipulates that the US will only obtain information for terrorism investigations; the US will periodically review the information received and delete any unnecessary information from its system; and no information will be kept by the US for longer than five years.⁴⁴ The Commission issued another decision about SWIFT in December 2008⁴⁵ in which it determined that the company complied with Belgian data protection laws and operated as a delegate ("*délégué de fait*") for the financial community.⁴⁶ The Privacy Commission considered that it was the controller who should make sure that adequate safeguards are installed before transferring the data. The Privacy Commission gave credit to SWIFT's attitude, in that it had entered into negotiations with the US government in order to provide safeguards with regard to the quality of data processing. These safeguards included control mechanisms (designation of control officers from SWIFT), limitations on accessed data, the banning of "fishing expeditions", and limitations on further use of

⁴¹ Opinion of 22 November 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

⁴² Reply of European Central Bank, January 30, 2007, available at http://www.europarl.europa.eu/comparl/econ/questions_ecb/econ_january.pdf.

⁴³ Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 28 June 2007, available at <http://www.epic.org/privacy/pdf/swift-agmt-2007.pdf>.

⁴⁴ *Id.*

⁴⁵ Décision, "Contrôle et procédure de recommandation initiés à l'égard de la société SWIFT scrl", 9 December 2008, available at <http://www.privacycommission.be/fr/static/pdf/cbpl-documents/swift---projet-de-d-cision-modifications-09-12-200.pdf>.

⁴⁶ The decision finds in first instance that it is the financial community and the banks that are liable for compliance with most data protection rules. "Belgium Privacy Commission Publishes Decision on 'SWIFT Case,'" *supra*. The Privacy Commission recalled that whereas the transfer of personal data from SWIFT's EU-based to US-based offices could benefit from the certification of SWIFT under the Safe Harbor framework, this regime could not apply to the transfer of personal data to US law enforcement authorities for national security purposes since the transfer fell outside the scope of application of the Data Protection Directive (95/46/EC). In this specific case, the Belgian Privacy Act remained, however, applicable to data processing for national security purposes.

such data by US authorities for the purposes of combating terrorism. The Commission considered that SWIFT had acted diligently, and now points to it as a reference for further similar cases.⁴⁷ It recommends that companies contact the specific Contact Group established between the US and EU authorities to deal with difficult cases.

Cybercrime

In November 2000, the Belgian Parliament enacted a Computer Crime Law.⁴⁸ The law creates four new crimes: computer forgery ("*faux en informatique*"), computer fraud ("*fraude informatique*"), hacking, and sabotage of computer data ("*sabotage de données informatiques*"). Recent case law tends to temper the harshness of some of the provisions of the new law.⁴⁹

In December 1999, the Commission issued an opinion on the Computer Crime Bill in which it raised serious concerns about its potential negative impact on the protection of privacy. It recommended certain amendments to the Bill including the establishment of a "police monitoring system", which would report back to the Commission, and a three-year review provision.⁵⁰ These suggestions were not included in the law, and the data retention provision even goes against the Commission's official opinion. However, the law makes it mandatory to get the Privacy Commission's opinion before any royal decree is enacted on the issue of data retention.

In March 2009, Yahoo! was fined for not disclosing the personal data of individuals involved in a cybercrime investigation.⁵¹ A Belgian court rejected Yahoo!'s argument that it was inappropriate for investigators to request the disclosure of personal data from a commercial entity.⁵² Yahoo! argued further that if the Belgian authorities had contacted the United States government first, as required by the treaty between Belgium and the United States, Yahoo! would not have objected to the order for Yahoo! to release the information.⁵³ The Belgian court held that Yahoo!'s business operations in Belgium

⁴⁷ Fanny Coudert & Geert Somers, International Transfers of Personal Data – Treatment of Personal Data Transfers in Europe – Belgium, *International Privacy Guide*, Vol. I, West - Thomson Reuters, November 2009, at 88-106.

⁴⁸ Loi du 28 novembre 2000 relative à la criminalité informatique, *Moniteur belge* (Belgian State Gazette), 3rd February 2001, available at http://www.cass.be/cgi_loi/legislation.pl.

⁴⁹ See Jeoffrey Vigneron, "Pour la première fois, un juge belge applique la "nouvelle" loi sur la cybercriminalité", 26 January 2004 http://www.droit-technologie.org/1_2.asp?actu_id=881.

⁵⁰ Opinion n° 33/99 by the Belgian Privacy Commission (Commission de la protection de la vie privée), available in French at <http://www.privacy.fgov.be/> "><http://www.privacy.fgov.be/>.

⁵¹ EDRI-gram, No. 7.5, "Yahoo Penalised in Belgium for not Disclosing Personal Data," 11 March 2009 <http://www.edri.org/edri-gram/number7.5/belgium-decision>.

⁵² *Id.*

⁵³ *Id.*

required the company to adhere to Belgian laws.⁵⁴ Yahoo! appealed and was cleared by the Court of Appeals of Ghent. The Court found no basis under Belgian law to compel email service providers to turn over users' data.⁵⁵

Critical infrastructure

No update to report under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

Since 2003, the use of email for direct marketing purposes is prohibited without the prior, free, specific, and informed consent of the recipients in compliance with the EU Directive on Electronic Commerce,⁵⁶ transposed by the Law of March 11, 2003,⁵⁷ and with the EU Electronic Communications and Privacy Directive.⁵⁸ Further spam provisions were implemented by the royal decree of April 4, 2003.⁵⁹ The deadline for the implementation of the Directive expired on 31 October 2003, and subsequently the European Commission launched infringement proceedings against Belgium for failing to transpose the remaining provisions into national law. In April 2005, Belgium's failure to transpose the Directive was upheld in a judgment of the European Court of Justice. In June 2005, Belgium finally adopted its Law on Electronic Communications.⁶⁰ Belgium has now fully implemented the EU Directive on Privacy and Electronic Communications of 2002.⁶¹

⁵⁴ *Id.*

⁵⁵ "Gand: Yahoo! acquitté en appel de ne pas avoir transmis des données à la justice", *Le Vif L'Express*, 30 June 2010, available at <http://levif.rnews.be/fr/news/belga-generique/gand-yahoo-acquitte-en-appel-de-ne-pas-avoir-transmis-des-donnees-a-la-justice/article-1194765233838.htm>.

⁵⁶ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market, available at http://www.ebu.ch/CMSImages/en/leg_ref_ec_directive_e_commerce_080600_tcm6-4338.pdf.

⁵⁷ Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *Moniteur belge* (Belgian State Gazette), 17 March 2003, at 12960-12970, available at http://www.droit-technologie.org/3_1.asp?legislation_id=142.

⁵⁸ For more information, see generally Thibault Verbiest, "La loi belge enfin adoptée!", *Droit et Nouvelles Technologies*, 22 April 2003 http://www.droit-technologie.org/1_2.asp?actu_id=747 ; and Jos Dumortier & Mieke Loncke, "Ongevraagde Reclame langs Elektronische Post", 21 *Mediarecht, Telecommunicatie en Telematica*, at 43-74 (Mechelen 2003).

⁵⁹ Royal Decree of 4 April 2003 regulating advertising by electronic mail, *Moniteur belge* (Belgian State Gazette), 28 May 2003.

⁶⁰ Law of June 13, 2005 on electronic communications, *Moniteur belge* (Belgian State Gazette), 20 June 2005.

⁶¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002.

At end of 2000, IFPI Belgium, the recording industry trade association, started tracking people downloading and uploading music files from MP3 audio file-sharing Web sites such as Napster, Gnutella, and KaZaa. In a move that left many Belgian music fans outraged, IFPI entered into simple "gentlemen's agreements" with Internet service providers,⁶² outside any legal framework, to get the names and addresses of high-speed Internet connection subscribers in order to send them personalised letters threatening them with legal action if they did not stop engaging in file-sharing. In November 2001, the Privacy Commission released an initial opinion⁶³ severely condemning the way IFPI had behaved with respect to the protection of people's privacy and stating that IFPI had violated several Belgian and European telecommunications privacy and data protection laws.⁶⁴

In June 2007, the Belgian Society of Authors, Composers, and Publishers (SABAM) won a case against the ISP Scarlet Extended SA in which the court ruled that Scarlet would be required to use Audible Magic filtering technology to stop the spread of music on P2P networks.⁶⁵ Scarlet was given six months to comply with the order. The Court of First Instance of Brussels ruled that such filtering would not violate user privacy nor create a general expectation of network surveillance. Scarlet appealed the decision. The Court of Appeals of Brussels, aware of the impact of filtering on fundamental rights such as privacy, confidentiality of communications, and freedom of expression, as well as the societal impact of its decision, decided to ask the European Court of Justice a few prejudicial questions before rendering its judgement. These questions bear upon whether the Copyright directives, read together with the E-commerce Directive (which refers to the principle of net neutrality), the Data Protection and e-Privacy and Electronic Communications directives, and Articles 8 (privacy) and 10 (freedom of expression) of the European Convention of Human Rights, would allow a national judge to order an ISP to implement "in abstracto," for preventive purposes, without time limit, and at the ISP's cost, a system that would filter all electronic communications to block the exchange of files protected by copyright (music, movies, or audiovisual content).⁶⁶ If the European

⁶² Olivier Van Vaerenbergh, "L'IFPI poursuit, mais la justice renâcle – Napster: plaintes en Belgique," *Le Soir*, 16 February 2000, available at <http://www.lesoir.be>.

⁶³ Avis No. 44/2001 of 12 November 2001, Avis d'initiative concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, available at <http://www.privacy.fgov.be>. For comments, see Etienne Wéry, "La Commission vie privée n'aime pas les manières de l'IFPI de traquer les pirates sur l'internet", 17 December 2001 http://www.droit-technologie.org/1_2_1.asp?actu_id=497.

⁶⁴ The Commission de protection de la vie privée found that IFPI had violated Belgian data protection law of 8 December 1992, Belgian telecommunications privacy laws, and EU Directive 2000/31/EC on electronic commerce. See Avis No. 44/2001, *supra*.

⁶⁵ *SABAM v. SA Scarlet* (formerly Tiscali), Tribunal de Première Instance de Bruxelles, 29 June 2007, available at: http://cedriclaurant.files.wordpress.com/2010/12/tpi_bruelles-070629.pdf.

⁶⁶ *SA Scarlet Extended v. SABAM*, Cour d'Appel de Bruxelles, 28 January 2010, No. RG 2007/AR/2424, available at http://cedriclaurant.files.wordpress.com/2010/12/cour_appel_bruelles-100128.pdf.

Court of Justice answered affirmatively, the Brussels Court intended to then ask whether the national judge should apply the principle of proportionality when assessing the efficiency and the deterrent effect of the measure. Whereas SABAM initially tried to use the ruling of the Court of First Instance to convince other ISPs to follow suit,⁶⁷ it has now changed strategy and is pushing for the adoption of a new piece of legislation similar to the French "Hadopi"⁶⁸ law⁶⁹ that would legitimise Internet filtering for copyright enforcement purposes.⁷⁰

Cybersecurity

The Commission has adopted guidelines to help organisations comply with their security obligations under the Law on Protection of Personal Data of 1992 (Opinion n° 48/2003). The concrete implementation of these standards, however, is left to the controller, who carries out this task on the basis of the specific needs of the company, taking into account the following aspects: the nature of the personal data processed and of the data processing; the requirements in terms of confidentiality, integrity, and availability; the specific legal requirements; the size of the entity (including the number and profile(s) of persons likely to access the data); the significance and complexity of the information systems, computer systems, and applications involved; the openness of the entity and the possibility of accessing the data from the outside; and the risks involved for the entity and the persons.⁷¹ When part of the data processing is sub-contracted, the same security obligations as those the controller's entity must meet must be included in the contract.

The standard security measures put forward by the Privacy Commission include the drafting of a security policy, the appointment of a security officer, the implementation of organisational and physical security measures, the security of networks and logical access, the logging, tracking, and monitoring of access, the follow-up of security measures, the implementation of adequate incident response and business continuity schemes, and the keeping of complete and up-to-date records on data security.⁷²

⁶⁷ Nate Anderson, "Belgian ISP must filter P2P music; files appeal," 23 July 2007 <http://arstechnica.com/news.ars/post/20070723-belgian-isp-must-filter-p2p-music-files-appeal.html>.

⁶⁸ Acronym of "Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet".

⁶⁹ Loi ("Hadopi") n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n° 0135 of 13 June 2009, at 9666, available in French at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&fastPos=3&fastReqId=1896908772&categorieLien=id&oldAction=echTexte> ; available in English at http://www.laquadrature.net/wiki/HADOPI_full_translation.

⁷⁰ Etienne Wery & Thibault Verbiest, "Que faire du piratage musical ? La Belgique rêve de "son" Hadopi," *Droit et Technologies*, 1st February 2010 <http://www.droit-technologie.org/actuality-1297/que-faire-du-piratage-musical-la-belgique-reve-de-son-hadopi.html>.

⁷¹ Fanny Coudert & Geert Somers, International Transfers of Personal Data – Treatment of Personal Data Transfers in Europe – Belgium, *International Privacy Guide*, Vol. I, West – Thomson Reuters, November 2009, at 88-106.

⁷² *Ibid.*

Online behavioural marketing and search engine privacy

In September 2007, the Commission issued an opinion on profiling practices made possible by interactive TV, which includes not only on-demand TV services, but also provides access to e-government, gaming, email applications, etc. (Opinion n° 29/2007).

In February 2007, following a lawsuit brought by Copiepresse (the Belgian newspaper association) on 22 September 2006, Google was ordered⁷³ to remove Belgian newspaper content from its search engine results and it is no longer allowed to reference to articles, pictures, or drawings.⁷⁴ In July 2007, the Court of First Instance of Brussels ordered a Belgian ISP to implement technical measures in order to prohibit its users from illegally downloading music files.⁷⁵ The appellate decision is pending, however, until the European Court of Justice decides upon its interpretation of the Copyright Directive in light of the E-Commerce, Data Protection, and e-Privacy and Electronic Communications directives, as well as Articles 8 and 10 of the ECHR. In July 2008, Copiepresse initiated another complaint against the European Commission (EC) claiming copyright infringement through the "NewsBrief" and "NewsExplorer" aggregation services.⁷⁶ The Brussels Court, however, found that only institutions with a Europe-wide jurisdiction would have the authority to deal with the matter, and so the Court could not rule on whether the European Commission had infringed Belgian copyright rules.⁷⁷

Online social networks and virtual communities

Nothing to report under this section.

Online youth safety

Nothing to report under this section.

⁷³ *Google Inc. v. Copiepresse SCRL*, High Court of Brussels (Tribunal de Première Instance de Bruxelles) of 13 February 2007, No. 06/10.928/C, available at http://cedriclaurant.files.wordpress.com/2010/12/copiepresse_google-070213.pdf.

⁷⁴ EDRI-gram, No. 5.13, "Belgium Court Backs Decision against Google", February 2007 <http://www.edri.org/edriagram/number5.3/google-belgium>. See generally Philippe Laurent, "Brussels High Court Confirms Google News' Ban – *Copiepresse SCRL v. Google Inc.* - Prohibitory Injunction/Stop Order of the President of the High Court of Brussels, 13 February 2007 [opposition procedure against the first default stop order by the same President]", *Computer Law & Security Report* 23 (2007) 290-293, also available at <http://www.crid.be/pdf/public/5512.pdf>.

⁷⁵ EDRI-gram, No. 5.14, "Belgium ISP Ordered by the Court to Filter Illicit Content", July 2007, <http://www.edri.org/edriagram/number5.14/belgium-isp>.

⁷⁶ EDRI-gram, No. 5.14,, "Copiepresse Attacks EC for Copyright Infringement, but Gets Dismissed", July 2008 <http://www.edri.org/edriagram/number6.14/copiepress-european-commission>.

⁷⁷ Civ. Bruxelles (cess.), 2nd October 2008, R.G. n° 2008/2443/A.

TERRITORIAL PRIVACY

Video surveillance

A new law regulates the use of camera surveillance. Enacted on 21 March 2007, it came into force, after a transition period, on 10 June 2010. Several proposals to modify the law have already been introduced,⁷⁸ and modifications were adopted through the Law of 12 November 2009.⁷⁹ These modifications aim at regulating police use of mobile cameras.

Location privacy (gps, mobile phones, location based services, etc.)

Nothing to report under this section.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

Belgium began a test programme in May 2004 that made it the second country in the world (after Malaysia) to issue passports with an embedded computer chip designed to store personal information.⁸⁰ The government began issuing these RFID⁸¹ passports to the public on 30 January 2005. Passports issued since August 2007 are in full compliance with the European, US, and ICAO⁸² standards and recommendations for biometric-based e-passports.⁸³ The RFID chip is currently used to store basic information, such as name, date, and place of birth, passport number, date, and place of issuance, digital photo, and signature. It also supports the ability to store fingerprints, an iris scan, and other biometrics.⁸⁴ Although the Belgian passport received "the world's most secure passport"

⁷⁸ See proposal approved in the Senate in June 2009, and proposal n° 2076/004 thereafter introduced in the Chamber.

⁷⁹ Law of 12 November 2009 modifying the law of 21 March 2007 for the position and the use of surveillance cameras, *Moniteur belge* (Belgian State Gazette), 18 December 2009 (and erratum 26 March 2010).

⁸⁰ BBC Worldwide Monitoring, "Passport Acquires Chip", 19 May 2004.

⁸¹ Radio frequency identification.

⁸² International Civil Aviation Organisation.

⁸³ Rudi Veestraeten, Oversight Hearing on "October 2005 Statutory Deadline for Visa Waiver Program Countries to Produce Security Passports: Why It Matters to Homeland Security", Committee on the Judiciary, US House of Representatives, 20 April 2005, available at http://commdocs.house.gov/committees/judiciary/hju20711.000/hju20711_0f.htm.

⁸⁴ *Id.*

award from Interpol in 2003,⁸⁵ now that it is equipped with an RFID chip it may present new privacy and security risks, including the unauthorised reading of its data.⁸⁶

In January 2010, the Privacy Commission issued an opinion about the European and US agreement concerning Passenger Name Records (PNRs).⁸⁷ The Commission regretted that its opinion was not requested until two years after the 2007 PNR agreement, even though the Council of the EU adopted the proposal on 23 July 2007.⁸⁸ The Commission retains the right to make a further analysis of the execution of the PNR agreement, and requires that it be notified in case of any modification.

National id & smart cards

Belgium was the first European country to roll out smart ID cards supporting digital signatures at a national level.⁸⁹ The Belgian electronic identity ("eID") card project, originally called "BELPIC" (which stood for "Belgian Personal Identity Card"), started in 2000. In 2001, the Belgian Council of Ministers (Conseil des ministres) decided to proceed with the further development of an electronic identity card for all Belgian citizens.⁹⁰ In February 2003, the Belgian Federal Parliament approved the issuance and testing of the proposed eID cards in 11 municipalities (communes). After a positive evaluation of this pilot phase, the federal government decided to roll out eID cards to the

⁸⁵ *Id.*

⁸⁶ Jim Waldo, Alan Ramos, Weina Scott, William Scott, Doug Lloyd & Katherine O'Leary, "A Threat Analysis of RFID Passports – Do RFID Passports Make Us Vulnerable to Identity Theft?", ACM Queue, 1 October 2009. See also Ari Juels, David Molnar & David Wagner, "Security and Privacy Issues in E-Passports," *IEEE SecureComm 2005*, available at <http://www.cs.berkeley.edu/~dmolnar/papers/RFID-passports.pdf>.

⁸⁷ Avis n° 01/2010 du 13 janvier 2010, avis d'initiative relatif au projet de loi portant assentiment à l'Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au Ministère américain de la sécurité intérieure (DHS) (Accord PNR 2007), fait à Bruxelles le 23 juillet 2007 et à Washington le 26 juillet 2007, available at http://www.privacycommission.be/fr/docs/Commission/2010/avis_01_2010.pdf.

⁸⁸ Agreement between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), 23 July 2007, available at <http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf>.

⁸⁹ "Belgium Plans Digital ID Cards," "Belgium Plans Digital ID Cards," BBC News Online, 4 October 2003 <http://news.bbc.co.uk/2/hi/technology/2295433.stm> and TB6/SINCE Interoperability Group, Open Smart Cards Infrastructure for Europe, eESC Common Specifications v2; Volume – Part 3, 18 February 2004, available at http://www.eurosmart.com/Update/Download/February04/SINCE_survey.pdf.

⁹⁰ "Documents d'identité" [http://www.elections.fgov.be/index.php?id=2589&no_cache=1&L=0&no_cache=1&tx_irfaq_pi1\[cat\]=123](http://www.elections.fgov.be/index.php?id=2589&no_cache=1&L=0&no_cache=1&tx_irfaq_pi1[cat]=123).

rest of the Belgian population.⁹¹ The nationwide roll-out started in September 2004. Since September 2005, practically all newly issued ID cards have been eID cards. By the end of 2009, all Belgian citizens had been issued with the new card.

With its eID card, Belgium has created a means by which cardholders can identify and authenticate themselves, as well as provide a qualified electronic signature within the meaning of Directive 1999/93/EC.⁹² The Belgian eID card is a classic smartcard integrating traditional public key technologies. The card's chip contains a total of five X.509v3 certificates, two of which are tied specifically to the citizen/cardholder.⁹³ The first of these certificates, also referred to as the "authentication certificate," allows cardholders to authenticate themselves online. The second certificate, also known as the "non-repudiation certificate," can be used to produce qualified electronic signatures. The use of both functionalities is protected with a single personal identification number (PIN) that consists of four to six digits that citizens can change themselves.⁹⁴ Both certificates contain the cardholder's full name and National Registry number.⁹⁵ One should note that this number acts as a single unique identifier within the Belgian government: save for a limited number of exceptions, the National Registry number is the identifier that is used by all governmental agencies to identify any citizen, regardless of context or sector.

In addition to supporting remote authentication and electronic signatures, the Belgian eID card contains an "identity file" and an "address file". The identity file holds, *inter alia*, the citizen's name, first names, gender, national registry number, and nationality, as well

⁹¹ Arrêté royal du 1er septembre 2004 portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique, *Moniteur belge* (Belgian State Gazette), 15 September 2004, at 67.527, available at http://www.droit-technologie.org/redirect.asp?type=legislation&legis_id=199&url=legislations/AR_usage_generalise_CI_electronique_010904.pdf. See also "La Belgique adopte la carte d'identité électronique," *NetEconomie.com*, 7 September 2004 <http://www.neteco.com/49483-la-belgique-adopte-la-carte-d-identite-electronique.html>; Etienne Wéry & Sébastien Mélardy, "La Belgique généralise la carte d'identité pour l'ensemble de la population," 21 September 2004 <http://www.droit-technologie.org/actuality-814/la-belgique-generalise-la-carte-d-identite-electronique-pour-l-ensembl.html>.

⁹² See Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures, O.J., L 13, 19 January 2000, at 12. (Brendan Van Alsenoy & Danny De Cock, "Due Processing of Personal Data in eGovernment? A Case Study of the Belgian Electronic Identity Card", *Datenschutz und Datensicherheit*, March 2008, at 178, available at <http://www.fidis.net/fileadmin/fidis/publications/2008/DuD-2008-03-Due-processing-of-personal-data-in-eGovernment.pdf>).

⁹³ Danny De Cock, Koen Simoens & Bart Preneel, "Insights on Identity Documents Based on the Belgian Case Study", *Information Security Technical Report*, 2008, at 56.

⁹⁴ Brendan Van Alsenoy & Danny De Cock, *supra* at 178, and Danny De Cock, Koen Simoens & Bart Preneel, *supra*, at 56. The remaining three certificates can be used to check the validity of the address file, the identity file, as well as the two citizen certificates.

⁹⁵ This number can be characterised as a "meaningful" identifier because two of its three components refer to personal attributes of the citizen in question: the first six digits refer to the citizen's date of birth, the following three refer to a sequence number (whereby odd values refer to males, even to females); the last two digits form a checksum to detect typing errors. Art. 1-3 of the Royal Decree of 3 April 1984, *Moniteur belge* (Belgian State Gazette), 21 April 1984. See also Brendan Van Alsenoy & Danny De Cock, *supra*, at 179.

as the date and location of birth. The address file contains the citizen's last known official address.⁹⁶ Accessing the content of these files remotely (e.g., in the context of an online transaction) requires both the physical presence of the eID card and specific software on the citizen's computer. When the card is accessed locally, both files are freely accessible (i.e. publicly readable) using standard software tools provided by the government.

Belgium currently issues three types of electronic identity cards: eID cards for Belgian citizens of age 12 or older, "Kids-ID cards", and foreigners' eID cards. A Kids-ID card is issued upon request by the parent or legal guardian of a child younger than 12.⁹⁷ The Kids-ID was introduced to improve the security of identity and travel documents (as compared to paper certificates). A Kids-ID is valid for three years (a classic eID card is valid for five or ten years). Children older than six can use the Kids-ID to authenticate themselves, e.g. when accessing a chat Web site. The nationwide roll-out of the KidS-ID started on 16 March 2009, following the Ministerial Decree of 3 March 2009.⁹⁸ As of January 2010, all Belgian municipalities only issue Kids-IDs for Belgian citizens younger than age 12. The foreigner's eID card can be issued to any foreigner with a residence permit. Practically all features of the foreigners' eID cards are identical to those of the classic Belgian eID card. The only difference lies in the fact that the identity file of the foreigner's eID card indicates the nationality of the holder.⁹⁹

The introduction of the Belgian eID card triggered reactions from both the Belgian Privacy Commission and civil liberties organisations. The Commission expressed multiple concerns, *inter alia* the potential disclosure of the national number to entities that have not been authorised to process it (Opinion n° 19/2002); the inclusion of a digital picture that can be easily copied (Opinion n° 19/2002); the likelihood of excessive registration of the information stored on the eID card, both because it's likely that citizens will be asked increasingly often to present their eID card and because registration of the information stored on the card is easy enough to make it likely that registration will take place even when not strictly necessary (Opinion n° 8/2003); and access to the identity file by the private sector (Opinion n° 8/2003).

Other critics complained that the e-commerce identity of Internet users should not be linked to day-to-day authentication; that the integration of data has the potential to

⁹⁶ For a complete overview of information contained in the identity file of the Belgian electronic eID card see Danny De Cock, Koen Simoens & Bart Preneel, *supra*, at 56.

⁹⁷ The Royal Decree of 18 October 2006, *Moniteur belge* (Belgian State Gazette), 31 October 2006) sets the scene of the electronic identification document for children below the age of 12 years, and changes the Royal Decree of 10 December 1996 regarding identity documents and identity proofs for children below the age of 12 years. The most recent decree replaces for children the paper identity documents with their electronic equivalent.

⁹⁸ This ministerial decree was published in *Moniteur belge* (Belgian State Gazette), 11 March 2009.

⁹⁹ Children of foreigners younger than age 12 cannot be issued a Kids-ID card, even if their parent (or other legal guardian) has a Belgian residence permit. They can only be issued a paper-based identification document from the municipality in which they are registered.

damage users' integrity and rights, and that the fact that the Belgian government handed the operational aspects of the project over to a private company¹⁰⁰ jeopardises citizens' privacy rights.¹⁰¹

In 2009, the SNCB (Belgium's national railway company) introduced the ability to use the eID as a virtual train ticket¹⁰² by linking the citizen's National Registry number with the ticket number, despite users' privacy concerns.¹⁰³

Rfid

In 2009, the Commission for the Protection of Privacy (the Commission) issued an opinion clarifying the application of Data Protection Law to RFID systems processing personal data.¹⁰⁴

The Brussels public transportation company, the STIB (Société des Transports Intercommunaux de Bruxelles), launched the "MoBIB" card in 2008. The new card uses radio frequency identification technology and in the course of 2011 is scheduled to replace all magnetic cards currently in use. It is also expected to be adopted soon by other Belgian mass transit companies (SNCB, DeLijn, and TEC). RFID technology experts¹⁰⁵ and at least one human rights organisation, the Human Rights League (Ligue des droits de l'Homme), have criticised the way the MoBIB RFID system has been implemented, asserting that it violates the Data Protection Law, while the Commission has emphasised the importance of the compliance of public transportation companies using RFID systems with technical and security measures, rather than implementing a processing system that would allow tracking of their customers.¹⁰⁶ The critics assert that the MoBIB system violates Belgian data protection law: STIB customers have no option of travelling anonymously; MoBIB users have no opportunity to withhold consent to tracking; the technical and security measures used so far have proved inadequate; and there is a lack of

¹⁰⁰ Security firm Ubizen, acquired by Cybertrust and more recently by Verizon Business.

¹⁰¹ "Belgium Plans Digital ID Cards," *supra*.

¹⁰² <http://mobile.b-rail.be/en/Novelties/Use-your-Belgian-e-ID-as-ticket>.

¹⁰³ "Lancement de la campagne sur la carte d'identité électronique", *La Libre*, 22 April 2009 <http://www.lalibre.be/actu/belgique/article/497217/lancement-de-la-campagne-sur-la-carte-d-identite-electronique.html>.

¹⁰⁴ Commission de la protection de la vie privée (Commission for the Protection of Privacy), Avis d'initiative relatif à la RFID n° 27/2009 du 28 octobre 2009 (A/2009/003), 28 October 2009, available at http://www.dice.ucl.ac.be/~fstandae/mobib/CPVP_RFID_2009.pdf.

¹⁰⁵ François-Xavier Standaert <http://www.dice.ucl.ac.be/~fstandae/mobib/> [contains a list of the key documents about MoBIB and related legal and security considerations].

¹⁰⁶ Commission de la protection de la vie privée (Commission for the Protection of Privacy), Recommandation n° 01/2010 du 17 mars 2010 relative aux principes de base à respecter dans le cadre de l'utilisation de la télébilletique par les sociétés publiques de transport en commun (A-2010-003), 17 March 2010, available at http://www.dice.ucl.ac.be/~fstandae/mobib/CPVP_e-tickets_2010.pdf.

proportionality between the personal data collected and further processed, and the purposes for which they are used.¹⁰⁷ STIB's answer rejected all these arguments.¹⁰⁸

BODILY PRIVACY

No updates to report under this section.

WORKPLACE PRIVACY

After almost a year of negotiations, a national collective labour organisation of employers and employees' representatives (the Conseil national du travail) eventually agreed on common rules regulating electronic surveillance of workers' computers in the workplace. The collective labour agreement (called "Convention collective de travail" or CCT) entered into force on June 29, 2002 through a royal decree¹⁰⁹ and applies to all employers and employees in the country. It determines how to apply the existing and enforceable European and Belgian general data protection regulations to the specific setting of the workplace by ensuring the workers of fairness, information, and compliance with the basic data processing principles of proportionality, purpose specification, and transparency.¹¹⁰ In an earlier opinion on the same topic,¹¹¹ the Data Protection Authority had referred to general principles: the prohibition of the interception of telecommunications, proportionality and transparency, balance of interests, and limited storage of personal data. Another CCT was released in 1998 to regulate the surveillance

¹⁰⁷ François-Xavier Standaert, Franck Dumortier, François Koeune & Antoinette Rouvroy, "Carte MoBIB – Un bon exemple de mauvaise mise en œuvre", available at http://www.dice.ucl.ac.be/~fstandae/mobib/IEB_2010.pdf; Ligue des droits de l'Homme, "Carte MOBIB: ma vie privée ne voyage pas en commun", September 2010 http://www.liguedh.be/index.php?option=com_content&view=category&layout=blog&id=115&Itemid=288.

¹⁰⁸ STIB, "MOBIB respecte la vie privée" http://www.stib.be/corporate.html?l=fr&news_rid=/STIB-MIVB/INTERNET/ACTUS/2010-05/WEB_Article_1274963883674.xml.

¹⁰⁹ Arrêté royal rendant obligatoire la Convention Collective de Travail No. 81 du 26 avril 2002, conclue au sein du Conseil National du travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, *Moniteur belge* (Belgian State Gazette), at 29489-29501, available at <http://www.droit-technologie.org/legislation-109/arrete-royal-rendant-obligatoire-la-cct-sur-la-cybersurveillance-des-t.html>.

¹¹⁰ See Bertrand Gérardin, "La convention collective de travail relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données des communications électroniques en réseau du 26 avril 2002", 14 June 2002 http://www.droit-technologie.org/redirect.asp?type=dossier&dossier_id=77&url=dossiers/analyse_CCT81_260402.pdf.

¹¹¹ Privacy Commission (Commission de la protection de la vie privée), Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, opinion No. 10, 3rd April 2000, available at <http://www.privacy.fgov.be>.

of workers by video cameras.¹¹² The Commission also issued an opinion on the use of badges and on employee tracking by means of GPS systems. The Commissioner concluded that continual surveillance of employees is disproportionate and unnecessary, particularly the use of badges that collect both geographic identifiers and biometric identifiers.¹¹³

HEALTH & GENETIC PRIVACY

Health privacy

In August 2002, a new law was enacted that better protects patients' privacy rights by giving them, e.g., the right to be clearly informed about the state of their health, to consent to any medical interventions, and to have access to their medical files.¹¹⁴ There are also laws relating to consumer credit,¹¹⁵ social security,¹¹⁶ electoral rolls,¹¹⁷ the national ID number,¹¹⁸ professional secrets,¹¹⁹ and employee rights.¹²⁰

The Council of Ministers accepted the principle of electronic information exchange in health care in 2004. The actual development of the "eHealth-platform", however, only

¹¹² Convention Collective de Travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail, 16 June 1998, available at http://www.privacy.fgov.be/textes_normatifs/cct-68_FR.pdf. See generally on recent developments in workplace privacy, Olivier Rijckaert, "Surveillance des travailleurs: nouveaux procédés, multiples contraintes", in Orientations, "L'employeur et la vie privée du travailleur," n° spécial 35 ans, at 41 et seq. (2005), available at http://www.droit-technologie.org/redirect.asp?type=dossier&dossier_id=144&url=dossiers/Surveillance_Travailleurs_nouvelles_contraintes.pdf.

¹¹³ Ninth Annual Report of the Article 29 Working Party on Data Protection, June 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf.

¹¹⁴ See Loi du 22 août 2002 relative aux droits du patient (Law on Patient's Rights of 22 August 2002), available at http://www.cass.be/cgi_loi/legislation.pl; see also Dominique Mayerus & Pascal Staquet, *Actualité en détail*: "La loi du 22 août 2002 relative aux droits du patient", DroitBelge.Net, 8 October 2002 <http://www.droitbelge.be/actualites.asp?display=detail&id=81>.

¹¹⁵ Loi du 12 juin 1991 relative au crédit à la consommation, available at http://mineco.fgov.be/protection_consumer/Credit/law_credit_011.pdf; l'arrêté royal du 11 janvier 1993 modifiant l'arrêté royal du 20 novembre 1992 relatif à l'enregistrement par la Banque Nationale de Belgique des défauts de paiement en matière de crédit à la consommation, available at http://www.cass.be/cgi_loi/legislation.pl.

¹¹⁶ Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale. Modified by the loi du 29 avril 1996, available at http://www.privacy.fgov.be/textes_normatifs/loicarrefour.PDF.

¹¹⁷ Loi du 30 juillet 1991, available at <http://www.users.skynet.be/psetranger/moniteur.htm>.

¹¹⁸ Loi du 8 août 1993: le registre national, available at http://www.privacy.fgov.be/textes_normatifs/loiregistre.PDF.

¹¹⁹ Article 458 of the Penal Code.

¹²⁰ See Roger Blanpain, Employee Privacy Issues: Belgian Report, 17 Comp. Lab. L. 38, Fall 1995. Employers generally has no right to obtain medical information from their employees unless the information is absolutely necessary for the appropriate fulfillment of the employee's obligations under the employment contract.

came into existence with the federal Law of 21 August 2008. The eHealth-platform is described as "a secured electronic exchange platform where care providers, health care organisations, collective insurance organisations, government authorities, and patients may exchange information in confidence and in full respect of their privacy". Article 6 of the Law expressly states that it does not derogate from data protection legislation, the legislation relating to patients' rights, or the legal and regulatory provisions relating to medical practice. Use of the platform is not mandatory. The idea is for the platform to provide some basic services, such as encryption of data exchanges, a system of user and access management, the encoding and anonymisation of information, time stamping, and a reference directory. The latter indicates, once the patient's consent has been obtained, where what information, about which patient, is stored, so that the system does not need to store the medical records itself. The National Registry number, the identification number used by the Social Security administration, will be used to identify most patients.¹²¹ Every communication sent to or from the platform requires the Social Security and Health Committee's authorisation. A royal decree may determine which data shall be transmitted electronically by government entities for the execution of their tasks to the platform and which data they may receive.

A labour court of appeals confirmed that a victim of an accident at work had the right to access his medical file held by the physician controlling his labour capacity.¹²²

Genetic privacy

No developments to report under this section.

FINANCIAL PRIVACY

Bank secrecy is still the law in Belgium under the "Code des impôts sur les revenus 1992" but a 2009 bill named "Van Der Maelen-Mathot"¹²³ intends to give more access rights to financial investigators, including to personal banking information. In March 2010, the Privacy Commission issued an opinion¹²⁴ that included recommendations for improving the bill, especially clarifying the scope of investigation and the terminology used in the bill.

¹²¹ See also Privacy Commission (Commission de la protection de la vie privée), Opinion no. 14/2008, available at <http://www.privacycommission.be>.

¹²² Labour Court of Appeals, 5 March 2009, *Computerrecht* 2009/6, at 260.

¹²³ Proposition de loi du 16 octobre 2009 modifiant certaines dispositions du Code des impôts sur les revenus 1992 relatives à la levée du secret bancaire, introduite par messieurs Dirk Van Der Maelen et Alain Mathot, Doc. Parl. Chambre, DOC. 52, 2205/001.

¹²⁴ Privacy Commission (Commission de la protection de la vie privée), Opinion n° 12/2010 of 31 March 2010, Proposition de loi modifiant certaines dispositions du Code des impôts sur les revenus 1992 relatives à la levée du secret bancaire (A-2010-005), available at http://www.privacycommission.be/fr/docs/Commission/2010/avis_12_2010.pdf.

E-GOVERNMENT & PRIVACY

The Flemish community adopted a decree relating to the administrative electronic exchange of information that provides a legal framework for the organisation of e-government.¹²⁵ Its most essential features are the use of authentic sources and the single collection of information. A Flemish control authority will be established and issue authorisations so that public authorities can start exchanging information. Other provisions include the obligation to take organisational and technical security measures, maintain data accuracy, and appoint a security consultant under some circumstances.

Voting privacy

Voting is mandatory for those 18 years and older.¹²⁶ The laws regarding voting, enacted in 1919 and amended to include women in 1949, are strictly enforced.¹²⁷ Non-voting requires an acceptable explanation and may result in a fine, imprisonment, loss of civil rights, disenfranchisement, or a block on employment in the public sector.¹²⁸ Voter registration lists are publicly posted in polling locations on Election Day and may also be obtained for political campaign purposes.¹²⁹ Election administrators take an oath to maintain the secrecy of the ballots cast. Voters are guaranteed the right of secrecy of their vote.¹³⁰ In 1989, Belgium became one of the first countries to use electronic means of casting ballots in public elections.¹³¹ In 1991, experiments began with the use of electronic voting machines at polling locations.¹³² The Election Law was amended by the Act of April 11, 1994 to allow a "system of electronic voting" and was amended again on December 18, 1998 to allow "automated" voting.¹³³ The Federal Council of Ministers Rulings of June 20 and July 18, 1997 formally endorsed the adoption of electronic voting. By 1999, 40 percent of voters participating in Belgium's public elections used electronic

¹²⁵ Decree of the Flemish Community of 18 July 2008, *Moniteur belge* (Belgian State Gazette), 29 October 2008.

¹²⁶ CIA Country Fact Book Online, available at <https://www.cia.gov/library/publications/the-world-factbook/index.html>.

¹²⁷ International Institute for Democracy and Electoral Assistance, Report: Compulsory Voting, 11 February 2005, available at http://www.idea.int/vt/compulsory_voting.cfm.

¹²⁸ *Id.*

¹²⁹ European Commission, CyberVote Report, Contract number IST-1999-20338, Project: Cybervote, 1st June 2001, available at <http://www.eucybervote.org/MSI-WP6-D21-v1.0.pdf>.

¹³⁰ Article 55, Belgian Constitution, available at http://www.oefre.unibe.ch/law/icl/be00000_.html.

¹³¹ Basque Government, Home Office Department, Management of Electoral Processes and Documentation, Voto Electrónico, 5 April 2004, available at http://www.euskadi.net/botoelek/otros_paises/sim0_i.htm.

¹³² Strengthening Regional and Local Democracy in the European Union, Volume I, Belgium, February 2004, at 148, available at http://www.cor.eu.int/document/documents/cdr171_2004_vol1_etu_en.pdf.

¹³³ *Id.*

voting machines.¹³⁴ The direct recording electronic (DRE) system identified was used by 44 percent of voters in 2000. By 2003, an estimated 3 million votes were cast using electronic voting technology.¹³⁵ The expiration of the maintenance contract of the voting machines at the end of 2008, together with the recommendations of the OSCE to implement a ticketing system, pushed the Belgian State to look for a renewed e-voting system. A study was commissioned from a consortium of universities to assess the e-voting systems in place in other countries and suggest a new one for Belgium.¹³⁶ The consortium came back with two proposals: one for general elections based on ticketing, where a bar code or RFID chip would be printed on a paper ballot in order to facilitate recounts; and another to gather the votes cast by Belgians living abroad based on homomorphic encryption (Internet voting). Both systems ensure the anonymity of the ballots cast.

OPEN GOVERNMENT

The Constitution recognises that "everyone has the right to consult any administrative document and have a copy made, except in the cases and conditions stipulated by laws, decrees, or regional council decrees (i.e., the "rulings referred to in Article 134").¹³⁷ Freedom of information laws implement this constitutional right as well as the right of access to administrative documents on the federal,¹³⁸ regional,¹³⁹ community,¹⁴⁰ provincial, and municipal levels.¹⁴¹ The basic exemptions to the general rule of access are public security, the protection of fundamental rights, international interests, public order,

¹³⁴ *Id.*

¹³⁵ "Belgian National Elections on May 18, 2003 - Over 3.2 Million Belgians Voted Electronically," M2 Presswire, 23 May 2003.

¹³⁶ "BeVoting, Study of Electronic Voting System", Parts I and II, available at: <http://www.ibz.rn.fgov.be/index.php?id=1062>.

¹³⁷ Article 32, Constitution of Belgium, 1994 http://www.fed-parl.be/constitution_uk.html.

¹³⁸ Loi du 11 avril 1994 relative à la publicité de l'administration des actes des autorités administratives fédérales, *Moniteur belge*, 30 juin 1994, modifiée par la loi du 25 juin 1998 et la loi du 26 juin 2000. The Law allows individuals to request in writing for access to any document government authorities hold, including documents in judicial files. The Law also includes a right to have the document explained. Government agencies must respond immediately, or within 30 days if the request is delayed or rejected.

¹³⁹ Région flamande (Flemish Region), Décret relatif à la publicité de l'administration, 18 May 1999), *Moniteur belge* (Belgian State Gazette), 15 June 1999; Région wallonne (Walloon Region), Décret relatif à la publicité de l'administration dans les intercommunales wallonne, 7 March 2001, *Moniteur belge* (Belgian State Gazette), 20 March 2001; Région wallonne (Walloon Region), Décret relatif à la publicité de l'Administration, 30 March 1995, *Moniteur belge* (Belgian State Gazette), 28 June 1995, available at http://www.cass.be/cgi_loi/legislation.pl ">http://www.cass.be/cgi_loi/legislation.pl .

¹⁴⁰ Commission Communautaire Commune de Bruxelles-Capitale, Ordonnance relative à la publicité de l'administration, 26 June 1997; Commission communautaire française, Décret relatif à la publicité de l'administration, 11 July 1996, *Moniteur belge* (Belgian State Gazette), 27 August 1996.

¹⁴¹ Loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes, available at http://www.cass.be/cgi_loi/legislation.pl.

security or defence, confidentiality, and privacy. Each jurisdiction has a Commission of Access to Administrative Documents (Commission d'Accès aux Documents Administratifs, or CADA) that oversees the Act. Citizens can appeal refusals of information requests to the administrative agency, which in turn requests advice from the CADA. The CADA issues advisory opinions both on request and on its own initiative. Information seekers can then pursue a limited judicial appeal to the Counsel of State (Conseil d'Etat).¹⁴² At the federal level, each public authority is required to provide a description of its functions and organisation, and must have an information officer.¹⁴³ The Law on Protection of Personal Data gives individuals the right to access and correct files about themselves that public and private entities hold, and is enforced by the Commission for the Protection of Private Life. Access to administrative documents that contain personal information is regulated by the Law of April 11, 1994.

OTHER RECENT FACTUAL DEVELOPMENTS

Two months after the new data protection regime came into effect, the government announced that it had put in place an Internet Rights Observatory (Observatoire des droits de l'Internet)¹⁴⁴ to better assess and analyse the impact of the Internet on the economy and consumer protection. The Observatory aims, through its composition, to be an open forum for all Internet stakeholders, and will issue advisory opinions and annual reports, organise a dialogue between economic actors, and inform the public.¹⁴⁵ The Observatory has released reports on the protection of minors on the Internet,¹⁴⁶ e-commerce,¹⁴⁷ e-

¹⁴² David Banisar, The Freedominfo.org Global Survey: Freedom of Information and Access to Government Records around the World, May 2004, at 14, available at http://www.freedominfo.org/survey/global_survey2004.pdf.

¹⁴³ *Id.*

¹⁴⁴ <http://www.internet-observatory.be/>.

¹⁴⁵ Alain Jennotte, "Un Observatoire au chevet du Net," *Le Soir*, 1st December 2001, available at <http://www.lesoir.be>.

¹⁴⁶ Observatoire des Droits de l'Internet, The Protection of Minors on the Internet, Opinion No. 1, February 2003, available at <http://www.internet-observatory.be/>

¹⁴⁷ Observatoire des Droits de l'Internet, Pistes pour renforcer la confiance dans le commerce électronique / Betreffende denkplaatjes om het vertrouwen in de elektronische handel te versterken, Opinion No. 3 submitted to the Federal Minister of Economy, June 2004, available at <http://www.internet-observatory.be/>.

government,¹⁴⁸ Voice over IP,¹⁴⁹ the right of reply in the media,¹⁵⁰ and cyber-harassment.¹⁵¹

Since 1998, the Commission has been called upon several times to determine the legality of "blacklists", ranging from casinos' lists of cheaters to insurance companies' lists of bad debtors and bad risks. In 2002, the Commission was asked to assess whether publication on the Internet of a blacklist of renters by the National Association of Property Owners (Syndicat National des Propriétaires) was legal.¹⁵² In its opinion, the Data Protection Authority found the database illegal under the Data Protection Act, and stated that it required prior legislative action to authorise it – if it were to be authorised – and determine the conditions of access.¹⁵³ In 2005, the Commission was asked to deliver an opinion concerning the legality of blacklists in the private sector. The Commission recommended that they be regulated by law, especially where they are likely to violate a fundamental right or restrain access to an "essential service." In the latter case, the Commission should authorise the establishment of blacklists only upon prior approval. Where the lists process sensitive data (e.g., medical data), they should be regulated by a specific law and strictly follow the provisions of the Law on Protection of Personal Data.¹⁵⁴ In 2008, a legislative proposal on blacklists was introduced in the Parliament, on

¹⁴⁸ Observatoire des Droits de l'Internet, Facteurs de succès de l'e-gouvernement / Betreffende de succesfactoren van het e-government, Opinion No. 2, December 2003, available at <http://www.internet-observatory.be/>

¹⁴⁹ In its opinion, the Observatory examines the opportunities and challenges related to the development of VoIP services. It concludes that it is important right now to make clear choices about VoIP services and determine the applicable legislation, while avoiding the creation of too many regulatory obstacles to their development, in order to protect consumers and provide legal security. Observatoire des Droits de l'Internet, Opportunités et défis liés au développement des services Voice over IP / Over de kansen en de uitdagingen die gepaard gaan met de ontwikkeling van de Voice over IP-diensten, Opinion No. 4, May 2005, available at <http://www.internet-observatory.be/>.

¹⁵⁰ Observatoire des Droits de l'Internet, Opinion No. 5, Droit de réponse dans les médias / Recht van antwoord in de media, September 2006, available at <http://www.internet-observatory.be>. In this Opinion, the Observatory analyses the Belgian legal framework applicable to the right to reply. It concludes there is a need to simplify it, harmonise it, and broaden its scope of application to new types of media. It further recommends clarifying the field of competences of the competent bodies and the rules applicable to applicable law in case of conflict.

¹⁵¹ Observatoire des Droits de l'Internet, Opinion No.6, Cyberharcèlement / Cyberpesten: pesten in bits & bytes, February 2009, available (in French) at http://www.internet-observatory.be/internet_observatory/home_fr.htm, and in Dutch at http://www.internet-observatory.be/internet_observatory/home_nl.htm. In this Opinion, the Observatory formulates a series of recommendations directed to school staff such as teachers or inspectors, parents, and children. It recommends raising awareness and increasing the knowledge of new medias used by young people. It observes that the current civil liability regime is not adapted to the new social, cultural, and family environment, and considers that ISPs should be fully involved in the fight against cyber-harassment. Finally, it stresses that there are too many competent authorities and that they are ill-informed about the phenomenon.

¹⁵² The list was available at <http://www.check4rent.com>.

¹⁵³ Opinion n° 52/2002.

¹⁵⁴ Opinion n° 9/2005.

which the Commission has given its advice.¹⁵⁵ The Commission also advocates prior legal authorisation for more sensitive blacklists, such as those that include minors or that cross sectors. Blacklists by themselves are seen as an interference with privacy because they trigger high risks of discrimination and limit the freedom to enter into contractual relationships. The Commission moreover recommended that the law define more precisely the purposes for which blacklists could be promulgated. References to "fight against fraud" or "security" are too general to effectively frame the use of blacklists. This legislative proposal has since been abandoned.

In November 2007, the Commission issued a guideline on the redistribution of visual materials and the application of privacy law to photographs, movies and publications.¹⁵⁶

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

In 2009, a group of Belgian human rights groups, Internet and telecommunications users, and journalists, physicians, and bar associations¹⁵⁷ launched a campaign against data retention in which they call upon the legislator not to transpose the EU Data Retention Directive (2006/24/EC) into Belgian law.¹⁵⁸ This legal instrument mandates that all EU Member States transpose into national legislation the obligation for all telecommunications companies and Internet service providers to retain some of their customers' communications and location data ("traffic data") for up to two years. They also asked the government to improve that Directive and launched a petition open to every concerned individual.¹⁵⁹

The Human Rights League (Liga voor Mensenrechten) organised a campaign in 2010 that offered people the chance to "fight back and regain their privacy".¹⁶⁰ Numerous activities were organised, such as guided "privacy walks", street events, classes, and video camera spotting.¹⁶¹ It ended on 17 November 2010 with the Belgian version of the "Big Brother

¹⁵⁵ Advice n° 34/2008.

¹⁵⁶ Opinion n° 33/2007

¹⁵⁷ They are: the Liga voor Mensenrechten (Human Rights League for the Flemish-speaking Community), the Ligue des droits de l'Homme (Human Rights League for the French-speaking Community), the Orde van Vlaamse Balies (association of Flemish bars), the Ordre des barreaux francophones et germanophones (Association of French and German-speaking bars), the Ordre des Médecins (the order of Physicians), the Vlaamse Vereniging voor Journalisten (the Flemish association of journalists), the Association des journalistes professionnels (the association of professional journalists) and the Tik vzw (Internet and telecommunications users group) <http://bewaarjeprivacy.be/fr/content/qui-sommes-nous>.

¹⁵⁸ <http://bewaarjeprivacy.be/fr/content/qui-sommes-nous>.

¹⁵⁹ <http://bewaarjeprivacy.be/fr/user/register>. See also EDRI-gram, No. 7.21, "Petition against data retention in Belgium", 5 November, 2009 <http://www.edri.org/edriagram/number7.21/data-retention-belgium-petition>.

¹⁶⁰ <http://www.mensenrechten.be/>.

¹⁶¹ <http://www.winuwprivacy.be/>.

Awards"; the overall winner was the EU Data Retention Directive (2006/24/EC).¹⁶² Other nominees for the award, all branded as violating Belgians' right to privacy, included an increasingly pervasive CCTV surveillance project in a city on the Belgian coast, the Brussels transportation company (STIB)'s new "MoBIB" RFID card,¹⁶³ inquiries conducted by Antwerp city police agents into unconsummated marriages or marriages of convenience, police and judicial authorities' use of airline companies' passenger data (the so-called "passenger name records"), an owner association's collection practices vis-à-vis tenants looking for accommodation, and the handling of a debtors' database (*schuldencentrale*) by the private credit reference agency (*Beroepsvereniging voor het Krediet*).¹⁶⁴

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Belgium is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹⁶⁵ It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁶⁶ It is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The government has signed, but not ratified, the CoE Convention on Cybercrime.¹⁶⁷ In 2007, Belgium ratified the Protocol amending the European Convention on the Suppression of Terrorism.¹⁶⁸

¹⁶² <http://www.winuwprivacy.be/kandidaten>.

¹⁶³ The Ligue des droits de l'Homme is also organising a specific campaign against STIB's "MoBIB" RFID-card. See http://www.liguedh.be/index.php?option=com_content&view=article&id=916:carte-mobib-&catid=109:actualite&Itemid=280.

¹⁶⁴ *Id.*

¹⁶⁵ Signed 7 May 1982; ratified 28 May 1993; entered into force 1st September 1993, available at <http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm>.

¹⁶⁶ <http://conventions.coe.int/treaty/EN/Treaties/html/005.htm>.

¹⁶⁷ Signed 23 November 2001, available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

¹⁶⁸ Ratified 16 August 2007, available at <http://conventions.coe.int/treaty/en/Treaties/Html/190.htm>.

REPUBLIC OF BULGARIA*

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Bulgarian Constitution of 1991 recognises rights of privacy, secrecy of communications, and access to information.¹ Article 32 states, "(1) The private life of citizens shall be inviolable. Everyone shall be entitled to protection against any illegal interference in his private or family affairs and against encroachments on his honour, dignity and reputation. (2) No one shall be followed, photographed, filmed, recorded, or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law." Article 33 states, "(1) The home shall be inviolable. No one shall enter or stay inside a home without its occupant's consent, except in the cases expressly stipulated by law. (2) Entry into, or staying inside, a home without the consent of its occupant or without the judicial authorities' permission shall be allowed only for the purposes of preventing an immediately impending crime or a crime in progress, for the capture of a criminal, or in extreme necessity."

Article 34 states, "(1) The freedom and confidentiality of correspondence and all other communications shall be inviolable. (2) Exceptions to this provision shall be allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime." The right to freedom of expression is also protected by Article 39 of the Bulgarian Constitution, which states, "(1) Everyone shall be entitled to express an opinion or to publicise it through words, written and oral, sound or image, or in any other way. (2) This right shall not be used to the detriment of the rights and reputation of others, or for the incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of enmity or violence against anyone."

Article 41 states, "(1) Everyone shall be entitled to seek, obtain, and disseminate information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health, and morality. (2) Citizens shall be entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or other secret prescribed by law and does not affect the rights of others."

The Constitution provides equality and protection against discrimination for the rights of citizens.² However, discrimination still exists, particularly against women and Roma.

¹ Constitution of the Republic of Bulgaria of 13 July 1991, *State Gazette* (SG) No. 56, 13 July 1991 (effective 13 July 1991), amended and supplemented, SG No. 85 of 6 September 2003, SG No. 18 of 25 February 2005, SG No. 27 of 31 March 2006, Decision No. 7 of the Constitutional Court of the Republic of Bulgaria of 13 September 2006 - SG No. 78 of 26 September 2006, SG No. 12 of 6 February 2007, available in English at http://www.vks.bg/english/vksen_p04_01.htm.

² *Id.*, at article 6(2).

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Law for Protection of Personal Data (LPPD) was adopted by the National Assembly in December 2001 and came into effect in January 2002.³ The law's adoption was a key part of the administrative reforms that were undertaken in preparation for accession to the European Union (EU), which occurred on 1 January 2007.⁴ The law closely follows the EU Data Protection Directive. It sets out rules for the fair and responsible handling of personal information by the public and private sectors. Personal information is defined as any information that makes it possible to identify an individual directly (e.g. through a personal ID number) or indirectly through one or more specific characteristics related to his physical, physiological, psychological, genetic, economic, cultural, or social identity. Entities collecting personal information must inform people why their personal information is being collected and what it is to be used for; allow people reasonable access to information about themselves and the right to correct it if it is wrong; ensure that the information is securely held and cannot be tampered with, stolen, or improperly used; and limit the use of personal information for purposes other than the original one without the consent of the person affected, or in certain other circumstances. Sensitive information, including information concerning racial or ethnic origin, political or religious affiliation, health, sexual life, and beliefs, is given special protection and may only be processed with the express written consent of the individual.⁵

During the years since, the regulation of personal data protection has changed. LPPD was amended in 2004, 2005, and 2006; each time, parts of the text were changed in contradictory directions. For example, the law's original text introduced the requirement that a wide range of data controllers register with the Personal Data Protection Commission. In 2005, the range of data controllers was narrowed; in 2006 it was expanded again. In 2005, after a public debate between the first and second readings, Parliament rejected the suggestion of repealing Art. 35 of the Law, which guaranteed free access to personal data as long as they are part of a public register or are contained in public documents. In 2006, however, Art. 35 was repealed, which meant that access to such data would be regulated by the general regime covering access to information and that the consent of the data subject would be required. Decision No. 7 of 1996 of the Bulgarian Constitutional Court on case No. 1 established that public figures should be subject to increased scrutiny as compared to other citizens. At the same time, Art. 4 paragraph 1 item 5 of the LPPD allows for the processing of personal data when data

³ Law for Protection of Personal Data, SG No. 1 of 4 January 2002, amend. SG No. 70 of 10 August 2004, SG No. 93 of 19 October 2004, SG No. 43 of 20 May 2005, SG No. 103 of 23 December 2005, SG No. 30 of 11 April 2006, SG No. 91 of 10 November 2006, SG No. 57 of 13 July 2007, SG No. 42 of 5 June 2009, available in English at <http://www.cdpd.bg/en/index.php?p=element&aid=128>.

⁴ Europa Press Release, "Two New Members Join the EU Family," 28 December 2006, available at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1900>.

⁵ Law for Protection of Personal Data, *supra* Artt. 2-5.

controllers act in the public interest. The provisions of Art. 35 gave data controllers some clarity, though this can only be fully restored with the establishment of good practices.⁶ Other amendments to the LPPD were made in 2007 and 2009.

Administrative sanctions in the form of fines for violations of the LPPD range from BGN10,000 (approx. €€5,000) to BGN100,000 (approx. €50,000). In particular: violation of the fundamental rights of the physical bodies – a fine ranging from BGN10,000 to BGN100,000 (approx. €5,000 to €50,000); illegal processing of sensitive data – a fine ranging from BGN10,000 to BGN100,000 (approx. €5,000 to €50,000); violation of the obligation to register – a fine ranging from BGN2,000 to BGN20,000 (approx. €1,000 to €50,000); and incorrect processing of data – a fine ranging from BGN2,000 to BGN20,000 (approx. €1,000 to €10,000). Data controllers are liable for any damage caused to an individual as a result of unlawful processing or from breaching the technical requirements of data protection. The data controller is also liable for any damage caused by a data processor acting on behalf of the data controller.⁷

The transfer of personal data from data controllers to foreign individuals or legal persons or to foreign government authorities shall be allowed, with the permission of the Commission for Personal Data Protection, only if the legislation of the recipient country guarantees a level of data protection that is equivalent to or better than that provided by Bulgarian law. The assessment of the adequacy of the level of personal data protection in a third country shall be made by the Commission for Personal Data Protection, taking into consideration all the circumstances of the data transfer operation or operations, including the nature of the data, the purpose and duration of their processing, the legal basis, and the security measures provided in the third country.⁸

Sector-based laws

The LPPD sets forth the general minimum standard that must be met with regard to the processing of personal data in all spheres of public relations. Different, sector-based laws contain provisions that guarantee lawful processing of personal data in specific spheres. Parts of these sector-based laws refer to the general provisions of the LPPD.

However, there are also sector-based laws that set forth more detailed regulation with regard to the processing and protection of personal data. Among these laws are: the Law

⁶ Access to Information Programme Foundation (AIP), "Access to Information in Bulgaria 2006," at 19, available at <http://www.aip-bg.org/pdf/report2006-en-end.pdf>.

⁷ Law for Protection of Personal Data, *supra* Artt. 41 and 42. See also <http://www.investnet.bg/bulgarian-economy/LegalFramework/CommercialLawOverview/Regulatory/DataProtection.aspx>.

⁸ *Id.*, Art. 36.

on Health;⁹ the Electronic Document and Electronic Signature Law (EDES�);¹⁰ the Electronic Commerce Act (ECA);¹¹ the Law on Electronic Communications;¹² the recently approved Law for Providing Services;¹³ the Law for the Credit Institutions (LCI);¹⁴ the Law for Measures against Money Laundering (LMAML);¹⁵ the Access to Public Information Act;¹⁶ the Law on Prevention and Disclosure of Conflict of Interests;¹⁷

⁹ Law on Health, SG No. 70 of 10 August 2004, in force as of 01 January 2005, amend. SG No. 46 of 03 June 2005, SG No. 76 of 20 September 2005, SG No. 85 of 25 October 2005, SG No. 88 of 04 November 2005, SG No. 94 of 25 November 2005, SG No. 103 of 23 December 2005, SG No. 18 of 28 February 2006, SG No. 30 of 11 April 2006, SG No. 34 of 25 April 2006, SG No. 59 of 21 July 2006, SG No. 71 of 01 September 2006, SG No. 75 of 12 September 2006, SG No. 81 of 06 October 2006, SG No. 95 of 24 November 2006, SG No. 102 of 19 December 2006, SG No. 31 of 13 April 2007, SG No. 41 of 22 May 2007, SG No. 46 of 12 June 2007, SG No. 59 of 20 July 2007, SG No. 82 of 12 October 2007, SG No. 95 of 20 November 2007, SG No. 13 of 08 February 2008, SG No. 102 of 28 November 2008, SG No. 110 of 30 December 2008, SG No. 36 of 15 May 2009, SG No. 41 of 02 June 2009, SG No. 74 of 15 September 2009, SG No. 82 of 16 October 2009, SG No. 93 of 24 November 2009, SG No. 99 of 15 December 2009, SG No. 101 of 18 December 2009, SG No. 41 of 01 June 2010, SG No. 42 of 04 June 2010, SG No. 50 of 02 July 2010, SG No. 59 of 31 July 2010, SG No. 62 of 10 August 2010.

¹⁰ Electronic Document and Electronic Signature Law, SG No. 34 of 06 April 2001, in force from 6 October 2001, amend. SG No. 112 of 29 December 2001, SG No. 30 of 11 April 2006, SG No. 34 of 25 April 2006, SG No. 38 of 11 May 2007.

¹¹ Electronic Commerce Act, SG No. 51 of 23 June 2006, in force from 24 December 2006, amend. SG No. 105 of 22 December 2006, SG No. 41 of 22 May 2007, SG No. 82 of 16 October 2009.

¹² Law on Electronic Communications in SG No. 41 of 22 May 2007, amend. SG No. 109 of 20 December 2007, SG No. 36 of 04 April 2008, SG No. 43 of 29 April 2008, SG No. 69 of 05 August 2008, SG No. 17 of 06 March 2009, SG No. 35 of 12 May 2009, SG No. 37 of 19 May 2009, SG No. 42 of 05 June 2009, SG No. 45 of 16 June 2009, SG No. 82 of 16 October 2009, SG No. 89 of 10 November 2009, SG No. 93 of 24 November 2009, SG No. 12 of 12 December 2010, SG No. 17 of 02 March 2010, SG No. 27 of 09 April 2010.

¹³ Law for Providing Services in SG No. 15 of 23 February 2010, in force from 23 February 2010.

¹⁴ Law for the Credit Institutions in SG No. 59 of 21 July 2007, in force from 1 January 2007, amend. SG No. 105 of 22 December 2006, SG No. 52 of 29 June 2007, SG No. 59 of 20 July 2007, SG No. 109 of 20 December 2007, SG No. 69 of 05 August 2008, SG No. 23 of 27 March 2009, SG No. 24 of 31 March 2009, SG No. 44 of 12 June 2009, SG No. 93 of 24 November 2009, SG No. 95 of 01 December 2009, SG No. 94 of 30 November 2010.

¹⁵ Law for the Measures against Money Laundering in SG No. 85 of 24 July 1998 amend. SG No. 1 of 02 January 2001, SG No. 31 of 04 April 2003, SG No. 103 of 23 December 2005, SG No. 105 of 29 December 2005, SG No. 30 of 11 April 2006, SG No. 54 of 04 July 2006, SG No. 59 of 21 July 2006, SG No. 82 of 10 October 2006, SG No. 108 of 29 December 2006, SG No. 52 of 29 June 2007, SG No. 92 of 13 November 2007, SG No. 109 of 20 December 2007, SG No. 16 of 15 February 2008, SG No. 36 of 04 April 2008, SG No. 67 of 29 July 2008, SG No. 69 of 05 August 2008, SG No. 22 of 24 March 2009, SG No. 23 of 27 March 2009, SG No. 93 of 24 November 2009, SG No. 88 of 09 November 2010.

¹⁶ In SG No. 55 of 7.07.2000, subsequently amended SG No. 1 of 4 January 2002, SG No. 45 of 30 April 2002, SG No. 103 of 23 December 2005, SG No. 24 of 21 March 2006, SG No. 30 of 11 April 2006, SG No. 59 of 21 July 2006, SG No. 49 of 19 June 2007, SG No. 57 of 13 July 2007, SG No. 104 of 05 December 2008.

¹⁷ In SG No. 94 of 31 October 2008 r., in force from 1 January 2009 r., amended SG No. 10 of 6 February 2009, in force from 31 March 2009, amended SG No. 26 of 7 April 2009, amended SG No. 101 of 18 December 2009 r.

the Law for Publicity of the Property of Persons Occupying High State Positions;¹⁸ the Law on Access and Disclosure of Documents and on Announcement of Affiliation of Bulgarian Citizens to the State Security and the Intelligence Services of the Bulgarian National Army;¹⁹ the Ministry of the Interior Act, in force from 24 February 2006; the Bulgarian Special Investigation Devices Act.²⁰

The Family Code provides adequate protection of personal data for birth parents, adopted children, and adoptive parents. The regulation creates two new registers, one containing information about children available for adoption, the other about parents wishing to adopt children. Both registers contain information about the subjects' health and family status and property, as well as various details about the personal and family lives of the individuals concerned.

DATA PROTECTION AUTHORITY

The LPPD establishes an independent public authority, the Commission for Personal Data Protection (CPDP or the Commission) to supervise compliance and implementation, maintain a national register of data controllers, examine complaints, and take legal action for violations.²¹ It is an independent, jointly governed authority, and consists of a chairperson and four members. The members of the Commission and its chairperson are proposed by the Council of Ministers and elected by the Parliament for a term of five years. They may be re-elected for another mandate. The Commission was established by decision of the Parliament on 23 May 2002.

In compliance with the Rules on the Activity of the Commission for Personal Data Protection and its Administration, the total number of staff is 81 full-time positions

¹⁸ In Official SG No. 38 of 9 May 2000, amended SG No. 28 of 19 March 2002, amended SG No. 74 of 30 July 2002, amended SG No. 8 of 28 January 2003, in force from 1 March 2003, amended SG No. 38 of 11 May 2004, amended SG No. 105 of 29 December 2005, in force from 1 January 2006, amended SG No. 38 of 9 May 2006, amended SG No. 73 of 5 September 2006, in force from 1 January 2007, amended, SG No. 109 of 20 December 2007, in force from 1 January 2008, amended SG No. 33 of 28 March 2008, SG No. 69 of 5 August 2008, amended SG No. 94 of 31 October 2008, in force from 1 January 2009, amended SG No. 93 of 24 November 2009, in force from 25 December 2009, SG. No. 18 from 5 March 2010, in force from 5 March 2010.

¹⁹ In SG No. 102 of 19 December 2006, amended SG 41 of 22 May 2007, amended SG No. 57 of 13 July 2007, amended SG No. 109 of 20 December 2007, in force from 1 August 2008, amended SG No. 69 of 5 August 2008, amended SG No. 25 of 3 April 2009, amended SG No. 35 of 12 May 2009,, amended SG No. 42 of 5 June 2009, amended, SG No. 82 of 16 October 2009, amended SG No. 93 of 24 November 2009, amended SG No. 18 of 5 March 2010, in force from 5 March 2010, amended, SG No. 54 of 16 July 2010.

²⁰ In SG No. 95 of 21 October 1997 г., amended SG No. 70 of 6 August 1999 г., in force from 1 January 2000 г., amended SG No. 49 of 16 June 2000 г., in force from 16 June 2000 г., amended, SG No. 17 of 21 February 2003 г., amended, SG No. 86 of 28.10.2005 г., in force from 29 April 2006 г., amended SG No. 45 of 2 June 2006 г., amended SG No. of 10 October 2006 г., amended, SG No. No. 109 of 20 December 2007 г., in force from 1 January 2008 г., amended SG No. 43 of 29 April 2008 г. amended SG No. 109 of 23 December 2008 г., amended SG No. 88 of 6 November 2009 г., amended SG No. 93 of 24 November 2009 г., amended, SG No. 103 of 29 December 2009 г., amended SG No. 32 of 27 April 2010 г., in force from 28 May 2010 г.

²¹ See the CPDP official Web site at <http://www.cdpd.bg/en/index.php>.

(including five elective positions).²² The administration is organised in five Directorates whose powers are stipulated in the regulations, and the functional relations among the units are regulated by internal rules adopted by the Commission.

In compliance with the LPPD the Commission shall: analyse and exercise overall control of the observance of the normative acts in the sphere of protection of personal data; keep a register of personal data controllers and of the registers of personal data the controllers keep; carry out inspections of personal data controllers; express opinions and give permits in the cases stipulated by the law; issue obligatory prescriptions for administrators in connection with the protection of the personal data; impose, upon prior notice, temporary prohibitions from processing personal data that violate the norms of personal data protection; consider claims against the actions of data controllers that have violated the rights of the natural persons as well as of the appeals of third persons in connection with their rights; participate in obligatory consultations on the drafts of primary and secondary legislation in the field of personal data protection; and apply the decisions of the European Commission in the field of personal data protection.²³

The Commission publishes a bulletin providing information on its activity and decisions taken²⁴ as well as annual reports on its activities.²⁵

The Commission also wrote an Ethics Code of Behaviour of Data Controllers, which sets out specific legal obligations and attempts to "balance the interests of the persons and the interests of the data controllers within the framework of the law on adequate measures for personal data protection."²⁶

²² Rules on the Activity of the Commission for Personal Data Protection and its Administration, promulgated SG No. 11 of 10 February 2009, available at <http://www.cdpd.bg/en/index.php?p=element&aid=36>. "The necessity of the elaboration and adoption of the Rules of 2009 was based on the new priorities adopted by the Commission for Personal Data Protection in its capacity of an independent supervisory authority in the field of personal data processing. This regulatory act aims at synchronising the activity of the administrative units of the Commission while exercising overall control over the observance of the regulatory acts in the field of personal data protection in the course of personal data processing. The regulations set out in the Rules allowed the Commission to achieve flexibility when adopting decisions, which inevitably results in raising the efficiency of the activity of the Commission as a whole." See Annual Report for the Activity of the Commission for Personal Data Protection in 2009, available in English at <http://www.cdpd.bg/en/index.php?p=element&aid=249>.

²³ Law for Protection of Personal Data, *supra* Art. 10.

²⁴ For the time being, the Information Bulletin is published only in Bulgarian and is available at <http://www.cdpd.bg/index.php?p=home&aid=0>.

²⁵ Available in English at <http://www.cdpd.bg/en/index.php?p=rubric&aid=14>.

²⁶ Bulgaria Data Protection Commissioner Annual Report 2006, available at http://www.cdpd.bg/otcheti/annual_report2006.pdf.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The relevant case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.²⁷

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Under the Criminal Procedure Code (CPC) of 2006²⁸, search and seizure within private premises for the purpose of collecting evidence for criminal investigation is permissible only on request by a public prosecutor and subsequent to a warrant issued by a judge (Art. 161 therein).²⁹ The grounds for permitting search and seizure are "presence of sufficient bases to suspect" that in certain premises there are "matters, papers, or databases of significance to a case". In cases of pressing need, when no other opportunity for saving the evidence is available, search and seizure may be performed immediately, subject to approval by a judge within the following 24 hours.

With regard to access to private sector databases, Art. 159 of the CPC of 2006 states that all private sector bodies are obliged to keep and make available to law enforcement agencies on request documents, information stored in computer files, and data concerning computer service customers including traffic data. The necessary precondition for asking for such data is that a criminal investigation has been opened.

For the purpose of criminal investigations, the relevant bodies within the Ministry of Interior can compel private persons to grant cooperation. The Ministry of the Interior Act³⁰ specifies the obligation of granting access to office premises, technical connections, or other possessions (Art. 148, paragraph 2). In practice, in some cases the authorities refer to this provision even for requesting access to electronic data. The same powers are awarded to the State Agency for National Security (Art. 27 of the State Agency for National Security Act).³¹

Policies regarding this issue are unclear. One could conclude that although in the 1990s there was a tendency to set higher requirements for access to premises or data, the last

²⁷ *Cfr.* Sections "Wiretapping, access to, and interception of communications," "Data retention," "Cybercrime," "Bodily Privacy," "Open Government," *infra* in this Report.

²⁸ Available in English at http://www.mjeli.government.bg/Npk/docs/CRIMINAL_PROCEDURE_CODE.pdf.

²⁹ The former Criminal Procedure Code of 1974 allowed search and seizure on permission of the public prosecutor. A substantial amendment in force from 2000 changed this to the current regime. The amendment was reflected in the new CPC of 2006.

³⁰ Available in English at http://www.mvr.bg/NR/rdonlyres/5F939B72-40AD-45AB-A78A-D09207DB695C/0/ZMVR_EN.pdf.

³¹ Available in English at http://www.dans.bg/index.php?option=com_content&view=category&layout=blog&id=12&Itemid=10&lang=en.

several years have seen the reverse. Security concerns are about to jeopardise the enjoyment of civil liberties. Regarding some issues, however, such as the data retention legislation, there has been strong public and political debate.

Wiretapping, access to, and interception of communications

Until the Constitution of 1991 was adopted, there were no legal guarantees for wiretapping, access and interception of communications in Bulgaria. As already noted, Article 34 of the Constitution allowed the interception of correspondence only for the prevention or investigation of serious crimes after a warrant has been issued by a judicial body.³²

In 1997 Parliament passed a special law regulating the matter, namely the Special Intelligence Means Act (SIMA).³³ It underwent minor amendments in August 1999 and June 2000, more extensive ones in February 2003, and some further minor changes in April 2006. Its essential provisions have, however, remained intact since its adoption, and the account which follows is based on the present version. There are two main groups of bodies authorised to use interception: law enforcement authorities and security services. Respectively, there are two main grounds for interception: to prevent or uncover a "serious criminal offence" or to protect national security. Article 93 paragraph 7 of the Criminal Code of 1968 defines a "serious criminal offence" as one punishable by more than five years' imprisonment. According to SIMA, in the case of the former special means of surveillance may be used when necessary if the requisite intelligence cannot be obtained through other means. "Special means of surveillance" are defined as technical devices that can be used for creating photographs, audio and video recordings, and marked objects, as well as the methods for operating these devices.³⁴ They may be used against persons suspected – on the basis of the information available – of planning, committing, or having committed serious offences, or against persons whom the suspected perpetrators may unwittingly involve in the above. Such means may also be used against persons and objects relating to national security and in respect of persons who have agreed to it in writing in order to protect their lives or property.

³² See Constitution of the Republic of Bulgaria, *supra* Art. 34.

³³ In SG No. 95 of 21 October 1997, supplemented SG No. 70 of 6 August 1999, in force from 1 January 2000, amended SG No. 49 of 16 June 2000, SG. No 17 of 21 February 2003, supplemented SG No. 86 of 28 October 2005, in force from 29 April 2006, amended SG No. 45 of 2 June 2006, SG No. 82 of 10 October 2006, amended and supplemented SG No. 109 of 20 December 2007, in force from 1 January 2008, SG No. 43 of 29 April 2008, SG No. 109 of 23. December 2008, SG No. 88 of 6 November 2009, available in English at http://www.dans.bg/index.php?option=com_content&view=category&layout=blog&id=12&Itemid=10&lang=en.

³⁴ Special Intelligence Means Act, Section 2(1).

The Act was found to be in violation of Art. 8 of the European Convention of Human Rights by the European Court of Human Rights (ECtHR).³⁵

By 2009, practically speaking there was no effective oversight of security services with respect to wiretapping. In November 2000, the Movement for Rights and Freedoms (*Dvizhenie za prava i svobodi* or DPS), a party of ethnic Turks, reported that its leaders were being monitored by the security services.³⁶ Earlier, in August 2000, listening devices were found in the apartments belonging to the Prosecutor General, Nikola Filchev, and several politicians. Filchev blamed the bugs on the Interior Ministry's Criminal Intelligence Service (CIS). A Parliamentary session was held after 53 Democratic Left Parliamentarians demanded a hearing.³⁷ Following the debate, members of the opposition Bulgarian Socialist Party (BSP) submitted draft amendments to put in place a system of judicial oversight for the use of surveillance.³⁸ A Parliamentary Commission held hearings in 2001 on the activities of "public order" agencies, which include the National Intelligence Service, the National Bodyguard Service, and the National Security Service.³⁹ In October 2001, the Interior Ministry reported that they had found illegal wiretapping devices, in recording mode, in the Central Telephone Exchange in Sofia and preparations for such devices in several of the city's other exchanges. The bugging of telephone subscribers has been taking place since 1994 and was said to be economically motivated.⁴⁰ In November 2001, the director of the NSS resigned from his position. Several allegations were made that he wiretapped politicians, but they were never substantiated.⁴¹ In December 2002, the media reported allegations, partly confirmed by the Minister of the Interior, that the telephones of a number of public figures, including the former National Security Service director and the Minister of Justice, had been unlawfully tapped and that a person dubbed "Gnom" had been investigated.⁴²

³⁵ ECHR, Application No. 62540/00, *Association of European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Judgment of 28 June 2007 (final on 30 January 2008), available at [@http://www.eurorights-bg.org/bg/categories/legal/eu_courts/62540.html](http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbk&action=html&highlight=62540/00&sessionid=61882562&skin=hudoc-en)

³⁶ "Security Services Bugged Ethnic Turk's Leaders," BBC Worldwide Monitoring, 26 November 2000.

³⁷ "Buggate Scandalises Bulgaria," *Transitions online*, 31 July – 6 August 2000.

³⁸ "Courts Should Be Involved in Controlling Bugging Devices," BBC, 9 August 2000.

³⁹ United States Department of State, *Country Reports on Human Rights Practices 2001*, 4 March 2002, available at <http://www.state.gov/g/drl/rls/hrrpt/2001/eur/8238.htm>.

⁴⁰ "Bugging Affair 'Economically Motivated', Interior Ministry Says," BBC Worldwide Monitoring, 4 October 2001.

⁴¹ "Security Chief Says 'Low Confidence' in Office Led to Resignation," BBC Worldwide Monitoring, 28 November 2001.

⁴² "Bulgarian Government Faces New Bugging Scandal," RFE/RL, 23 December 2002, available at <http://www.rferl.org/content/article/1142824.html>.

After the ECtHR judgment, the SIMA was amended several times in 2008 and 2009. According to the last of these amendments, in 2010 a Parliamentary sub-committee was entrusted with the oversight of wiretapping. So far there have been no practical results of its work, though this is partly due to the fact that the subcommittee was selected only few months ago.

The use of intercepts is subject to authorisation by a judge. However, judges are typically not informed in depth about the subject matter of the investigation and are never told the results of the surveillance. Telecommunication providers are required by law to provide "intercept capability". There are no official statistics available on the use of intercepts. In 2000, a leaked report from the Supreme Prosecution's Office said that over 10,000 warrants were issued over a period of a year and a half, beginning in January 1999. Of these, only 267 to 269 were used as evidence in criminal proceedings. It is highly expected that the new Parliamentary subcommittee will publish statistics.

National security legislation

No specific information has been provided under this section.

Data retention

Soon after joining the EU, the Bulgarian government started drafting a regulation to implement Directive 2006/24/EC (the "Data Retention Directive").⁴³ There was no substantial consultative process on the matter. On 7 January 2008, Regulation No. 40 on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/or services for the needs of national security and crime investigation was issued by the State Agency on Information Technologies and Communication (SAITC) and the Ministry of the Interior (MoI). On 29 January 2008, Regulation No. 40 was promulgated in the *Bulgarian State Gazette*. It allowed easy access to traffic data by law enforcement authorities, security services, and a directorate in the Ministry of the Interior that is responsible for technical operations. Direct technical public authorities' access to databases of private providers of e-communications was planned under the Regulation.⁴⁴

The adoption of Regulation No. 40 triggered a massive wave of criticism and anger among the country's civil society and business community, as it implied serious intrusion into private life and correspondence. On 19 March 2008, Access to Information Programme (AIP), a prominent Bulgarian NGO working in the field of access to public information and personal data protection, filed an appeal to the Bulgarian Supreme Administrative Court (SAC) against Regulation No. 40. According to AIP, the adoption of this regulation was in violation of the Constitution of the Republic of Bulgaria, the

⁴³ OJ L 105, 13 April 2006, at 54–63, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML>.

⁴⁴ See more at http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm.

European Convention on Human Rights, and European Union legislation.⁴⁵ On 17 July 2008 a three-member panel of the Supreme Administrative Court rejected the complaint.⁴⁶ AIP appealed the decision before a five-member panel of the SAC which, on 11 December 2008, struck down the decision of the lower court and Art. 5 of the challenged Regulation No. 40. Article 5 provided for "passive access through a computer terminal" by the Ministry of the Interior, as well as access without court permission by security services and other law enforcement bodies, to all data retained by Internet and mobile communications providers. The Court held that data can be accessed only after a warrant has been issued by a judge, based on a case-by-case assessment.

Currently, data retention is required by the Law on Electronic Communications.⁴⁷ Traffic data should be kept by the providers of e-services for a period of 12 months. Warrants to access data must be issued by a judge, and providers should speedily grant access. The Parliamentary subcommittee responsible for wiretapping also oversees data retention issues.

Since then, there have been persistent attempts by two governments and some MPs to restore direct access. All these proposals failed. Most recently, a proposal to establish direct technical connection, made by the new government (elected in 2009) but after much public debate and strong resistance by NGOs and bloggers at both government and Parliamentary stages, the judicial warrant was retained in the law.

As a result of judgments of the ECtHR and the Bulgarian Supreme Court, the government and Parliament were forced to make changes in the normative framework for wiretapping and data retention. For their part, NGOs had a crucial role in bringing these legal actions. There are still issues to be resolved, especially in the area of wiretapping, but the foundations for oversight by the Parliament have been created. Judges issue warrants for wiretapping or access to traffic data. NGOs are active in the field.

National databases for law enforcement and security purposes

The only national database containing data about all individuals is the citizens' register. It is kept electronically by a Directorate in one of the ministries and data are filled in by the municipalities. There are no law enforcement data in this register.

The police maintain a register of suspects against whom criminal charges have been raised *ex officio*. It is provided for by the Regulation on the Order for Carrying out Police Registration of 2007.⁴⁸ Minors are not subject to registration. Suspects' biometric data (fingerprints) are also gathered. The register is kept in compliance with the principles of the LPPD, to which the regulation specifically refers. The purpose of the registration is

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ Law on Electronic Communications, *supra* at Artt. 250(a-f), 251 and 251(a).

⁴⁸ Regulation on the Order for Carrying out Police Registration, SG No. 56 of 10 July 2007, in force from 11 October 2007.

not specifically stated in the law. It is obvious that it is connected with the role of the police in law enforcement and the protection of public order.

There is also a register of people with criminal convictions. This register is kept with the courts. Data about convictions are kept as long as the effects of rehabilitation are incomplete. For years there have been policy plans to create a unified register of individuals connected with organised crime that can be used by all the bodies. The positive effect of such a register is not clear.

Bulgaria's Interior Minister, Tsvetan Tsvetanov, has officially opened the National Supplementary Information Request at the National Entry (SIRENE) Bureau. Its main task, established in all Schengen States, is the exchange of additional or supplementary information on alerts between the States. The Bulgarian National SIRENE Bureau is a specialised operational unit in the International Operational Police Cooperation Directorate in the Ministry of the Interior. The final evaluation of Bulgaria's readiness to enter the Schengen zone, at the beginning of December 2010, depends upon the Schengen Information System (SIS) and the SIRENE Bureau.⁴⁹

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

In August 2004, the Appeal Prosecution of the city of Plovdiv issued an order stating that all Internet clubs and cafés in Plovdiv should require and keep records of customers' social security numbers and personal data, as well as the times when they accessed the Internet.⁵⁰ On 24 March 2005, the National Service for combating organised crime for the Ministry of the Interior delivered a "Direction for action" to Bulgarian Web site hosting companies. It was issued and signed by the Chief of the Department of Intellectual Property, Trademark, Computer Crimes, and Gambling. The document imposed an obligation on ISPs' executives, stating: "...in seven days from the date of issuing this order you must terminate free hosting Web space with a quota bigger than 100MB to anonymous users. More than 100MB of Web space should be given only to customers with a signed user contract accompanied by a copy of their ID card or other relevant document for identification".⁵¹

Under the Bulgarian Penal Code, sanctions can only be imposed on individuals, not companies. This "Direction for action" is considered by the Internet community as an attempt to make ISPs liable for the content they host. Such actions may result in lawsuits in cases where content that the ISPs have mistakenly considered illegal has been

⁴⁹ "Bulgaria Wired into SIRENE-Schengen Information System," *Novinite.com*, 22 October 2010, available at http://www.novinite.com/view_news.php?id=121405.

⁵⁰ Order No. 30 of 27 July 2004 issued by Plovdiv Appeal Prosecution.

⁵¹ This order has been issued and sent personally to the ISP executives. Not available online.

removed. ISPs cannot be held liable unless the individual in question has been properly informed by the police about illegal content and the individual refuses to remove it. This warning should be in writing so the interests of all users are protected. The case was widely reviewed in Bulgarian and foreign media.⁵²

Critical infrastructure

No specific information has been provided under this section.

INTERNET AND CONSUMER PRIVACY

E-commerce

The Law on Electronic Communication provided for special regulation of the protection of personal data in national electronic networks.

The Electronic Commerce Act, adopted in 2006, transposed the standards set forth by Directive 2000/31/EC on Electronic Commerce.⁵³ According to the Act, commercial communication consists in promotional or other communication designed to present, directly or indirectly, the goods or image of a person pursuing a commercial or craft activity, or exercising a regulated profession.

Under the Bulgarian Law on Electronic Communication, all calls, messages, or email for the purposes of direct marketing shall be allowed only if the recipient's prior consent has been obtained. Consent may be withdrawn at any time. Prior consent shall not be required when the sender has obtained the recipient's contact details in the context of a commercial transaction or provision of service to customers and the message is sent for the purpose of direct marketing of the undertaking's own services. In any case where prior consent has not been obtained, any person who sends messages for marketing purposes shall be obliged to offer each recipient the chance to opt out of receiving further such messages and respect any refusal to receive messages for marketing purposes. Sending messages for marketing purposes shall be prohibited even when the requirements under the law are fulfilled if the identity of the sender cannot be established or if the message has no valid address to which the recipient may send a refusal to receive messages.

At the end of 2009, the National Statistics Institute announced the results of two nationwide surveys: Information and Communication Technologies Usage and E-Commerce in Enterprises 2009 and ICT Usage in Households and by Individuals Aged between 16 and 74.⁵⁴ The results show that the most active age group regularly using the Internet in 2009 is the group aged 16 to 24 and the proportion of individuals spending their own time on the Internet from this group increased by 41.7 percent in the last five years, reaching 75.1 percent in 2009.

⁵² See German edition of *Heise.de* available at <http://www.heise.de/newsticker/meldung/58114>.

⁵³ Electronic Commerce Act, *supra*.

⁵⁴ Available in English at <http://www.nsi.bg/otrasalen.php?otr=48>.

Cybersecurity

The Penal Code provides for the definition of computer crimes.⁵⁵ This type of crime encompasses public relations@@@ with regard to the proper functioning of computers, computer systems, and computer networks, as well as the lawful generation and exploitation of information. The term "computer crimes" includes illegally accessing, changing, harming, and destroying data or programs, introducing a virus, and disclosing passwords.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

No specific information has been provided under this section.

TERRITORIAL PRIVACY

Video surveillance

Specific provisions regulating the use of video surveillance can be found in different, sector-based laws.⁵⁶

According to a statement issued by the Commission for Personal Data Protection on 21 July 2010, personal data controllers shall inform the physical persons about video surveillance by using visible on-site notices to immediately alert the public to the fact that monitoring is taking place and provide essential information about the processing and the relevant personal data controller, including contact information.⁵⁷

Location privacy (gps, mobile phones, location based services, etc.)

No specific information has been provided under this section.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

On 10 March 2010, the Commission for Personal Data Protection – acting on request of Deputy Minister of the Interior V. Vuchkov – issued a statement about the admissibility of the collection and processing of Passenger Name Records (PNR)/Advanced

⁵⁵ Penal Code, Art. 319, items from (a) to (f).

⁵⁶ See, for example, Private Security Business Act in SG No. 15 of 24 February 2004, amended SG No. 105 of 29 December 2005, amended SG No. 30 of 11 April 2006, amended SG No. 34/25 April 2006, amended SG No. 82 of 10 October 2006, available in English at http://www.naftso.org/?current=documents&lang=en&id_sess=pta9qcip2viflrrbdkn6fi9ld4.

⁵⁷ Available in Bulgarian at <http://www.cdpd.bg/index.php?p=home&aid=0>.

Passengers Information (API) by the UK Border Agency with regard to the e-Borders electronic system.⁵⁸

NATIONAL ID& SMART CARDS

Pursuant to the Law for the Bulgarian Identification Documents,⁵⁹ all Bulgarian identification documents contain biometric data. The law sets forth special measures for protection with regard to the processing of these data, as well as guarantees for the citizens in respect of their rights.

Rfid

No specific legal framework dealing with processing personal data through this kind of technology exists in Bulgaria. The general standards for personal data protection set forth in the ECA shall be applied. In 2007, the Communications Regulation Commission adopted a list of radio equipment using frequency bands harmonised throughout the EU and electronic communications terminal equipment— adopted with Decision No. 1472 as of 20 December 2007 of the Communications Regulation Commission and promulgated in the State Gazette, issue 8 as of 25 January 2008.

BODILY PRIVACY

Bulgarian legislation stipulates a limited number of cases where medical examinations may be made obligatory. For example, under the Code of Labour (Art. 140(a) and Art. 302) employees starting their first job should undergo mandatory medical examination. Bulgarian legislation does not stipulate cases in which obligatory genetic examination shall be undertaken. The Law on Health (Art. 57) stipulates a specific number of required immunisations, as well as the mechanism of implementation and control.⁶⁰

In Bulgaria, DNA profiles made for the purposes of police registration are collected and processed by the National Criminology and Criminalities Research Institute to the Ministry of the Interior. In two decisions the CPDP has found violations by the Ministry of the Interior with regard to the holding of data from police registration.⁶¹

⁵⁸ More information available in Bulgarian at <http://www.cdpd.bg/index.php?p=rubric&aid=15>.

⁵⁹ Law for the Bulgarian Identification Documents, SG No. 93 of 11 August 1998, in force as of 01 April 1999, amend. SG No. 53 of 11 June 1999, SG No. 67 of 27 July 1999, SG No. 70 of 06 August 1999, SG No. 113 of 28 December 1999, SG No. 108 of 29 December 2000, SG No. 42 of 27 April 2001, SG No. 45 of 30 April 2002, SG No. 54 of 31 May 2002, SG No. 29 of 31 March 2003, SG No. 63 of 15 July 2003, SG No. 96 of 29 October 2004, SG No. 103 of 23 November 2004, SG No. 111 of 21 December 2004, SG No. 43 of 20 May 2005, SG No. 71 of 30 August 2005, SG No. 86 of 28 October 2005, SG No. 88 of 04 November 2005, SG No. 105 of 29 December 2005, SG No. 30 of 11 April 2006, SG No. 82 of 10 October 2006, SG No. 105 of 22 December 2006, SG No. 29 of 06 April 2007, SG No. 46 of 12 June 2007, SG No. 52 of 29 June 2007, SG No. 66 of 25 July 2008, SG No. 88 of 10 October 2008, SG No. 110 of 30 December 2008, SG No. 35 of 12 May 2009, SG No. 47 of 23 June 2009, SG No. 82 of 16 October 2009, SG No. 102 of 22 December 2009, SG No. 26 of 06 April 2010.

⁶⁰ Law on Health, *supra*.

⁶¹ CPDP, Decision No. 8 of 21 March 2007 and Decision No. 16 of 5 July 2006.

WORKPLACE PRIVACY

According to the Labour Code⁶² and Insurance Code,⁶³ employees/workers must provide their employers with their personal data when necessary for the implementation of legal requirements with regard to labour and insurance relations.

Currently, the practice of the CPDP with regard to determining the scope of the right of the employer to process employees' personal data is based on appeals from employees claiming that their employers are processing personal data to a greater extent than necessary, or have illegally transferred personal data to third parties.

HEALTH & GENETIC PRIVACY

Medical records

The general law regulating the collection and processing of medical information about the citizens is the Law on Health. Processing, using, and keeping anonymised medical data, and exchanges of medical-statistical information, are carried out pursuant to the Regulations of the Minister of Health,⁶⁴ in concert with the National Statistical Institute. A priority for the Bulgarian Government is the establishment of a National Register of Patients with Rare Diseases.

The Executive Agency for Transplantation in Bulgaria is a specialised body whose functions are the management, coordination, and control of transplantation activities. The Agency holds several registers containing sensitive personal data. The disclosure of information that would allow the identification of either donors or recipients is prohibited.

The legal framework regulating the processing of personal data in the sphere of reproductive medicine is provided by the Law of the Transplantation of Organs, Tissues, and Cells. It was adopted in 2007 without public debate. Currently, pursuant to the existing regulations, the registers of donors and recipients of genetic material are maintained by the licensed reproduction medicine clinics. The data from these registers are sent to the Executive Agency for Transplantation. However, they are not processed there. The medical specialists working directly with the genetic material are the only ones allowed to access the data.

⁶² In SG No. 26 of 1 April 1986 and No. 27 of 4 April 1986, available in English at <http://www.mlsp.government.bg/en/docs/labour/index.htm>.

⁶³ Insurance Code, SG No. 103 of 23 December 2005, in force as of 01 January 2006, amend. SG No. 105 of 29 December 2005, SG No. 30 of 11 April 2006, SG No. 33 of 21 April 2006, SG No. 34 of 25 April 2006, SG No. 54 of 04 July 2006, SG No. 59 of 21 July 2006, SG No. 82 of 10 October 2006, SG No. 105 of 22 December 2006, SG No. 48 of 15 June 2007, SG No. 97 of 23 November 2007, SG No. 100 of 30 November 2007, SG No. 109 of 20 December 2007, SG No. 67 of 29 July 2008, SG No. 69 of 05 August 2008, SG No. 24 of 31 March 2009, SG No. 41 of 02 June 2009, SG No. 19 of 09 March 2010, SG No. 41 of 01 June 2010, SG No. 43 of 08 June 2010, SG No. 86 of 02 November 2010.

⁶⁴ In SG No. 57 of 14 July 2000.

According to the Law on Blood, Blood Donation, and Blood Transfusion,⁶⁵ blood transfusion centres should process the data of the blood donors.

In September 2007, Bulgaria started issuing its first electronic health cards as part of the pilot project launched by the Ministry of Health and the National Health Insurance Fund (NHIF) in February 2007. Each e-health card is equipped with a microchip that stores data about the patient and the issuer, including the card number and a security certificate. With this information, the patient's insurance status and his/her assignment to a General Practitioner can be automatically checked. In addition, electronic prescriptions for medications covered by the Bulgarian health insurance fund will be recorded on the chip.⁶⁶

Genetic identification

No definition of the term "genetic information" is provided by the Bulgarian legislation. The legal framework regulating the collection and processing of such information about Bulgarian citizens is provided by the Law on Health.⁶⁷ General principles for the protection of citizens from the illegal collection and processing of genetic information are provided by Section IV of the Law on Health – Genetic Health, and Genetic Examination – as well as in the ethical principles with regard to genetic examinations adopted by the Ethics of Scientific Research Committee at the Medical University, Sofia.

FINANCIAL PRIVACY

The relevant legal framework regulating the processing of financial information is provided by the Law for the Credit Institutions⁶⁸ and the Law for Measures against Money Laundering.⁶⁹ The framework regulates the collection of personal data when using different types of bank services. The maximum time frames within which the information may be held are also defined. A legislative balance was struck between the protection of citizens' personal data and the prevention of money laundering. The legislation is in line with the requirements of Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.⁷⁰

⁶⁵ SG No. 102 of 21 November 2003, available in English at <http://www.mlsp.government.bg/BG/integration/euro/chapter13/euro/09.Public%20Health/02.bg%20legislation/law%20on%20blood%20en.pdf>.

⁶⁶ ePractice, eGovernment Factsheet – Bulgaria – National Infrastructure (March 2010), available at <http://www.epractice.eu/en/document/288399>.

⁶⁷ Law on Health, *supra*.

⁶⁸ Law for the Credit Institutions, *supra*.

⁶⁹ Law for the Measures against Money Laundering, *supra*.

⁷⁰ Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF>.

E-GOVERNMENT& PRIVACY

The new e-government portal of Bulgaria was officially launched in October 2007.⁷¹ It comprises a catalogue of public services provided by the central State Administration and enables citizens and businesses to obtain online information on many public services, as well as forms to download. Some e-government services do require the use of special smart cards containing personal electronic signatures provided by the State-owned company *Informatsionno Obsluzhvane* (Information Services).⁷² Among these are the online submission of tenders, personal and corporate tax, and VAT declarations, social security declarations, and changes of address, as well as access to the Property Register.⁷³

The Law on Electronic Governance specifies the activity of administrative bodies related to work with electronic documents, the electronic provision of administrative services, and the exchange of electronic documents between the administrative bodies.⁷⁴ The law shall apply also to the activities of persons charged with public functions and of organisations providing public services. The electronic administrative services shall be the administrative services provided to citizens and organisations by the administrative bodies; the services provided by persons charged with public functions; and those public services that can be requested and/or provided remotely by electronic means. The administrative bodies, the persons charged with public functions, and the organisations providing public services shall be obliged to provide all services within their competence electronically unless a law provides for a special form for conducting separate actions or issuing relevant acts. The Minister of State Administration and Administrative Reform shall exercise overall control over compliance with this Law.

According to the Bulgarian National Statistical Institute, from the end of 2009, "While 5.9 percent of individuals have downloaded official forms from the Internet and 4.7 percent have filled them in and sent them back to the relevant institutions, the proportion of individuals who have used e-government services for obtaining information from public authorities' Web sites is 7.9 percent."⁷⁵

OPEN GOVERNMENT

In 2000, the Access to Public Information Act was adopted in Bulgaria.⁷⁶ It regulates the right of every individual to obtain access to the information generated and held by the bodies of the executive, legislative, and judicial powers, the local self-government

⁷¹ See <http://www.egov.bg>.

⁷² ePractice, eGovernment Factsheet – Bulgaria – National Infrastructure, *supra*.

⁷³ *Id.*

⁷⁴ In SG No. 46 of 12 June 2007, in force from 13 June 2008, available in Bulgarian at <http://www.mtitc.government.bg/page.php?category=486&id=3634>.

⁷⁵ For more detailed information see <http://www.nsi.bg/otrasalen.php?otr=48>.

⁷⁶ Access to Public Information Act, *supra*.

bodies, public-law entities, as well as individuals or legal bodies whose activities are financed with funds from the consolidated state budget, subsidies from the European Union funds or allocated through EU projects and programmes. On 5 December 2008, key amendments to the Bulgarian Access to Public Information Act were promulgated. The amendments reflect necessary changes that the Access to Information Programme Foundation formulated and recommended in 2007 and 2008 in its annual reports "Access to Information in Bulgaria". They were introduced through two draft laws that, according to the rules of work of the National Assembly, were combined into a single bill before the Parliamentary vote. The key amendments to the Access to Public Information Act concern: the extension of the scope of the "obliged bodies" by including regional units of the central authorities, natural or legal persons financed under EU funds, projects, or programmes, and companies financed or controlled by the state; the introduction of obligation for proactive publication online by public authorities; the definition of "trade secret" for the purposes of protection against unfair competition and the placing of the burden of proof of infringements on the "obliged bodies"; the introduction of the overriding public interest test in the disclosure of information which might fall within the exemptions; and the changing of the discretionary power of "obliged bodies" to provide partial access to information.

In 2008, the Law on Prevention and Exposure of Conflict of Interest was adopted. In Bulgaria, some provisions of the law repeat pre-existing norms, which have not been applied efficiently. A considerable development of the law is the establishment of a wide range of high-level officials who have the obligation to avoid conflict of interests and to declare some information publicly. The law gives a definition of conflict of interests (Art. 2) and describes specific types of conduct and relations which are unacceptable (Artt. 5-11). A mechanism for disclosure and establishing conflict of interests is provided, as well as the possibility of court oversight. Particular circumstances are subject to the declaration requirement, such as the incompatibility of official position and influence, decision making, or participation in public activities with private interests (Chapter III). Four types of declarations shall be submitted by officials and published under the law. In the beginning of January 2009, high numbers of declarations of obliged public officials were submitted and published online. The question was raised whether some data from these declarations should not be published in the interests of personal data protection.

In this regard, the Commission for Personal Data Protection presented its opinion on 15 January 2009. According to that opinion, besides the name of the declaring person, all other personal data may be published after obtaining the person's consent. The publication shall not contain any image of a signature. It is not clear enough from the opinion which data from the declarations are regarded as personal and which public.

In Access to Information Programme's opinion⁷⁷ the conditions subject to declaration are public under the explicit legal provisions. This issue has been resolved in a very similar

⁷⁷ Access to Information in Bulgaria 2008 - Annual Report, Published by Access to Information Programme, Sofia, 2009.

matter by publishing all data contained in the asset declarations of high-ranking officials. The declarations were made accessible online on the National Audit Office Web site. The reopening of this discussion without taking into consideration what has been achieved already is counter-productive with regard to the aim of the law – transparency of public figures and prevention of conflict of interests.

In April 2009, new amendments to the Act on Prevention and Exposure of Conflict of Interests were promulgated. They had been prepared without analyses of the implementation practices. Most of these amendments do not improve the regime. A step backwards with regard to transparency was allowed with the amendment of Art. 2 paragraph 25. Narrowing the obligation for avoiding conflict of interest in the administration to include only officials who perform activities related to management, decision-making, regulation, or control puts a number of officials holding expert positions outside the scope of the law.

After a heated debate, in 2006 the Bulgarian Parliament adopted the Act for Access and Disclosure of Documents and for Revealing Affiliation of Bulgarian Citizens with the State Security and Intelligence Services of the Bulgarian Army.⁷⁸ Access to Information Programme took an active part in the discussion, submitted an official statement to Parliament, and also offered suggestions for specific changes to the draft law. Finally, after a five-year regulatory vacuum, the law was adopted. For the first time, it established a procedure for passing the archives of the former state security services over to a newly established committee.

According to an explicit provision of the law, information about full-time and part-time agents (collaborators) of the secret services is not personal data. Another provision establishes that the archive of the former security services is not classified information. The newly established committee (to be formed after Parliament votes on committee members nominated from all Parliamentary groups) is responsible for reviewing and publishing documents from the archive. The Committee checks whether those holding the high-level official positions listed in the law have collaborated with the former state security services. The law regulates the right of everyone to access not only information about themselves and immediate relatives, but also guarantees access to information to those doing scientific research or working for publications. Access to documents from the archive cannot be fully restricted; instead, partial access is provided even where the interests (that is, personal data) of third parties are concerned. Critics are slightly concerned about the opportunity the law affords the Committee to withhold information in cases when disclosure might harm the interests of the Republic of Bulgaria and its international relations, or when disclosure could put someone's life in danger. The decision about whether to disclose information will be made by the Committee after considering the opinion of the secret services.

⁷⁸ Access to Information in Bulgaria 2006- Annual Report, Published by Access to Information Programme, Sofia, 2007.

Psychological and aptitude tests are regularly taken by individuals when applying and/or re-applying for a post within the Ministry of the Interior. These tests can be only taken at the Institute of Psychology, which turns it into the last and only institution that determines whether a person is psychologically healthy. In September 2001, Mr. Ivan Yonchev, a Bulgarian official, learned that the result of the test he took in order to obtain the post of police observer of the UN mission in Kosovo was negative.⁷⁹ His attempts to access the results of the psychological expertise were unsuccessful. In October 2002, he was allowed to retake the psychological test, but the results from his psychological test were again negative. As before, all his attempts to receive detailed examination results were unsuccessful. Legally assisted by Access to Information Programme, on 12 February 2003 Mr. Yonchev filed a written request under the Personal Data Protection Act to the Ministry of the Interior for access not only to the test's results, but also to his entire personal file. In response, he received a written refusal signed by the Head of Human Resources of the Ministry and grounded in the provision of Art. 1 paragraph 4 of PDPA, which gives data controllers an opportunity to abide by special regulations when processing and disclosing personal data collected for certain purposes. In this case the "special regulations" that would have been applicable were unpublished 1996 guidelines of the Minister of the Interior, according to which the personal files of all acting and retired officials are highly confidential and restricted from public access.

This refusal was appealed making – among others – the following arguments: every person has the right to access all personal data relating to him under Art. 26 paragraph 1 of the PDPA; the guidelines of the Minister could not be considered "special regulations" in the sense of Art.1 paragraph 4 of the PDPA because they had not been promulgated and thus had not normative status; and information can only be classified as "highly confidential" and constitute state secrets under the provisions of the Protection of Classified Information Act (PCIA). The list of items subject to classification under Art. 25 of PCIA does not include the personal files of Ministry of the Interior officials.

On 16 March 2003, appending the decision for the appointment of the first court hearing on the case, the Minister of Health promulgated Regulation No. 6 for the sites of specialised medical and psychological examinations and the places of periodic health check-ups.⁸⁰ The entire Section III of the Regulation describes the procedures for conducting medical and psychological check-ups of officials working for the security services, public order services, and other units of the Ministry of Defence, the Ministry of the Interior, the Ministry of Justice, and the Ministry of Transportation. Under the provision of Art. 16 paragraph 6 of the Regulation, access to documents related to check-ups is granted to the medical staff that conducted the examination, the examined person, and authorised officials from the institution that requested it. There is no doubt that Regulation No. 6 is applicable in this case, because it refers to specialised institutions for psychological diagnostics of the listed ministries, which undoubtedly includes the

⁷⁹ See <http://www.aip-bg.org/library/dela/yonchev.htm>.

⁸⁰ SG No. 35 of 16 April 2003.

Institute of Psychology of the Ministry of the Interior. In relation to the claims of confidentiality of personal files by the Ministry of Interior, the final provisions of Regulation No. 6 are of special interest. They state that Regulation No. 6 is adopted in line with the PCIA and is co-ordinated with the State Commission of Information Security.

In September 2003, seven months after the personal data request, the Sofia City Court declared the refusal of the Head of Human Resources null and void, and returned the file to the Minister for reconsideration. The ruling of the court held that even before the Minister of the Interior was explicitly defined as a personal data controller by the amendments of the Ministry of the Interior Act (MIA), he acted as such under the Rules for the implementation of MIA, because the procedure for keeping and processing personal files had been determined by him. The lawfulness of the refusal was not reviewed by the court. Instead of deciding on the request, the Minister filed a cassation appeal against the judgement of the Sofia City Court before the Supreme Administrative Court, which led to a further delay of eight months. The SAC confirmed the first-instance decision, declaring the refusal null and void and obliged the minister to reconsider the request of Mr. Ivan Yonchev.

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

The Access to Information Programme Foundation (AIP) was established on 23 October 1996 in Sofia, by journalists, lawyers, sociologists, and economists who work in the area of human rights.⁸¹ They joined their efforts to promote the right to information and initiate a public debate on relevant issues. The Access to Information Programme Foundation is a founder and member of the international Freedom of Information Advocates Network (FOIA Net). AIP facilitates the exercise of the right to access public information, it encourages individual and public demand for government-held information through civic education in the right-to-know area, and it works for government transparency at all levels, advocating for better supply of public information.

⁸¹ AIP's official Web site, at http://www.aip-bg.org/index_eng.htm.

Although it mainly deals with the right to access information it also considers related privacy issues.⁸²

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Bulgaria has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol that establishes an individual complaint mechanism.⁸³

Bulgaria is a member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁸⁴ It has adopted the CoE's Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data⁸⁵ and its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows.⁸⁶ Both conventions are part of the domestic legislation under Article 5 paragraph 4 of the Constitution and take precedence over contravening statutes. Bulgaria signed the Council of Europe Cybercrime Convention (ETS No. 185) in November 2001, but still has not ratified it.⁸⁷

* Updates to the Bulgarian Report published in the 2010 edition of EPHR have been provided by: Alexander Kashumov, Fani Davidova and Gergana Jouleva, Access to Information Programme, Bulgaria; Plamen M. Borissov, Borissov & Partners, Bulgaria..

⁸² AIP mainly: sustains a country-wide network of journalists, which collects cases of information refusals in 26 regional centers in Bulgaria; categorises and analyses cases of illegal information refusal – more than 2200 cases – monitors the practice of information provision and gives recommendations for their improvement; provides legal assistance in individual cases; gives recommendations to the central and local administration for efficient implementation of the Access to Public Information Act; promotes the right of access to information through the media, expresses expert opinion on issues of present interest, and participates in public debates on the access to information and the misfeasance at all levels; supports the activity of environmental organisations in their search for environmental information; organises workshops, seminars, and conferences on freedom of information issues; organises special training on the freedom of information for public officials, journalists, and NGOs; publishes and distributes information materials in the local and national media; publishes handbooks for the exercise of the right of access to information, as well as other printed materials that focus on particular aspects of the access to information legislation; publishes and disseminates a monthly electronic newsletter on the current national and international news, problems, and specific cases of access to information implementation; broadcasts a weekly radio show on socially sensitive issues; and participates actively in the International Freedom of Information Advocates Network.

⁸³ Bulgaria signed the ICCPR on 8 October 1968 and ratified it on 21 September 1970. It acceded to and ratified the First Optional Protocol to the ICCPR on 26 March 1992. The text of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁸⁴ Signed 10 May 1992, ratified 7 September 1992, entered into force 7 September 1992. Text and other relevant information concerning all the Conventions adopted within the Council of Europe are available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

⁸⁵ Signed 2 June 1998; ratified 20 May 2002; entered into force 1 January 2003.

⁸⁶ Signed 2 June 2010; ratified 8 July 2010; entered into force 1 November 2010.

⁸⁷ Signed 23 November 2001; ratified 7 April 2005; entered into force 1 August 2005.

REPUBLIC OF CROATIA

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Personal data protection in Croatia is primarily a constitutional category arising from Article 37 of the Croatian Constitution, which came into force 22 December 1990.¹ The Croatian Constitution regards personal data protection as part of the protection of human rights and fundamental freedoms. Everyone is guaranteed security and secrecy of personal data. Personal data may only be collected, processed and used under the conditions determined by law unless the person's consent is given. Usage of personal data contrary to the purpose of its collection is forbidden.

The Croatian Constitution was amended in 2010, but there were no changes regarding privacy and data protection.²

On 16 November 2009, the Constitutional Court of the Republic of Croatia passed a resolution rejecting³ a motion for a procedure regarding an evaluation of the constitutionality of the Personal Data Protection Act⁴ and the Act on the Amendment of the Personal Data Protection Act.⁵ The motion was introduced by a Croatian citizen who claimed that the Personal Data Protection Act wasn't approved by the special majority that the Constitution requires in order to approve "organic acts". These acts regulate rights of national minorities, constitutionally defined human rights and fundamental freedoms, electoral system, organisation and jurisdiction of state's bodies, and organisation and jurisdiction of local self-government. The Constitutional Court (ruling U-I/1242/2004) ruled that the Personal Data Protection Act should have been considered "organic" and that in turn it should have been approved with the required majority of all representatives in the Croatian Parliament. This was not the case because the Personal Data Protection Act was approved with a simple majority. However, according to the

¹ Croatian Constitution, *Official Gazette* No. 56/90, 135/97, 8/98 – revised text –, 113/00, 124/00 – revised text –, 28/01, 41/01 – revised text –, 55/01 correction. The consolidated text published in the *Official Gazette*, No. 41/01 of 7 May 2001 together with its corrections published in the *Official Gazette* No. 55 of 15 June 2001 is available in English at http://www.usud.hr/default.aspx?Show=ustav_republike_hrvatske&Lang=en.

² Decision on Amendments to the Croatian Constitution, *Official Gazette* No. 76/10. Most of the amendments entered into force on 16 June 2010; a few of them will enter into force on the day of Croatia's accession to the European Union.

³ Available in Croatian at <http://sljeme.usud.hr/usud/praksaw.nsf/Pojmovi/C12570D30061CE53C125767100308973?OpenDocument>.

⁴ Personal Data Protection Act, *Official Gazette* No. 103/03, entered into force on 4 July 2003. At http://narodne-novine.nn.hr/clanci/sluzbeni/2003_06_103_1364.html.

⁵ Act on Amendments to the Personal Data Protection Act, *Official Gazette* No. 118/06, entered into force on 10 November 2006. At http://narodne-novine.nn.hr/clanci/sluzbeni/2006_11_118_2616.html.

Court, the fact that its subsequent Amendments were passed with such a majority validated the Act in full.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Croatian Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) entered into force on 4 July 2003.⁶ The Croatian Parliament also passed a decision promulgating the Act on Amendments to the Personal Data Protection Act in 2006 (*Zakon o dopunama Zakona o zaštiti osobnih podataka*), which entered into force on 10 November 2006,⁷ and another decision concerning further amendments in 2008 which entered into force on 17 April 2008 (*Zakon o izmjenama i dopunama Zakona o zaštiti osobnih podataka*).⁸

The Personal Data Protection Act regulates the protection of personal data regarding natural persons and the supervision of collecting, processing, and using personal data in the Republic of Croatia. The purpose of personal data protection is to protect the privacy of individuals as well as human rights and fundamental freedoms in the collection, processing, and use of personal data. The protection of personal data in the Republic of Croatia has been ensured for every natural person irrespective of his or her citizenship or place of residence, and regardless of race, colour, sex, language, religion, political or other convictions, national or social background, property, birth, education, social standing, or other characteristics.

Data protection principles provided for the Croatian Personal Data Protection Act are similar to those provided for other European countries' data protection laws. Personal data must be collected and processed for only the purposes allowed by the law and about which the data subject has been expressly informed. Collection must be limited to what is necessary for achieving the stated purpose. Personal data has to be accurate, complete and up to date. Personal data has to be kept in a form limiting identification of the subject to the period necessary for the purpose for which the data is collected or further processed.

Pursuant to Personal Data Protection Act, violations of this law are punishable as misdemeanours with relatively low fines, between €2,740 and €5,480. A responsible person within a legal entity can also be fined between €685 and €1,370.⁹ Pursuant to the Penal Law, a person who, without the consent of the data subject and contrary to the conditions determined by the law, collects, processes, or uses personal data or uses such data contrary to the purpose of its collection, can be sentenced to a fine or to

⁶ Personal Data Protection Act, *supra*.

⁷ Act on Amendments to the Personal Data Protection Act, *supra*.

⁸ *Official Gazette* No. 41/08. At http://narodne-novine.nn.hr/clanci/sluzbeni/2008_04_41_1381.html.

⁹ Personal Data Protection Act, *supra* at Article 36.

imprisonment for up to six months.¹⁰ There is no reliable data on the actual penalties imposed since (i) they are administered by various local misdemeanour courts and (ii) there have been no reported criminal law penalties.

The Croatian Agency for Personal Data Protection has claimed that the Personal Data Protection Act has also been harmonised with all relevant provisions of European Union Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.¹¹ However, the European Commission in its most recent (2009) Progress Report on Croatia's preparation for EU membership stated that full alignment with the Data Protection Directive and the Council of Europe legal instruments remains to be completed.¹² The report does not specify the actions Croatia is required to complete.

Pursuant to the Personal Data Protection Act, the Government of the Republic of Croatia has also passed two regulations concerning the personal data protection domain. The first is the Regulation on the Manner of Maintaining Records on Personal Data Collections and the Form of such Records (*Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka*), which entered into force on 5 August 2004.¹³ The Regulation defines the relevant data which the records on personal data collections should contain: name of the collection; name of the data handler and its domicile, purpose of processing; legal basis for the personal data collection; categories of persons to which the data relates; type of data contained in the collection; method of collecting and storing the data; time period for collecting and using the data; name and domicile of the users of the collection; notice of import or export of data from the Republic of Croatia with either the notice of the state or international organisation and foreign user of personal data and the purpose of the export or import determined by the international treaty, law, or other regulation, or the written consent of the person to whom the data relates; and notice of the measures taken for protection of personal data. The Regulation also defines the forms for such records. As for methods, the following are provided in the form: (i) manual processing of data; (ii) automatic processing of personal data; (iii) partially automated processing with a corresponding manual file register

The second is the Regulation on the Procedure for Storage and Special Measures of Technical Protection of Special Categories of Personal Data (*Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija podataka*), which

¹⁰ Penal Law, Article 133, *Official Gazette* No. 110/97 and its corrections and amendments No. 27/98, 51/01, 111/03, 105/04, 84/05, 71/06, 110/07, 152/08.

¹¹ Directive 1995/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, 24 October 1995, available at <http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation>.

¹² See http://www.eu-pregovori.hr/files/Izvijsce/Progress_report_2009.pdf.

¹³ *Official Gazette* No. 105/04. At <http://www.nn.hr/clanci/sluzbeno/2007/2484.htm>.

entered into force on 14 October 2004.¹⁴ It defines the measures, means and conditions of storing, securing, protecting, and transferring special categories of personal data, and sets forth personal data collection measures such as maintaining and verifying the proper operation of computer and telecommunication equipment and software of the systems for maintaining special personal data collection, the security of the workspace where such equipment is located, and the authorisation of persons responsible for the implementation and supervision of such measures.

Sector-based law

So far there have been no significant developments regarding personal data protection in sector-based law, except for the law concerning the general protection of information, related to information society (information security and fight against cybercrime, information society services), electronic communications, and consumer protection.

As far as information security and the fight against cybercrime are concerned, the relevant legal framework is the Information Security Act,¹⁵ the Data Secrecy Act,¹⁶ the Regulation on Information Security Measures,¹⁷ the Regulation on Security Check-up for Access to Classified Data,¹⁸ the Regulation on the Manner of Labelling Classified Data, Contents, and Appearance of the Statement of the Executed Security Check-up and the Statement of Handling Classified Data¹⁹ and the Act on Confirming the Convention on Cybercrime.²⁰ The provisions of the Convention on Cybercrime have been implemented accordingly in the Penal Law (Articles 223, 223a, 224, 224a and 224b) and Criminal Proceedings Act.²¹

With regard to Information Society Services, the relevant legal framework is provided for under the Electronic Signature Act,²² the Regulation on the Measures and Procedures of the Usage and Protection of the Electronic Signature and Advanced Electronic Signature, Certification System, and Obligatory Insurance of the Service Provider, and the Issuing

¹⁴ *Official Gazette* No. 139/04.

¹⁵ *Official Gazette* No. 79/07.

¹⁶ *Id.*

¹⁷ *Official Gazette* No. 46/08. At <http://www.nn.hr/clanci/sluzbeno/2008/1547.htm>.

¹⁸ *Official Gazette* No. 72/07. At <http://www.nn.hr/clanci/sluzbeno/2007/2237.htm>.

¹⁹ *Official Gazette* No. 102/07. At <http://www.nn.hr/clanci/sluzbeno/2007/2985.htm>.

²⁰ *Official Gazette* No. 173/03.

²¹ Penal Law, *supra*.

²² *Official Gazette* Nos. 10/02 and 80/08. At http://narodne-novine.nn.hr/clanci/sluzbeni/2002_01_10_242.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2008_07_80_2604.html.

of Qualified Certificates,²³ the Electronic Commerce Act²⁴ and the Electronic Public Document Act.²⁵

Electronic Communications are regulated by: the Electronic Communications Act,²⁶ the Telecommunications Act,²⁷ the Act on the Amendments of the Telecommunications Act,²⁸ the Regulation on Awarding Addresses and Numbers,²⁹ the Regulation on the Transferability of Numbers,³⁰ the Regulation on the Manner and Conditions of the Prevention of Fraud in the Provision of Electronic Mail Services,³¹ the Regulation on the Directory and Service Providing Information about Subscribers,³² the Regulation on Universal Services in Electronic Communications,³³ the Regulation on the Working Procedure of the Interior Organisational Unit for Consumer Rights Protection,³⁴ the Regulation on the Manner and Conditions of the Performing the Activities of Electronic Communication Networks and Services,³⁵ the Regulation on the Manner and Conditions of the Access and Joint Usage of Electronic Communication Infrastructure and Related Equipment,³⁶ the Addressing Plan,³⁷ the Numeration Plan,³⁸ and the Regulation on the Obligations in the Area of National Security of the Republic of Croatia for Legal and Physical Persons in Telecommunications.³⁹

²³ *Official Gazette* No. 54/02. At <http://www.nn.hr/clanci/sluzbeno/2002/1023.htm>.

²⁴ *Official Gazette* Nos. 173/03 (http://narodne-novine.nn.hr/clanci/sluzbeni/2003_10_173_2504.html), 67/08 (http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_67_2228.html) and 36/09 (http://narodne-novine.nn.hr/clanci/sluzbeni/2009_03_36_796.html).

²⁵ *Official Gazette* No 150/05.

²⁶ *Official Gazette* No. 73/08.

²⁷ *Official Gazette* Nos. 122/03, 158/03 and 60/04. See <http://www.mmtpr.hr/UserDocsImages/04-Zakon-TK.pdf>.

²⁸ *Official Gazette* No. 70/05. See <http://www.nn.hr/clanci/sluzbeno/2005/1373.htm>.

²⁹ *Official Gazette* No 154/08. See http://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_154_4205.html.

³⁰ *Official Gazette* No.42/09. See http://narodne-novine.nn.hr/clanci/sluzbeni/2009_04_42_954.html.

³¹ *Id.* See http://narodne-novine.nn.hr/clanci/sluzbeni/2009_04_42_952.html.

³² *Official Gazette* No. 23/09. See http://narodne-novine.nn.hr/clanci/sluzbeni/2009_02_23_517.html.

³³ *Id.* See http://narodne-novine.nn.hr/clanci/sluzbeni/2009_02_23_516.html.

³⁴ *Official Gazette* No. 10/09. See http://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_10_239.html

³⁵ *Official Gazette* No. 154/08. See http://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_154_4202.html.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Official Gazette* No. 64/08. See http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_64_2178.html.

Consumer Protection is regulated by the Consumer Protection Act.⁴⁰

The only acts and regulations that may be providing for the protection of personal data are those that entered into force after the entering into force of the Personal Data Protection Act in 2003, and some improvements could be found in the acts, amendments, and regulations promulgated after the PDPA amendment in 2008. These include the Electronic Commerce Act,⁴¹ Electronic Signature Act,⁴² Electronic Communications Act,⁴³ Regulation on Awarding Addresses and Numbers,⁴⁴ Regulation on Transferability of Numbers,⁴⁵ Regulation on the Manner and Conditions of the Prevention of Fraud in the Provision of Electronic Mail Services,⁴⁶ Regulation on the Working Procedure of the Interior Organisational Unit for Consumer Rights Protection,⁴⁷ etc. For instance, the above-mentioned Regulation on the Transferability of Numbers specifies the form of the Request for the Transfer of a Phone Number, which includes the following statement: "In addition to this, the Subscriber consents explicitly by his/her signature on this request that his/her personal data may be used for the purpose of enabling the service of the transfer of a phone number and may be collected, processed and exchanged between the operator and the Agency. By signing this request, the Subscriber confirms that he/she has been thoroughly informed and consents to the conditions of the number transfer stated in this request".

However, telecommunications, consumer protection, and information society may be considered as essential sectors in personal data protection, whereas privacy protection in other sectors, e.g. health and social welfare, labour, economy and entrepreneurship, culture, agriculture, science, education, sports, regional development, construction, tourism, interior affairs, foreign affairs, or defence have not been specifically tackled by law. Perhaps some contributions to the sector-based law may be seen in a specific law related to credit institutions and their clients, namely the Credit Institution Act,⁴⁸ which covers financial, insurance, and banking business in Croatia.

⁴⁰ Official Gazette No. 79/07. The Act is also available in Croatian at <http://www.nn.hr/clanci/sluzbeno/2007/2485.html>.

⁴¹ *Supra*. In particular, see amendments in the *Official Gazette* Nos. 67/08 and 36/09.

⁴² *Supra*. In particular, see amendments in the *Official Gazette* No. 80/08.

⁴³ *Supra*.

⁴⁴ *Supra*.

⁴⁵ *Supra*.

⁴⁶ *Id*.

⁴⁷ *Supra*.

⁴⁸ *Official Gazette* Nos. 117/08, 74/09 and 153/09.

DATA PROTECTION AUTHORITY

As defined by the Personal Data Protection Act, the competent body for the protection of personal data in Croatia is the Agency for Protection of Personal Data (hereinafter the Agency).⁴⁹ The seat of the Agency is in Zagreb. The scope of the Agency is defined in Articles 32 and 33 of the Act, encompassing both administrative and specialised tasks related to personal data protection. The Agency is an independent body with public authority and is responsible to the Croatian Parliament, meaning (i) that the organisation and method of work of the Agency is determined by its statute, which is confirmed by the Croatian Parliament; (ii) that the director and the assistant director of the Agency are appointed and recalled by the Croatian Parliament on the suggestion of the Government of the Republic of Croatia; and (iii) that the Agency submits a written report on its activities to the Croatian Parliament at its request and at least once a year.

The Agency plays a central role in data protection in the Republic of Croatia. Pursuant to Article 32 of the Data Protection Act its tasks include: supervision of the implementation of personal data protection; indication of possible violations noted while collecting personal data; composition of a list indicating national and international organisations which have adequately regulated personal data protection; maintenance of the Central Registry of Personal Data Collections, which is publicly available;⁵⁰ resolution of requests regarding possible violations of rights guaranteed by Personal Data Protection Act. The Central Registry contains information concerning all personal data collections, namely: the name of the collection, the name and address of the person maintaining the collection, the purpose of processing the data, the legal basis for the personal data collection, the categories of persons the data covers, the type of data contained in the collection, the method of collecting and maintaining the data, the time period that the data will be maintained and used, the name and address of the user of the collection, notice of import or export of the data outside the Republic of Croatia including the user and purpose, and notice of the measures that have been implemented for the protection of personal data.⁵¹ Pursuant to the Annual Reports of the Agency for the years 2008⁵² and 2009,⁵³ the Central Registry contains 11,908 personal data collections (during the year 2008 a total of 2,230 personal data collections were registered with the Agency and 3,604 followed up in 2009).

In its supervisory activities the Agency is entitled to act *ex officio* and pursuant to individual requests to establish whether data subjects' rights have been violated during personal data processing. Pursuant to Article 34 of the Personal Data Protection Act, if

⁴⁹ <http://www.azop.hr>.

⁵⁰ <https://registar.azop.hr>.

⁵¹ *Id.*

⁵² <http://www.sabor.hr/Default.aspx?art=28265&sec=2878>.

⁵³ <http://www.sabor.hr/Default.aspx?art=34100&sec=3140>.

during supervision activity the Agency determines there have been violations of the law regulating the protection of personal data, it has the right to notify or warn the data controller and to issue a decision: ordering rectification of any irregularities; temporarily prohibiting the processing of personal data; ordering erasure of personal data; prohibiting the export of data from the Republic of Croatia or the usage of such data by other persons; and prohibiting processing of data by persons who do not fulfil the conditions of the law. Pursuant to the Annual Report for the year 2008 the Agency has supervised 626 cases either pursuant to the claims of other parties or *ex officio*. The most common violations of the Personal Data Protection Act relate to the registration of personal data collections, the legal grounds for collection and processing of personal data, the purpose and scope of data collection, a lack of protection of the data, the duration of the usage and erasure of the data, and delivery of the data to the users and usage for the purposes of marketing.

The Croatian Personal Data Protection Agency is also tasked with raising awareness regarding the importance of effective data protection and is cooperating with numerous ministries, authorities, NGOs and other bodies, such as the Ministry of Science, Education, and Sports and the Croatian Chamber of Economy. In order to commemorate European Data Protection Day on the 28th January, the Agency organises annual Regional Round Tables addressing data protection. This year, in cooperation with a distinguished NGO, Society for Consumers' Protection Potrošač', two presentations were given: "Identity and data protection for users of financial and banking services" and "Identity and data protection for users of telecommunication services." These presentations aimed to raise overall awareness and knowledge in a practical manner from the perspective of an individual. The Agency also organises numerous educational seminars (approximately 12 per year) for both individuals and data controllers concerning privacy and data protection in the Republic of Croatia. On 25 November 2010 the national Conference on Privacy ("Privacy 2010") was held in Zagreb.⁵⁴

The Agency proactively participates in international conferences and working parties as a member or observer, thus contributing to the development of data protection and aiding in the harmonisation of the Croatian legal framework of personal data protection with European norms and standards. It also ensures the fulfilment of stipulated obligations stemming from international conventions signed and ratified by the Republic of Croatia.⁵⁵

The Agency cooperates professionally with numerous agencies from EU member states, especially the Austrian, Slovenian, Hungarian and Spanish agencies that work on data protection.

The Croatian Personal Data Protection Agency has full member status in the so-called Spring Conference of the Commissioners for personal data and privacy protection, and in

⁵⁴ For more information see <http://www.case.hr/konferencije/privatnost2010>.

⁵⁵ See Section "International Obligation & International Cooperation," *infra* in this report.

the Working Group on Police and Justice. Thus it is facing the new field of data protection in connection with police and law enforcement.

The Agency has showed its ability to conduct investigations in response to complaints. In the case of a complaint of a client against a telecommunications firm, the firm provided the Agency for Protection of Personal Data with the customer data logs related to the personal data of the plaintiff. The logs for the previous six months were extracted from the aforementioned records and it was determined that the logs were made during the client's (plaintiff's) calls from his number to the firm's Customer Service line. The Agency discovered that the firm's employees were accessing the complainants' records in the Customer Service department even when he was not calling the department. The Agency ruled that the firm was at fault and had to install an internal control and monitoring system to monitor when and how staff members access client files. The Agency also required the firm to change the provisions contained in the "Customer Data Protection Procedure" to allow users to control periodically the processing carried out by the firm.

Major privacy & data protection case law

The relevant case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.⁵⁶

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Presently, communications surveillance must be authorised by the Supreme Court or by the investigatory judges in criminal proceedings for which the rights and liberties granted by the Constitution may be suspended, for the maximum period of seven months.

However, privacy is insufficiently protected under the current legal regime, and the supervision of the powers granted to the police and secret services is weak. For example, it is impossible to determine how the data gathered for the analysis by the police in the past ten years are kept and used. Also, there is no qualified supervisory body except for intelligence agencies authorised to perform the supervision of the Operative Technical Centre for Telecommunications Surveillance (OTC), and critics claim that the supervision by the Parliamentary Committee for Interior Policy and National Security and the Council for Civil Supervision of the Security and Information Agencies has been ineffective.

According to Croatian law, with the exception of legal wiretapping, if the voice of a person is recorded, he/she must be informed, so phone companies usually inform their

⁵⁶ *Cfr.* Sections "Online social networks and virtual communities", "Cybersecurity", "Workplace Privacy", *infra* in this report.

users about such a possibility via their pre-recorded messages. The evidence collected by secret recordings without informing the person that he/she is being recorded is not accepted in court proceedings.

National security legislation

The director of the Operative Technical Centre for Telecommunications Surveillance (OTC), the authority responsible for the legal interception (LI) of telecommunications services, has issued an instruction to the telecommunications operators and municipal and county courts to direct all orders to collect telecommunications data to the police or the OTC, and not to the telecommunications operators themselves. However, the opinion of the Supreme Court is that the courts have no obligation to adhere to the instructions from the intelligence community.

According to some experts, the problem is also in the opinion or the interpretation of the director of OTC that the secret surveillance of telecommunications pursuant to the Intelligence System Act should be considered equally admissible as the evidence that the court may request in criminal proceedings. The problem, however, is not in the information thus collected for the purposes determined by the court in the proceedings, for instance somebody's displacement in the past, as the right to privacy can be limited by a valid court order in criminal proceedings.

Whereas previously the courts issuing surveillance orders could be supervised by higher courts, the OTC is practically unsupervised (except for the formal supervision by the Parliamentary Committee) and almost uncontrollable in its collection of private data, which may even be used as valid evidence in courts, in case of criminal proceedings which have not yet been initiated.

Data retention

In the last year and a half, the Croatian authority responsible for the legal interception of telecommunications services (*Operativno-tehnički centar za nadzor telekomunikacija*) started exercising its rights towards the telecommunications operators in order to implement the Ordinance of the Government of the Republic of Croatia on Obligations of Telecommunication Operators in the Area of National Security (*Uredba o obvezama iz područja nacionalne sigurnosti RH za pravne i fizičke osobe u telekomunikacijama*).⁵⁷ The Ordinance requires fixed and mobile telephone operators, Internet service providers, email providers, Internet telephony providers, and other data communication providers to store extensive data on all electronic communications for 12 months, including, but not limited to, the IP address, caller and recipient phone numbers, date and duration of the communication, type of service, IMSI and IMEI, geographical location, and other data. Providers' implementation costs are not refunded.

The courts can also request that operators provide such data, e.g. from computers and mobile phones, which can be used in criminal proceedings in a court of law.

⁵⁷ *Official Gazette* No. 64/08 from 4 June 2008. The Ordinance entered into force on 4 June 2008.

National databases for law enforcement and security purposes

No specific information has been provided under this section.

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

According to experts from the National CERT (Computer Emergency Response Team) of CARNet (Croatian Academic Research Network), the most pervasive form of cybercrime in Croatia is phishing, and it is usually committed by foreign criminals.

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

In cases of violation of consumer privacy, the Agency has endorsed the following rule of consumer identity, provided under the Consumer Protection Act,⁵⁸ Art. 7 paragraph 3: "The Merchant is prohibited from providing the personal data of the consumer to any third person without prior explicit and written permission of the consumer, except if he/she is obligated to do it by the law or the decision of a competent authority." For a violation of this rule, the merchant that has provided a third person with the data of a consumer without prior consent and authorisation can be fined from €2,055 to €13,698 (Article 145 paragraph 1).

Cybersecurity

No specific information has been provided under this heading.

Online behavioural marketing and search engine privacy

No specific information has been provided under this heading.

Online social networks and virtual communities

The National CERT has published a brochure designed to protect privacy on Facebook.⁵⁹

The Agency for Protection of Personal Data has dealt with some cases concerning the disclosure of personal information online by different actors. For example, a Croatian NGO published a person's personal data on its Web page without his consent, thus violating Article 7 of the Personal Data Protection Act. Following the data subject's complaint to the Agency, the NGO was ordered to erase the plaintiff's photograph and personal data from the Web page within eight days. On 16 November 2007, the Agency

⁵⁸ *Supra*.

⁵⁹ Available in Croatian at http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku.

decided the case of a person whose personal data was unlawfully disclosed on a blog opened by another person. The service provider hosting the blog was ordered to remove the specific contents of the blog relating to the personal information within eight days.

In 2010, the journalist and blogger Damir Fintić from Vukovar, Croatia, was convicted of slander and ordered by court to pay a fine of HRK250,000 (approx €34,000) to the former mayor of Vukovar, Vladimir Štengl, and his wife for psychological distress. In 2005, Fintić published an anonymous letter on his site, Vukovarac.net, that provoked 300 citizens of Vukovar into writing negative comments about the Štengls. Offended, they sued Fintić because he did not remove the letter and did not delete the readers' comments. They also asked Fintić to provide them with the name of the letter's author. He refused to remove the contents from his Web page, claiming that according to the law a Web page was not legally considered a medium, and it did not have a publisher or editor. The service provider of the domain was notified of the Web page's slanderous content, which led to the page's being taken down. The author of the anonymous comment has never been sued.

Certain prominent human rights activists, journalists, and academics have made public requests in the media that the users of public Internet fora should not be granted the right to remain anonymous while posting their comments online. The policy of the largest Internet forum in the region⁶⁰ is to remove all anonymous posts upon the request of a person or firm that considers the information slanderous, untrue, or in any way harmful to their dignity and reputation (which is understood to be in line with the Vukovarac.net case). On the other hand, the forum also protects the anonymity of its users. The idea behind this policy is that all those who want their information to be considered valid and true should publicly disclose their true identity, because the firms and persons that are not anonymous are not granted the refuge of anonymity while commenting or providing information about themselves or the others. Theoretically, it would be possible to start criminal proceedings against an anonymous user by reporting the issue to the police, who can then search for the IP addresses of such users and track them down, but in practice it is the owner of the Internet site who is responsible for anonymous comments. The issue of the right to remain anonymous while posting public comments on the Internet has not yet been tackled by the government, and such comments have essentially become the legal responsibility of the owner of the Web site or domain.

Online youth safety

On its web pages, the Office of the Ombudsman for Children has issued a short note in called "Seven Golden Rules for Safe Chatting and SMS-Messaging."⁶¹

⁶⁰ <http://www.forum.hr/>.

⁶¹ See <http://www.dijete.hr/hr/preporuke-pravobraniteljice-mainmenu-81/zatita-interesa-djece-razno-mainmenu-82.html>.

TERRITORIAL PRIVACY

Video surveillance

The penal code provides for sanctions against persons who collect images or make videos of persons without their consent (via mobile phones, cameras, etc), but there have been no significant cases.

Video surveillance exists in many locations in large cities, usually in front of banks, embassies, and other important sites, and the evidence thus collected can be used in courts, as everybody is supposed to be aware of the fact that they are being recorded. Such evidence has actually been used in some cases of bank robberies. Video surveillance has been introduced in some schools, usually private schools with the permission of the students' parents, but its introduction in state schools has usually been opposed by the public.

Location privacy (gps, mobile phones, location based services, etc.)

The OTC and the police have the legal right to locate people with GPS and to supervise mobile phones, but so far there has been no obligation to register unregistered (non-subscription) mobile phones.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

The introduction of biometric passports has been proposed, as a part of the agreement to lift US visa requirements for Croatian citizens, but this has not yet been implemented.

National id and smart cards

The introduction of new IDs has suppressed the use of the citizen's identity number (MBG), which can be disclosed and processed only with the permission of the person. Instead, a new number has been introduced for identification of personal bank accounts and other financial transactions, called OIB (personal identification number), which can be accessed and searched online, or received via mobile phone.

In the context of collecting information for petitions or referenda the Agency for Personal Data Protection has concluded that the request for provision of the former unique citizen's number (MBG) or any other identification number (OIB) is neither necessary nor adequate for the purpose of data collection (Article 6 paragraphs 1 and 2 of the Act).

Social Security IDs containing data about illnesses and medication have been proposed as a part of the new e-Health project, which is to be implemented in 2011.

Rfid tags

No specific information has been provided under this section.

BODILY PRIVACY

No specific information has been provided under this section.

WORKPLACE PRIVACY

Critics have called for a review of workplace surveillance practices, and for regulatory guidance after a number of cases. One of the leading cases involved an employee of the Zagreb branch of Siemens PLC who was accused of using a company computer to visit a football fan forum where he used foul language in conversation with members of the opposing team. One of these members found his IP address, and informed the Siemens board of the event. This led to an investigation where the employee was placed under surveillance for five months, during which time all of his computer activities were monitored. The investigation concluded that he had violated the corporate rules regarding the use of inappropriate language.

HEALTH & GENETIC PRIVACY

Medical records

In 2008, the Croatian publisher Ivo Pukanić was expelled from the Croatian Journalists' Association for having published his wife's medical records in his weekly newspaper, *Nacional*. The Council of Honour of the Croatian Journalist Association has been contacted by the Media Committee of the Office for Gender Equality and the Parliamentary Committee for Human Rights and National Minority Rights regarding this case.⁶²

Genetic identification

No specific information has been provided under this section.

FINANCIAL PRIVACY

According to Article 7, paragraph 1 of the Personal Data Protection Act, personal data may be collected and processed only with the data subject's consent or if provided for under the law. Croatian banking law provides for the possibility that the bank associations may exchange information about the credit ratings of their clients and the processing and exchange of personal data, and does not require specific approval by the client. This permits wide-scale data sharing, as was encountered in one legal case where personal data had been exchanged among banks and other institutions, as well as among the employees of the bank, without prior written permission or any other approval; the Agency for the Protection of Personal Data dismissed the complaint under Croatian banking law.

In the previous Bank Act,⁶³ Article 99 paragraph 3 defined the obligation to preserve bank secrets, which included the personal data of clients found while doing business with them and providing banking services, as well as data about clients' personal account statements. According to the Bank Act, the data could be disclosed in the following cases:

⁶² Cfr. Section "E-government & Privacy," *infra* in this report.

⁶³ *Official Gazette* Nos. 84/02 and 141/06.

- 1) if the client gives written permission for the disclosure of certain confidential data;
- 2) if the confidential data disclosure is necessary for the collection and determination of facts in criminal proceedings or the proceedings leading to it, in the case that such a disclosure has been requested or ordered by a competent court;
- 3) if the confidential data are disclosed for the purposes of the Office for the Prevention of Money Laundering, on the basis of law regulating the prevention of money laundering;
- 4) if the disclosure of confidential data is necessary for determining a legal relationship between a bank and a client in litigation, and if a competent court has requested or ordered it in writing;
- 5) if the confidential data are disclosed for the purpose of proceedings concerning property or inheritance, on the basis of a written request of a competent court;
- 6) if the disclosure of confidential data is necessary for the execution of a foreclosure of property of a bank's client, and if it has been requested or ordered by a competent court;
- 7) if the confidential data are disclosed to the Croatian National Bank, Foreign Currency Inspectorate or other supervisory body for the purpose of supervision within their legal competence, on the basis of a written request;
- 8) if the confidential data are disclosed to a legal person, organised in an adequate form, that may be founded by banks with the purpose of collecting and providing data about the total amount, types and punctuality of fulfilling the obligations of physical and legal persons acquired on any basis;
- 9) if the confidential data are necessary for the tax bodies in the proceedings carried out within their legal authority, and disclosed upon their written request;
- 10) if the confidential data are disclosed for the purposes of the institutions insuring the deposits, on the basis of the law regulating the insurance of deposits.

This Article also permits the existence of the so-called *HROK* or the Croatian Credit Information Registry, which contains personal data about clients who have sought credit, as well as their credit ratings, any blacklists the individual may be on, etc. However, the law did not clearly define the purpose of the data collection as making a blacklist of customers who have failed to meet their obligations, including their personal data – it only defined the purpose as the determination of the amount and type or the obligations of legal and physical persons and their punctuality in fulfilling them.

In the new Credit Institution Act, Article 169 paragraph 3 provides for the possibility of disclosing a bank secret in a much-expanded list of cases:

- 1) if the client gives written permission for the disclosure of certain confidential data;
- 2) if it enables the realisation of interests of a credit institution for selling the client's claims;

- 3) if the confidential data are disclosed to the Croatian National Bank, Foreign Currency Inspectorate or other supervisory body for the purpose of supervision within their legal competence;
- 4) if the confidential data are exchanged within a group of credit institutions for the purpose of risk management;
- 5) if the confidential data are disclosed to a legal person created@@ in order to collect and provide data about the financial solvency of legal and physical persons, in accordance with a special law;
- 6) if the confidential data are exchanged among credit and/or financial institutions about clients who have not fulfilled their obligations in time, and the confidential data are disclosed to a legal person created@@ for the purpose of collection and exchange of such data;
- 7) if the disclosure of confidential data is necessary for the collection and determination of facts in criminal proceedings or proceedings leading to a criminal case, under the condition that it be requested in a written form or ordered by a competent court;
- 8) if the disclosure of confidential data is necessary for the execution of foreclosures or bankruptcy proceedings over the property of the client, inheritance or any other legal proceedings concerning property, if it is requested or ordered in written form by a competent court or a public notary in the execution of the duties entrusted to them on the basis of the law;
- 9) if the interests or obligations of credit institutions or clients require the disclosure of confidential data with the purpose of clarifying the legal relationship between the credit institution and a client in a lawsuit, arbitration or conciliation procedures.
- 10) if the confidential data are disclosed to the Office for the Prevention of Money Laundering, on the basis of a law regulating the prevention of money laundering and financing of terrorism;
- 11) if the confidential data are disclosed to the Office for the Prevention of Corruption and Organised Crime on the basis of the law regulating the prevention of corruption and organised crime;
- 12) if the confidential data are necessary for the tax bodies in the proceedings carried out within their legal authority, and disclosed upon their written request;
- 13) if the confidential data are disclosed for the purposes of the institutions insuring the deposits, on the basis of the law regulating the insurance of deposits;
- 14) if the state of the account clearly shows insolvency, and confirmation is requested in order to prove the reasons for opening the bankruptcy proceedings;
- 15) in order to disclose the data to insurance companies in the procedure of securing the claims of a credit institution;

- 16) disclosure of data in concluding legal deals that have an effect of securing the credit institution's claims, such as credit derivatives, bank guarantees and other similar business;
- 17) data disclosure with the written consent of the credit institution board to the owner of the qualified stake of that credit institution, person that intends to acquire a qualified stake in a credit institution, person with which a credit institution merges or is acquired by, legal person that intends to take over a credit institution as well as auditors, legal and other experts authorised by the owner of the qualified stake or a potential owner;
- 18) disclosure of data necessary for carrying out the activities of a credit institution, which are subject to externalisation, if the data are disclosed to the providers of such externalisation;
- 19) if the credit institution providing services of depositing and administering financial instruments on clients' behalf, including custody, delivers to a credit institution which is the issuer of intangible securities, on its request, the data on the owner of such securities;
- 20) if the confidential data are disclosed on the basis of a written request to social care centres within their legal authority, for the purpose of carrying out measures for the protection of the rights of minors (persons younger than 18 years) and persons under custody;
- 21) and if it is provided by other laws.

It is clear from this that the number of provisions for the disclosure of data has doubled, including the provisions for the creation of explicit blacklists of insolvent or overdue users of bank loans, special provision for persons under custody or whose property is under foreclosure or bankruptcy proceedings. The last line provides for the possibility of any other law that could demand the disclosure of private data, and the only extra protection is given in the paragraph 5 of the same Article, providing that a credit institution is obliged to ascertain that a customer has given his/her written permission for the processing of their personal data (above-said paragraph 3 of the same Article) in a separate document, upon conclusion of each contract concerning banking and/or financial services.

E-GOVERNMENT& PRIVACY

There are large, ongoing e-government projects in Croatia, notably the e-Firm project, e-Health and e-Justice. So far, there have been no legal cases emerging from these projects, as the whole issue is rather new (the implementation of some elements of e-government began in 2007).

As far as e-Health is concerned, the introduction of e-prescription and e-treatment orders may jeopardise the privacy of patients and the right to protection of their health data. Critics have claimed that with the implementation of e-prescriptions the doors will be wide open for all kinds of abuse of data about patients, whether they are politicians, businessmen, or just ordinary citizens. It will be easy to get to the protected information simply by knowing an individual's OIB (PIN – Personal Identification Number). All

information could be available over the phone, just by posing as a pharmacist or an employee in a hospital, claiming to a doctor that you there are problems in reading a specific e-prescription or e-medical records.

Critics have also argued that because of a lack of adequate safeguards, the Croatian Central Medical Information System (CEZIH),⁶⁴ infringes Article 37 of the Constitution, provisions of the Personal Data Protection Act, as well as the Convention 108 of the Council of Europe because citizens' personal medical records were included within the system without any notification or consent. The concern now is that with this central information system in place, information about the patients will circulate widely, including among the pharmacies, as well as public and perhaps even private institutions.

The Minister of Health has claimed that the system has been tested and ready and that the system of data protection (HL7) that has been implemented in accordance with principles from both the WHO and the European Commission. The Minister has also stressed that because there are two identical servers – in Rijeka and in Zagreb -- there is no risk of data loss. However, the president of the Chamber of Pharmacists has said that the system has not been fully functional so far, as there have been difficulties in accessing the system due to its sluggishness and other communication problems.

OPEN GOVERNMENT

No specific information has been provided under this section.

RECENT FACTUAL DEVELOPMENTS

A hot topic recently in Croatia was the anonymous and unauthorised publication on the Internet of the War Veterans Registry.⁶⁵ The War Veterans Registry was not publicly available and it contains various personal data on approximately 500,000 persons with the status of war veteran. Its publication was a highly discussed political subject in recent years due to requests for its publication, and claims that the number of war veterans and rights pertaining to them had been overinflated.

The Agency issued an opinion stating that the publication of the registry is a violation of personal data protection regulations, since there is no prior consent by the data subjects to the publication and no law that would allow the publication of such registry. The Agency clearly stated that the reasons of public interest are not above the relevant data protection laws.

The publication caused a crackdown by the authorities, which started a criminal investigation on the persons who made the registry public, though so far without results.⁶⁶

⁶⁴ For further info see <http://www.cezih.hr>.

⁶⁵ <http://www.registarbranitelj.com>.

⁶⁶ http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/features/2010/04/13/feature-02.

The Croatian authority responsible for legal intercept of telecommunication services, citing security reasons and the fight against crime, recently requested that the Government issue regulations requiring mobile phone operators to register their pre-paid mobile phone users. Non-registered numbers would cease to be valid. This caused resistance from the mobile phone operators and the public. Mobile phone operators are currently negotiating and trying to postpone adoption of the legislation needed for the abovementioned. Currently it seems that such plans will be put on hold until 2011 or 2012. According to the Agency, upon adoption of the necessary legal framework, registration of pre-paid mobile phone users itself will be possible and legitimate and will not be in conflict with data protection regulation. The draft of the legal framework is not yet publicly available.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

Some NGOs have cooperated with the Personal Data Protection Agency and there are many NGOs active in the field of human rights and consumer protection. Among them, the largest and most influential are Consumer (*Potrošač*), Croatian Helsinki Committee and others, which have done advocacy work on privacy as a part of their regular activities.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Croatia has been party to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol, which establishes an individual complaint mechanism.⁶⁷

Croatia, as a member state of the Council of Europe, has accepted the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.⁶⁸ Convention 108 also established the Consultative Committee of the Convention for the protection of Individuals with regard to automatic processing of personal data (T-PD). The Republic of Croatia has voting rights in the work of the T-PD.

⁶⁷ Croatia has been part to the ICCPR since 12 October 1992 and acceded to its First Optional Protocol on 18 October 1995. The text of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁶⁸ See <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?MA=10&CM=7&CL=ENG>.

The Republic of Croatia has signed an agreement with Eurojust on 9 November 2007 and has been exchanging opinions and information while cooperating closely on personal data issues ever since.⁶⁹

EUROJUST is an EU body established in 2002 and its main objectives are reinforcing the effectiveness of cooperation and coordination between competent bodies of the EU Member States in terms of investigation of serious cross-border organised crime and prosecution procedures as well as in terms of providing more complex forms of international legal aid in criminal matters and for the purpose of accelerating of extradition procedures.

The Republic of Croatia became a member state of the International Conference of Data Protection and Privacy Commissioners in 2008. The Republic of Croatia is also a member state of Central and Eastern European Data Protection Authorities (CEEDPA).

*Updates to the Croatian Report published in the 2010 edition of EPHR have been provided by: Ivan Gjurgjan, Gjurgjan and Šribar Radic, Croatia; Jan Klasinc, Croatian Institute for Public Administration - iDEMO Institute for Democracy), Croatia.

⁶⁹ The text of the Agreement is available at http://www.eurojust.europa.eu/official_documents/Agreements/EurojustCroatiaAgreement_9nov07.pdf.

REPUBLIC OF CYPRUS

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Constitution of the Republic of Cyprus¹ was established in July 1960 and has the following two provisions regarding privacy:

Article 15: (1) Every person has the right to respect for his private and family life; (2) There shall be no interference with the exercise of this right, except such as is in accordance with the law and is necessary in the interests of the security of the Republic, constitutional order, public safety, public order, public health, public morals, or the protection of the rights and liberties guaranteed by this Constitution to any person.

Article 17: Every person has the right to respect for, and to the secrecy of, his correspondence and other communication, if such other communication is made through means not prohibited by law.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

While the right to respect for the individual's private and family life has been enshrined in the Constitution since the Republic of Cyprus' independence in 1960, laws relating specifically to data protection are a relatively new development, with the first law specifically relating to the processing of personal data enacted as recently as 2001.

The Processing of Personal Data (Protection of Individuals) Law of 2001² (the "Law") came into force on 23 November 2001. The Law was introduced in the context of the harmonisation process with the European Data Protection Directive.³ The Law was amended again in 2003 in order to better align domestic legislation with Directive 95/46/EC.

The Law applies to living natural persons and covers automated, partially automated, and in some cases, non-automated processing operations, in both public and private sectors. It defines the rights and obligations of controllers and data subjects, and sets the parameters

¹ Constitution of the Republic of Cyprus, of July 1960, non-official English version available at <http://kypros.org/Constitution/English/>.

² Law No. 138(I)/2001.

³ Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

for lawful processing of data. In order for the Law to be applicable, a data controller resident in the Republic must carry out the processing of personal data. The Law also applies at a place where Cyprus law is applied by virtue of public international law or by a data controller who is not resident in the Republic, who, for the purpose of processing personal data, has recourse to automated or other means existing in the Republic, unless they were used only for the purpose of transmitting the data through the Republic. The Law does not apply to the processing of personal data that is carried out by a natural person for the exercise of exclusively personal or domestic activities.⁴

The collection and processing of sensitive data is generally prohibited, although there are a number of exceptions to this general principle. Sensitive personal data may be processed provided that the data subject has explicitly consented to it. Consent from the data subject may not be obtained unlawfully or be contrary to morals, custom, or a specific law.

The Law provides that the Council of Ministers can issue regulations providing for the processing of sensitive personal data in cases other than those mentioned above, when there are important reasons of public interest. No such regulation has been issued so far.

The international transfer of personal data in itself is an activity which falls within the definition of "processing of personal data" as provided under Section 2 of the Law.

By virtue of Section 9 of the Law, the transfer of processed data, or data that will be processed when they are transferred to another country which is not an EU member state, is allowed only when the COPPD has granted a permit for such transfer. The COPPD will only grant the permit if he thinks that the other country ensures a sufficient level of protection.

There is a general obligation under the Law for the data controller to notify the DPA in writing about international transfers. The data controller is discharged from the obligation to submit that notification in cases where a transfer is performed solely for purposes directly connected with the work to be done, and is necessary for the fulfilment of a legal obligation or the performance of a contract, but provided that the data subject has been previously informed.

However, insurance, pharmaceutical, and data provider companies as well as financial institutions such as banks and credit cards issuers, are not excluded from the obligation to notify.

The following factors may be accepted by the COPPD as sufficient guarantees that ensure a satisfactory level of protection of the transferred data to the recipient third country as to grant a transfer license: 1) standard contractual clauses (such clauses must be submitted to the COPPD for approval so that a licence can be issued before any international transfer of personal data takes place); 2) the "Safe Harbour" Agreement (transfer of data to the United States may be allowed if the company to which the data is transferred

⁴ Article 4, Directive 1995/46/EC.

certifies itself as complying with the Safe Harbour Agreement; 3) binding corporate rules (they can be used after being approved in advance by the COPPD).

Sector-based laws

The Regulation of Electronic Communications and Postal Services Law of 2004⁵ was enacted in April 2004. The Law, which transposes the provisions of the Directive on Privacy and Electronic Communications (2002/58/EC),⁶ regulates the secrecy of communications and the use of traffic and location data, telephone directories, and unsolicited communications. It particularises and complements the provisions of the Data Protection Law, and provides for the protection of the legitimate interests of subscribers of electronic communications networks and services who are legal persons.

The Law provides for the appropriate technical and organisational measures to be taken by providers of publicly available electronic communications services and public communications networks to safeguard the security of their services and networks.⁷ It also provides for the confidentiality of the communications and related traffic data,⁸ and mandates that such traffic data – which relates to subscribers and users – be erased or made anonymous when no longer needed for the purpose of the transmission of a communication.⁹

DATA PROTECTION AUTHORITY

The Commissioner's Office for the Protection of Personal Data (COPPD) was established in Nicosia on 1st May 2002.¹⁰ The COPPD is an independent administrative authority. The COPPD deals with the protection of personal information relating to an individual, against its unauthorised and illegal collection, recording, and further use. The COPPD also grants the individual certain rights, i.e. the right of information and access.¹¹ The

⁵ Law No. 112(I)/2004.

⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), available at http://www.dataprotection.ie/documents/legal/directive2002_58.pdf.

⁷ Section 98 of Law No. 112(I)/2004.

⁸ Section 99 of Law No. 112(I)/2004.

⁹ Section 100 of Law No. 112(I)/2004.

¹⁰ Email from Michalis Kitromilides, Office of the Personal Data Protection Commissioner, Cyprus, to Ula Galster, International Policy Fellow, Electronic Privacy Information Center (EPIC), 23 June 2005 (on file with EPIC). See also Commissioner's Office for the Protection of Personal Data, Year Review 2005, available at [http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/\\$FILE/Year%20review%202005.pdf](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/Year%20review%202005.pdf) at 3@@@.

¹¹ Commissioner's homepage http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument.

COPPD is responsible for monitoring the application of the Processing of Personal Data Law.¹²

The COPPD is appointed by the Council of Ministers following the recommendation of the Minister of the Interior and after consultation with the House Committee of European Affairs. The COPPD must be a person who holds or has held in the past the qualifications for appointment as judge of the Supreme Court of Justice. The COPPD cannot be discharged during the term of his service except for reasons of mental or physical disability or incapacity that renders him incapable of fulfilling his duties. As soon as the Council of Ministers ascertains the existence of one of these conditions, it publishes a notification in the *Official Gazette of Cyprus* that from a specific date he will no longer hold the position. The COPPD holds office for a term of four years, which may be renewed for one additional term.

Section 23 of the Law sets out the functions of the COPPD. These include: assisting in drawing up codes of conduct; reporting any contraventions to the law to the relevant authorities; and conducting inquiries following complaints or on his own initiative. The COPPD is also competent to keep the registers and grant the licences provided by the Law, issue directions, rules, and recommendations, conduct administrative inquiries, and impose sanctions for breaches of the Law. In 2004, with the enactment of Law 112(I)/2004, the responsibilities of the COPPD were extended to cover the regulation of the use of traffic data, location data, telephone directories, and unsolicited communications.¹³ Moreover, the COPPD maintains cooperation with the data protection authorities of European Union and Council of Europe Member States.¹⁴

The total number of complaints in 2005 reached 153, of which 41 were against public sector controllers, 112 were against private sector controllers, and 93 related to unsolicited communications.¹⁵ In 2005 the Office also received 16 applications to transfer data to third countries. By 2006, the Office had granted two applications and refused three, while the others were still pending.¹⁶

The COPPD's Office has issued two booklets with guidelines for the public. One educates the public about how to protect their personal data on the Internet and recommends that data controllers create Web sites that comply with data protection rules. The other includes guidelines about the lawful use of video surveillance cameras (*see more under the section on "Video Surveillance"*).¹⁷

¹² Processing of Personal Data Law, Section 18 (1).

¹³ *Id.*

¹⁴ Email from Michalis Kitromilides, *supra*.

¹⁵ Commissioner's Office for the Protection of Personal Data, Year Review 2005, *supra* at 2@@.

¹⁶ Article 29 Working Party on Data Protection, Ninth Annual Report (2006), *supra* at 24.

¹⁷ See Commissioner's Office for the Protection of Personal Data's homepage, *supra*.

Since its establishment in 2002, the Office has been engaged in numerous public awareness efforts. The Office organised seminars on the rights of data subjects, the lawful use of personal data, and workplace monitoring. Office employees delivered presentations to various government departments including the Police Academy, and also issued informational statements to the media and the University of Cyprus.¹⁸

In 2005, the European Commission notified the COPPD that certain sections of its Processing of Personal Data Law of 2001 did not fully comply with the European Data Protection Directive (1995/46/EC). The discordant provisions dealt with the right of information, transfer of data to third countries, and some procedural mechanisms. The COPPD is preparing legislation to further harmonise these regulations with the Directive.¹⁹

In 2005, the COPPD, as well as its counterparts in other EU member states, undertook an investigation regarding private health insurance carriers' processing of personal data. The objective was to determine whether this processing complies with EU data protection regulations.²⁰ (See more details under the "Health privacy" section.)

An audit the COPPD conducted in 2008 at the Land Registry Department found, among other things, that the Department collected information from third parties and did not inform them accordingly, and that certain documents it used included excessive and irrelevant information.²¹ In response, the COPPD issued guidance relating to the collection of fingerprints to check the arrival and departure times of employees, stating that the use was *prima facie* contrary to the law and should only be used in exceptional cases.²²

The COPPD reported that it had received very few complaints regarding email spam in 2005, but received many complaints regarding spam sent via mobile phone text messages. The Office conducted an audit of a company that engaged in unsolicited text message advertising. The audit revealed that the company's actions had breached the Regulation of Electronic Communications and Postal Services Law of 2004. The COPPD imposed a CYR1500 (€2,569) fine upon the company. The Office reported that its 2005 spam investigations met with substantially more cooperation from telecommunications companies than in 2004.²³

¹⁸ Commissioner's Office for the Protection of Personal Data, Year Review 2005, *supra* at 4.

¹⁹ Article 29 Working Party on Data Protection, Ninth Annual Report (2006), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf at 23.

²⁰ Commissioner's Office for the Protection of Personal Data, Year Review 2005, *supra* at 5.

²¹ Article 29 Data Protection Working Party, Eleventh Annual Report (2008), *supra* at 28.

²² Article 29 Data Protection Working Party, Eleventh Annual Report (2008), *supra* at 28.

²³ Commissioner's Office for the Protection of Personal Data, Year Review 2005, *supra* at 2-3.

In 2007, after receiving several complaints, the COPPD investigated a spam case involving the sending of unsolicited communications to mobile phones relating to horse racing results. The messages had been sent using prepaid telephone cards. The sender of the messages never responded to the COPPD's letters nor answered its questions. After following the prescribed procedure, the COPPD imposed a fine of £2,000.

In 2007, the COPPD investigated a case regarding the introduction of a biometric system by a data controller who was using employees' fingerprints for time registration purposes. The COPPD decided that the collection and use of fingerprints for this purpose was not in accordance with the Law and demanded that the controller discontinue this kind of processing and destroy the fingerprints already collected. (See more details under the "Workplace Privacy" section.)

Major privacy & data protection case law

The most recent reported case on the right to privacy and communications is the 1992 criminal case *The Police v Christodoulou Yiallourou*,²⁴ in which the Court affirmed the ruling from *The Police v Georgiades* (1983),²⁵ where the Court had held that "...evidence obtained in breach of a person's right to respect of his private life and confidential communications, under Articles 15 and 17 of the Constitution, could not be admissible." According to Judge Pikis: "the discretion given to English Courts of whether to admit or reject such evidence is unthinkable of in Cyprus, where the basic human rights are specifically guaranteed by the Constitution, which is not subject to judicial interference."²⁶

In the 1992 case, the defendant, who was the director of the Sewage Board of Nicosia, was monitoring and recording a number of teleconferences between an employee of the Board and a third person. During the trial, the issue of the admissibility of the recordings was raised. The Court held that the content of the tapes is a product of the violation of the rights of those involved, and as those rights are protected by the Constitution, therefore inadmissible as evidence.

This matter was also considered much later, this time in the civil case of *Takis Yiallourous v Engenios Nicolaou* in 2001.²⁷ This case was based on the same facts, and the defendant in the criminal case was also the defendant-appellant in this case. As in the criminal case, the Supreme Court confirmed the violation of the defendant's civil rights, as protected by the Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms,²⁸ and awarded general damages (aggravated and exemplary),

²⁴ 2 C.L.R., at 147.

²⁵ 2 C.L.R. at 33.

²⁶ Free translation.

²⁷ 8 May 2001, Civil Appeal 9931.

²⁸ The European Convention for the Protection of Human Rights and Fundamental Freedoms is also part of Cyprus national law by Law 89/62, Article 13, and its interpretation by the European Court of Justice in *Klass v FRG*, A 28, para. 64 (1979).

taking into account the purpose of the violations, their duration, and the humiliation to which the individual was subjected.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The Protection of Secrecy of Private Communications (Call Interception) Law of 1996 mandates that the Attorney General file for a court order before using wiretaps.²⁹ In 2006 a parliamentary committee amended Chapter 17 of the island's Constitution. Under the amended language, the Attorney General can authorise phone tapping if it is necessary to save time. The amendment also allows the police to monitor Web logs, downloads and emails as admissible evidence for criminal investigations.³⁰

National security legislation

Nothing to report under this section.

Data retention

Nothing to report under this section.

National databases for law enforcement and security purposes

In 2005, the Road Traffic Offences (Use of Automatic Detection Devices and Other Relevant Matters) Law of 2001 was also implemented. The Law authorises certain traffic offences to be recorded automatically under the supervision of the Cyprus Council of Ministers and the Deputy Chief of Police.³¹

National and international data disclosure agreements

Cyprus has recently agreed to participate in the cooperation procedure concerning the transmission of complaint and intelligence information relevant for the enforcement of Article 13 of the Privacy and Electronic Communication Directive, or any other applicable national law pertaining to the use of unsolicited electronic communications (also called "spam").

A Contact Network of spam authorities has put in place a cooperation procedure by which an authority will forward complaints to the authority of the country from which the

²⁹ Law No. 92(I)/1996.

³⁰ Xinhua News Agency, "Cyprus Parliament Committee Gives Green Light for Police Phone Tapping," Xinhua General News Service, 27 October 2006.

³¹ Article 29 Data Protection Working Party, Ninth Annual Report (2006), *supra* at 23.

emails originate so it can lead the investigations.³² Cyprus has also agreed to take part in the "Operation Spam Zombies" initiative of the United States Federal Trade Commission. The Operation is a new global effort to combat spam email sent through hijacked computers, known as "zombies."³³

Cybercrime

Nothing to report under this section.

Critical infrastructure

Nothing to report under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

In April 2004 Cyprus transposed the European Directive on Privacy and Electronic Communications.

In order to regulate the field of electronic commerce, Cyprus adopted in 2004 the Law on Certain Aspects of Information Society, and specifically Electronic Commerce, and Relevant Matters (the Electronic Commerce Law),³⁴ as well as the Law on the Conclusion of Distance Contracts of 2000.³⁵ The Electronic Commerce Law implements the "Directive on Electronic Commerce" (2000/31/EC).³⁶ This Law is aimed at ensuring the free movement of information society services between the Republic of Cyprus and the Member States of the European Union. It deals in particular with the establishment of service providers, commercial communications, the conclusion of electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, means of legal protection, and cooperation between Member States.

In 2004, Cyprus also adopted a Law on a Legal Framework for Electronic Signatures and Relevant Matters.³⁷ It establishes the legal framework governing electronic signatures and certain certification services for the purpose of facilitating the use of electronic signatures and their legal recognition. It does not, however, cover aspects related to the conclusion and validity of contracts or other legal obligations that are governed by

³² *Id.*

³³ See <http://www.ftc.gov/bcp/online/edcams/spam/zombie/partners.htm>.

³⁴ Law No. 156(I)/2004.

³⁵ Law No. 14(I)/2000.

³⁶ Directive of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on Electronic Commerce"), available at http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l24204_en.htm.

³⁷ Law No. 188(I)/2004.

requirements as regards their form. Moreover, it does not affect rules and limitations in relation to the use of documents provided by other applicable legislation in force. The Law grants power to the Minister of Commerce, Industry, and Tourism (the Competent Authority) to exercise control over and ensure the effective application of this Law.³⁸

The COPPD is the appropriate authority for enforcing anti-spam provisions.³⁹ The COPPD's Commissioner is discussing with Internet service providers ways to cooperate in the fight against spam. Cyprus has recently agreed to participate in the cooperation procedure concerning the transmission of complaint and intelligence information relevant for the enforcement of Article 13 of the Privacy and Electronic Communication Directive, or any other applicable national law pertaining to the use of unsolicited electronic communications (also called "spam"). (See more details under the "National and international data disclosure agreements" section.)

In 2007, after receiving several complaints, the COPPD investigated a spam case involving the sending of unsolicited communications to mobile phones relating to horse racing results. The COPPD imposed a fine of £2,000.

In September 2006, the Cyprus Neuroscience and Technology Institute launched an Internet safety awareness campaign called the CyberEthics project. The CyberEthics project includes a consortium comprised of the University of Cyprus Department of Social and Political Sciences, the Cyprus Broadcasting Corporation, the Family Planning Association, the Cyprus Youth Council, and the Olive Tree Branch. The project is focused on Cyprus' northern, rural, and minority populations, but is intended to serve the entire population of the island. The project addresses issues relating to pornography, racism, gender discrimination, the inappropriate use of peoples' images, and peer-to-peer file transfer. The CyberEthics project will also endeavour to inform users of European filtering software and services that enhance online privacy and filter unethical or illegal content.⁴⁰

Cybersecurity

Nothing to report under this section.

Online behavioural marketing and search engine privacy

Nothing to report under this section.

Online social networks and virtual communities

Nothing to report under this section.

³⁸ See http://www.ldlaw.com.cy/services/it_ecommerce.htm.

³⁹ Email from Michalis Kitromilides, *supra*.

⁴⁰ See CyberEthics, available at <http://www.cyberethics.info/>. See also European Commission Information Society, Awareness node for Cyprus, available at http://ec.europa.eu/information_society/activities/sip/projects/completed/awareness/cyberethics/index_en.htm.

Online youth safety

In 2009 Cyprus launched SafeWeb, a new Web site designed to provide concerned users with the online means to anonymously report various illegal matters.⁴¹ As part of the Safer Internet-Plus Programme, SafeWeb is funded by the EU to combat the illegal use of the Internet. The Web site hopes to help fight the problems of Internet piracy and child pornography in Cyprus.⁴²

TERRITORIAL PRIVACY

Video surveillance

In June 2007, the United Nations Peacekeeping Force in Cyprus (UNFICYP) announced it would "significantly" increase the number of surveillance cameras located on the island's ceasefire buffer zone.⁴³ The cameras will operate 24 hours a day, according to a UNFICYP spokesman, with the aim of positively affecting peoples' behaviour in a manner similar to the justification that traffic cameras improve driving.⁴⁴

The COPPD has issued a Directive on Video Surveillance to provide good practice guidance in relation to the application of the Data Protection Law ("the Law") to this kind of personal data processing, since images captured by CCTV systems are in some cases considered personal data.

The Directive covers two categories of premises in which video surveillance can be carried out: private ones, such as banks, shops and football fields, which are privately owned but freely accessible to the public; and public places, such as roads and parks, where the public expects greater privacy. Although not legally obliged to do so, people who are responsible for the operation of CCTV systems should consult with the COPPD before installing them, and follow its instructions. People responsible for the operation of CCTV systems that record individuals must be in a position to justify their action as if they were collecting personal data. The person responsible for the operation of a CCTV system must file a written notification with the COPPD, in accordance with Section 7 of the Law, unless it falls within one of the exemptions to the Law.

As in the case of CCTV operation, individuals whose images have been recorded by CCTV are unlikely to have given their express consent. Legitimate reasons that could be given for using CCTV could be the identification, investigation, and prosecution of crimes, public safety, the protection of premises, national defence or security, road traffic

⁴¹ SafeWeb, available at <http://www.safeweb.org.cy>.

⁴² John Leonidou, "Fighting the Illegal Use of the Internet," EDRI-gram, 13 February 2008, available at http://www.cyprus-mail.com/news/main.php?id=22120&cat_id=9.

⁴³ The United Nations Peacekeeping Force in Cyprus (UNFICYP) was established in 1964 to prevent hostilities between the Greek and Turkish Cypriot communities, and the buffer zone extends over 180 kilometers, approximately 3 percent of the island.

⁴⁴ Leo Leonidou, "UNFICYP Steps up Buffer Zone Surveillance," *Cyprus Mail*, 6 June 2007, available at <http://www.cyprus-mail.com/news/main.php?id=32825&archive=1>.

monitoring, and the like. The use of CCTV on private premises can usually be justified by the owners on the grounds of prevention or detection of crime, or ensuring the security of their property.

However, in order to justify CCTV monitoring in public places, a stricter justification is necessary. CCTV system owners must be in a position to demonstrate that monitoring is necessary and that its benefits outweigh any resulting harm to the rights, interests, and basic freedoms of monitored individuals. CCTV systems should only be installed where there is no other alternative and a less intrusive method to achieve its purpose, provided, however, that such an alternative method will not entail a highly disproportionate cost.

The individuals who will be recorded must be informed about it and given the right to decline to enter the building or public premises in which the recording takes place.

Images should only be retained for as long as necessary to achieve the purposes of the recording.⁴⁵ It is not possible to determine a fixed period covering all cases but it is important that the persons responsible for the operation of CCTV cameras (the "data controllers") have in place a specific retention policy for the recording of media and be in a position to justify the reasons why this retention period is considered necessary.

All appropriate technical and organisational measures should be taken to ensure the security and confidentiality of any recordings, which should be accessible only to those who can demonstrate a legitimate interest (e.g., the possibility for the general public to assist in identifying a criminal or a victim).

Individuals recorded on CCTV (the "data subjects") have the right to request that the videos concerning them be destroyed, not used or not shown, in part or in whole, where they believe that the recording has not been carried out in accordance with the Law.

In July 2007, Cypriot police investigated a breach of privacy claim into the government's Commission for the Protection of Competition (CPC). The probe came after complaints and strikes from the CPC's staff, which accused the Competition Commissioner of pervasive workplace surveillance. According to employees, the monitoring system included CCTV cameras and microphones throughout the offices, including restrooms, which could be remotely accessed through the Commissioner's personal computer.⁴⁶ In their ongoing investigation, the police accessed the Commissioner's computer and discovered about 600 pictures, freeze-frames from video recordings, including some 400 of a particular female employee.⁴⁷ The COPPD stated that the CPC should have notified them of the monitoring system, but failed to do so. (See more details under the "Workplace Privacy" section.)

⁴⁵ Section 4 of the Data Protection Law.

⁴⁶ Elias Hazou, "Police Probe 'Big Brother' Claims at CPC Offices," *Cyprus Mail*, 7 July 2007, available at <http://www.cyprus-mail.com/news/main.php?id=33448&catid=1>.

⁴⁷ Elias Hazou, "Staff Walkout Leaves CPC Boss on His Own," *Cyprus Mail*, 18 July 2007, available at http://www.cyprus-mail.com/news/main.php?id=33652&cat_id=1.

In September 2006, a network of traffic cameras was installed on Cyprus. The programme had been delayed nearly a year, in part due to privacy concerns. Originally the photographs were saved in a centralised database indefinitely, for "research and statistical purposes", but the Cyprus House Legal Affairs Committee stated in January 2006 that it would not accept the surveillance programme unless the photographs were destroyed immediately after the fine had been paid.⁴⁸ The system has since been installed, beginning with 40 cameras, with plans to deploy 450 across Cyprus in the next four years.⁴⁹ In addition to capturing speeders and drivers running red lights, the cameras can also tell if motorists are breaking other laws, such as failing to wear a seatbelt or talking on a mobile phone.⁵⁰ At first, offenders caught on camera received a hand-delivered ticket at their homes, but the cameras caught so many offenders that the police did not have the manpower to personally deliver each ticket; the tickets now arrive via post.⁵¹ The first 40 cameras caught about 367 offenders every day, one out of six motorists, and the addition of 120 more cameras was planned for October 2007.⁵² The COPPD expressed concern for personal privacy in October 2006, citing the claim of a private television station that it had received information from a police officer that a traffic camera had caught the chief of police committing a traffic offence. The chief of police responded to the COPPD that no data breach had occurred and that the database storing offenders' information was "totally secure".⁵³

Location privacy (GPS, mobile phones, location based services, etc.)

Nothing to report under this section.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The COPPD has adopted the document on biometrics issued by the Article 29 Working Party on 1st August 2003.⁵⁴

⁴⁸ Jacqueline Theodoulou, "Privacy Concerns over Traffic Camera Pictures," *Cyprus Mail*, 13 January 2006, available at <http://www.cyprus-mail.com/news/main.php?id=23753&archive=1>.

⁴⁹ Leo Leonidou, "Traffic Cameras Switched on at Last," *Cyprus Mail*, 19 September 2006, available at <http://www.cyprus-mail.com/news/main.php?id=27963&archive=1>"><http://www.cyprus-mail.com/news/main.php?id=27963&archive=1>.

⁵⁰ Leo Leonidou, "Traffic Cameras Start for Real," *Cyprus Mail*, 10 October 2006, available at <http://www.cyprus-mail.com/news/main.php?id=28347&archive=1>.

⁵¹ Jacqueline Theodoulou, "Police Swamped by Traffic Camera Fines," *Cyprus Mail*, 6 December 2006, available at <http://www.cyprus-mail.com/news/main.php?id=29490&archive=1>.

⁵² Leo Leonidou, "One in Six Caught on Camera," *Cyprus Mail*, 17 May 2007, available at <http://www.cyprus-mail.com/news/main.php?id=32437&archive=1>.

⁵³ Leo Leonidou, "325 Snapped by the Cameras," *Cyprus Mail*, 13 October 2006, available at <http://www.cyprus-mail.com/news/main.php?id=28398&archive=1>.

⁵⁴ Article 29 Working Party on Data Protection, Working document on biometrics, 1st August 2003, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf.

NATIONAL ID & SMART CARDS

In March 2009, the Cyprus Government initiated the procedures to introduce "e-ID" ("electronic identity" smart cards) to be used for electronic identification and authentication in public services.⁵⁵ This project will be undertaken in cooperation with other EU Member States in order to achieve seamless access to public services across national borders. E-ID standardisation or interoperability is essential in order to put in place key pan-European services such as cross-border company registration, electronic public procurement, job search, e-voting and e-health.⁵⁶ A prepared proposal is awaiting approval by the Ministry of Interior, and the Council of Ministers.⁵⁷

RFID tags

Nothing to report under this section.

BODILY PRIVACY

Nothing to report under this section.

WORKPLACE PRIVACY

There is an exception to the general regime of the Law where the processing of sensitive data is necessary for the data controller to fulfil his obligations or to carry out his duties under employment law and the Commissioner's Office for the Protection of Personal Data (COPD) has granted a derogation for this purpose. Under Section 11 of the COPPD's Employment Order, the employer may maintain data concerning an employee's previous convictions, such as traffic accidents made by a professional driver. The collection and processing of such data must be absolutely necessary for purposes connected to the employment relationship or where it is imposed by law. Where the collection is deemed necessary, employers must nevertheless inform employees of its purpose in advance.⁵⁸

According to the COPPD's Employment Order, every employee has the right to access his personal file and the right to know whether, and which of, his personal data are or have been the subject of processing by his employer.⁵⁹ This right involves information on all personal data relating to him, as well as their source. The employee is entitled to know not only the content but also the source of the information. For example, in the case of an employee's negligence committed within the scope of his work contract, the source of his

⁵⁵ European Egovernment Services, EGovernment in Cyprus 18 (September 2008), available at <http://ec.europa.eu/idabc/servlets/Doc?id=31765>.

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ In any event, its collection must be in accordance with Section 10 of the Police Law (Law 73(I)/2004) that provides that the Head of Police shall issue a certificate concerning the employee's clean record to include any sentencing, but only upon an application made by the employee or his employer.

⁵⁹ Section 17.3, *op. cit.*

employer's information, e.g. video recording or email monitoring, would have to be disclosed.

The employee's right of access also imposes an obligation for the employer to reply in writing to the employee within four weeks upon his request, to inform him of the following:

- (a) all of the personal data the employer keeps on the employee;
- (b) the sources of the personal data, if it has not been collected directly from the employee himself;
- (c) the employer's purpose in processing the data;
- (d) the recipients to whom the employee's personal data may be communicated;
- (e) how the processing of the employee's personal data has progressed since the last time the employee was informed of all of the above by his employer; and
- (f) the logic by which the employer made any decision concerning the employee and that was based on any automated processing of personal data concerning that particular employee.

If the employer does not reply within four weeks from the time that the employee submits the request to exercise the right of access or where the employee considers that the response given to him by his employer is unsatisfactory, the employee has the right to appeal to the COPPD. If the COPPD considers the employee's request justifiable under the Law, it may compel the employer to allow the employee to have access to the information requested.

The data subject has the right, for imperative and lawful reasons relating to his specific circumstances, to object to the processing of data that relates to him.

The right to object is implemented in the field of employment – as it clarified in the COPPD's Employment Order – consists of the employee's right to ask his employer to take a specific action relating to the processing of his personal data at any given time.

It is self-evident that within a labour relationship, personal data pursuant to law or the contractual arrangement are duly collected and the employee is generally not in a position to raise an objection, given that it would be unlawful and would contravene his employment contract. In consequence, the right to object, in order to have a legal basis, must concern any processing taking place beyond lawful and contractual purposes.

Upon his employer's failure to reply satisfactorily within 15 days, the employee has the right to apply to the COPPD to request that his objections be examined. The COPPD may then order the immediate suspension of the employer's data processing pending a final decision.

If a public authority or any other person carries out processing that concerns the evaluation of the data subject's personality, his productivity in his employment, his

financial solvency reliability, or his behaviour in general, the data subject can apply to a court for it to issue a preliminary injunction against the processing.

The COPPD's Employment Order regulates the assignment by employers of the hiring or candidate selection procedure to job-finding agencies that carry out this task on their behalf. Job-finding agencies usually operate in one of two ways. They either act on the employer's orders by publicising posts for which candidates apply, or they act on behalf of interested employees by applying to potential employers engaged in the sectors in which the employees are interested. Both ways presuppose the transfer of data concerning candidates, making the Employment Order directly applicable to job-finding agencies.

Despite the fact that job-finding agencies collect personal data that are processed exclusively for purposes connected to the employment relationship, when these data are communicated to third parties (potential employers), job-finding agencies are under an obligation, as data processors,⁶⁰ to notify the COPPD of said processing.

According to the COPPD's Employment Order, monitoring at work is a very important issue in the context of employment relationships, and must be given the appropriate attention by employers. When monitoring includes the collection, examination and storage of personal data of employees, the Law and Employment Order apply.

Complaints received by the COPPD usually concern the automated monitoring methods employers use in the workplace. Such methods include email, fax or Internet browsing monitoring, the tracking of phone calls or their recording, CCTV surveillance and GPS tracking.

Such monitoring is allowed under the Law provided that the employer is in a position to justify its legitimacy and need and that there is no other, less intrusive way of achieving its intended purposes. Such purposes, to be justified, must be such as to take priority over the employees' rights, interests and fundamental freedoms. An employer who would use a CCTV system to monitor the workplace for security reasons may not use that system for the purpose of monitoring employees during their breaks. The employer must choose the lowest level of monitoring which is sufficient to satisfy his purposes, with the aim of the minimum possible intrusion into the personal life of employees.

The voice, picture, email address, and phone number of employees are considered personal data, and if collected through monitoring systems installed by an employer in the workplace, must be used only for the specific purposes for which they were gathered, and destroyed or deleted after these purposes have been accomplished.

The employer must on all occasions notify his employees in advance about the purpose, manner, and duration of the control that he intends to apply. It is considered good practice to adopt a written policy that determines the parameters for the use of telephones, computers, and other means of communication and equipment by employees, and the

⁶⁰ A "data processor" is any person who processes personal data on behalf of a controller.

ways in which the employer will control or monitor their use. Secret monitoring or monitoring without previous notice is prohibited under any circumstances. Employers wishing to install monitoring systems at the workplace are recommended to consult employees or their trade union or other representatives to discuss the intended methods and consequences of monitoring. However, an employer is not allowed to access the personal emails of employees in any event but has the right to inform them that the use of workplace equipment for purposes unrelated to their work is not allowed and to penalise them for such use.

Under the Law, personal data may be processed without the data subject's consent where processing is necessary for the performance of a contract to which the data subject is a party. The COPPD has recognised that due to the nature of an employment relationship, an employee's personal data may on certain occasions be lawfully processed without his consent. Under the Employment Order, no consent is required for the processing of personal data by the employer in relation to the performance of a legal obligation or in the context of the performance of an employment contract.

In particular, the Employment Order suggests that individual consent by employees may not be required in order to transfer employees' personal data internationally in the case of payment of taxes or social insurance contributions (legal obligation), or when carrying out a performance evaluation or reporting an accident in the workplace (contract performance). However, such transfers should always take into account the general principles for processing personal data of the Law.

In 2007, a case was investigated by the COPPD regarding the introduction of a biometric system by a data controller who was using employees' fingerprints for time registration purposes. The employer had used other systems before but found them to be open to fraud and misuse. It was decided by the Commissioner that the collection and use of fingerprints for this purpose was not in accordance with the Law as this method should only be used in exceptional circumstances, e.g., where additional security measures to control access to premises are deemed necessary. The controller was asked to discontinue this kind of processing and destroy the fingerprints already collected.

An audit the COPPD conducted in 2008 at the Land Registry Department found, among other things, that the Department collected information from third parties and did not inform them accordingly, and that certain documents it used included excessive and irrelevant information.⁶¹ In response, the COPPD issued guidance relating to the collection of fingerprints to check arrival and departure times of employees, stating that the use was *prima facie* contrary to the law and should only be used in exceptional cases.⁶²

In July 2007, Cypriot police investigated a breach of privacy claim into the government's Commission for the Protection of Competition (CPC). The probe came after complaints

⁶¹ Article 29 Data Protection Working Party, Eleventh Annual Report (2008), *supra* at 28.

⁶² Article 29 Data Protection Working Party, Eleventh Annual Report (2008), *supra* at 28.

and strikes from the CPC's staff, which accused the Competition Commissioner of pervasive workplace surveillance. According to employees, the monitoring system included CCTV cameras and microphones throughout the offices, including restrooms, which could be remotely accessed through the Commissioner's personal computer. The employees further claimed that their emails and telephone conversations had been monitored. Trade unions became actively involved and the case became the main topic in the local media for many weeks, leading to the resignation of the CPC President, which finally put an end to the strike. The Commissioner denied some of these claims, countering that the system was not secret and was necessary to keep his employees on task.⁶³ In their ongoing investigation, the police accessed the Commissioner's computer and discovered about 600 pictures, freeze-frames from video recordings, including some 400 of a particular female employee.⁶⁴ Cyprus' Data Protection Commissioner stated that the CPC should have notified them of the monitoring system, but failed to do so; the Data Protection Commissioner also noted that since the CPC surveillance scandal broke, her office had received numerous similar complaints from across the island.⁶⁵

HEALTH & GENETIC PRIVACY

Health privacy

The COPPD, as well as its counterparts in other EU member-states, undertook an investigation regarding private health insurance carriers' processing of personal data. The objective was to determine whether this processing complies with EU data protection regulations.⁶⁶ The results of the investigation were published in a "Working Document on the Processing of Personal Data Health Relating to Health in Electronic Health Records" in February 2007.⁶⁷

Genetic privacy

Nothing to report under this section.

FINANCIAL PRIVACY

Nothing to report under this section.

⁶³ Elias Hazou, "Police Probe 'Big Brother' Claims at CPC Offices," *Cyprus Mail*, 7 July 2007, available at <http://www.cyprus-mail.com/news/main.php?id=33448&catid=1>.

⁶⁴ Elias Hazou, "Staff Walkout Leaves CPC Boss on His Own," *Cyprus Mail*, 18 July 2007, available at http://www.cyprus-mail.com/news/main.php?id=33652&cat_id=1.

⁶⁵ Elias Hazou, "Either Big Brother Boss Goes or We Do," *Cyprus Mail*, 11 July 2007, <http://www.cyprus-mail.com/news/main.php?id=33525&archive=1>.

⁶⁶ Commissioner's Office for the Protection of Personal Data, Year Review 2005, *supra* at 5.

⁶⁷ Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (February 2007), available at http://www.dataprotection.gov.sk/buxus/docs/wp131_en.pdf?buxus=c33673afa287cd38a32605ea68e69163.

E-GOVERNMENT & PRIVACY

Nothing to report under this section.

OPEN GOVERNMENT

Cyprus does not have an access to information law. Although such a law exists in the northern part of Cyprus, it has been very poorly implemented.⁶⁸ A civil society initiative⁶⁹ is currently working to promote and advance the right to know in both the northern and southern parts of Cyprus.

OTHER RECENT FACTUAL DEVELOPMENTS

Nothing to report under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

Nothing to report under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

The Republic of Cyprus is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108.⁷⁰ Cyprus is a signatory to the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Additional Protocols.⁷¹ Cyprus has also signed and ratified the Additional Protocol to the Convention regarding supervisory authorities and transborder data flows⁷² and the Council of Europe's Convention on Cybercrime.⁷³ The Law ratifying the Cybercrime Convention provides for the establishment of criminal offences of the acts described in Chapter II of the

⁶⁸ Helen Darbishire, David Pardo & Ilke Dagli, "World Press Freedom Day and Your Right to Know *Cyprus Mail*, 9 May 2010, available at http://www.access-info.org/documents/Access_Docs/Advancing/article_WPFD.pdf. See generally <http://www.access-info.org/en/cyprus>.

⁶⁹ <http://www.accessinfocyprus.eu>.

⁷⁰ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data No. 108, signed: July 25, 1986, ratified: February 21, 2002, entered into force on 1 June 2002, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=3&DF=22/08/2005&CL=ENG>.

⁷¹ Council of Europe, Cyprus' Treaties signed and ratified or having been the subject of an accession as of 18/6/2009, available at <http://www.conventions.coe.int/Treaty/Commun/ListeTraites.asp?PO=CYP&MA=999&SI=2&DF=&CM=3&CL=ENG>.

⁷² Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, signed on 3 October 2002; ratified on 17 March 2004; entered into force 1st July 2004.

⁷³ Signed on 23 November 2001; ratified on 19 January 2005; entered into force on 1st May 2005. Ratification Law No. 22(III)/2004.

Convention, such as illegal access, illegal interception, data interference, system interference, etc. and their respective penalties.

CZECH REPUBLIC

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The 1993 Charter of Fundamental Rights and Basic Freedoms provides for extensive privacy rights. Article 7(1) states, "The inviolability of the person and of privacy is guaranteed. They may be limited only in cases provided for by law." Article 10 states, "(1) Everyone has the right to demand that his human dignity, personal honour, and good reputation be respected, and that his name be protected. (2) Everyone has the right to be protected from any unauthorised intrusion into her private and family life. (3) Everyone has the right to be protected from the unauthorised gathering, publication revelation, or other misuse of his personal data." Article 13 states, "Nobody may violate confidentiality of letters or other papers or records, whether privately kept or sent by post or by some other means, except in cases and in the manner specified by law. The confidentiality of communications sent by telephone, telegraph or other such devices are guaranteed in the same way."¹

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

On 1 May 2004, the Czech Republic joined nine other countries in entering the European Union (EU), formally linking itself to the EU and to the EU regulatory framework for data protection.² In preparation for accession, the Czech Republic enacted a new act on "Personal Data Protection" (the Personal Data protection Act or the Act), which went into effect on 1 June 2000.³ The Act replaced the 1992 Act on Protection of Personal Data in Information Systems.⁴ The Act implements the requirements of the EU Data Protection Directive 1995/46/EC, granting exceptions from several key provisions to the police and intelligence services in matters of public and national security in accordance with the directive.⁵ Data controllers were required to register their processing systems and fully comply with the Act by 1 June 2001. A May 2001 amendment exempted political parties,

¹ Charter of Fundamental Rights and Basic Freedoms, 1993, available at <http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html>.

² Official Journal of the European Union, Vol. 4 L 168, 1 May 2004, available at <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2004:168:SOM:EN:HTML>.

³ Act No. 101/2000 Coll. on Personal Data Protection, available at <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en>.

⁴ Act No. 256/1992 Coll. on Protection of Personal Data in Information Systems.

⁵ Directive 1995/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, OJ L 281, 23 November 1995, at 31–50, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

churches, sports clubs, and other civic organisations engaged in standard and legitimate activities from some of the Act's requirements, such as registering their data processing activity or obtaining consent of individuals before collecting personal information.

A June 2004 amendment to the Act on Personal Data Protection completed harmonisation with EU Data Protection Directive 1995/46/EC.⁶ The amendment refines certain terms, as well as introducing new terms in accordance with the EU Directive. The amendment includes terms regulating the granting of consent for personal data processing, the relationship between data controllers and data subjects, the notification duty of controllers, and indemnification of data subjects for breaches of duty committed by data controllers or data processors.⁷

In 2007, an emphasis was placed on data security, and an amendment to the Act on Personal Data Protection introduced more detailed rules on risk assessment and security measures that must be adopted before the commencement of personal data processing.⁸ In 2009, a widely discussed amendment⁹ specifically provided for the protection of recordings of intercepted telecommunications gathered in the course of criminal proceedings.¹⁰

Sector-based laws

Privacy is also largely protected by the Penal Code.¹¹ It covers the infringement of the right to privacy in the definitions of criminal acts consisting of infringement of the home,¹² slander,¹³ unauthorised use of personal data (collected either on the basis of sectorial acts by state authorities or by controllers or processors),¹⁴ infringement of the confidentiality of mail,¹⁵ and infringement of the confidentiality of information "kept in privacy" (this is a newly introduced crime compared to the previous Penal Code).¹⁶

⁶ Act No. 439/2004 Coll.

⁷ Office for Personal Data Protection Annual Report 2004, at 31, available at http://www.uoou.cz/files/rep_2004.pdf.

⁸ Act No. 170/2007 Coll.

⁹ Act No. 177/2008 Coll.

¹⁰ See "Wiretapping, access to, and interception of communications," *infra*.

¹¹ Act No. 40/2009 Coll., the Penal Code (effective since 1 January 2010).

¹² *Id.*, at Section 178.

¹³ *Id.*, at Section 184.

¹⁴ *Id.*, at Section 180.

¹⁵ *Id.*, at Section 182.

¹⁶ *Id.*, at Section 183.

In addition to the Penal Code, several other Czech laws also regulate certain specific aspects of data processing activities. These laws concern statistics, medical personal data, banking law, taxation, social security, and police data.

DATA PROTECTION AUTHORITY

The Act also established an Office for Personal Data Protection (OPDP) as an independent oversight body.¹⁷ The Office is responsible for supervising the implementation of the Act; maintaining a register of databases; investigating complaints; imposing fines for violations; conducting audits and providing consultations on data protection; and commenting on legislative proposals. Igor Němec, the President of the OPDP, was appointed to a five-year term that began 1 September 2005 and reappointed in 2010. The President of the Czech Republic also appointed seven independent inspectors, each position carrying a ten-year term.

During 2007, the OPDP received 574 complaints and petitions. The number of complaints in 2007 increased by 21 percent compared to 2006.¹⁸ Two-thirds of these complaints were dismissed as unjustified, a rate that's comparable to 2006.

The OPDP also commenced 35 investigations in 2007.¹⁹ Inspections were aimed at telecommunications carriers, media outlets, police, financial institutions such as banks and credit lenders, transportation authorities, law offices, city and municipality bodies, retail chains, Internet business, schools, and social and health care facilities. The OPDP imposed administrative fines in the total amount of CZK4,668,500 (approximately. €191,270) pursuant to the Code of Administrative Procedure.²⁰

Many 2006 complaints continued to refer to excessive utilisation of birth certificate numbers based on an incorrect opinion that a birth certificate number is an absolute identifier of a natural person and is thus a natural supplement to the name. An attempt to improve this practice was brought about in 2004 by the adoption of an amendment to Act No. 133/2000 Coll. on Register of Population and Birth Numbers, through Act No. 53/2004 Coll. The Amendment to the Act on Register of Population and Birth Numbers imposed supervisory duties on the OPDP in the area of management of birth certificate numbers.²¹ The Amendment's detailed new rules concerning the use of birth certificate numbers came into effect 1 January 2006. Article 13c(1)(c) prohibits the use of birth certificate numbers in the private sphere unless the number holder has given free and

¹⁷ Office for Personal Data Protection, at <http://www.uoou.cz/>.

¹⁸ Office for Personal Data Protection Annual Report 2007, at 36, available at http://www.uoou.cz/files/rep_2007.pdf.

¹⁹ *Id.*

²⁰ *Id.*, at 26.

²¹ Email from Karel Neuwirt the President of the Office for Personal Data Protection, to Ula Galster, International Policy Fellow, Electronic Privacy Information Center, 18 May 2005, (on file with EPIC). See also Office for Personal Data Protection Annual Report 2004, *supra* at 4.

informed consent. Article 13(1)(a) of the Act continues to grant authorisation to State administrative bodies to use the birth certificate number as an identifier. Despite this measure, however, the OPDP noted that it was still common to treat the birth certificate number as a unique identifier.²²

Complaints also followed similar patterns as in the past, including lack of awareness by controllers of their notification duties under the Personal Data Protection Act, unclear sources of data used to address clients in direct marketing, excessive use of birth certificate numbers, inappropriate copying and retention of personal documents, and publishing of lists of debtors as a method of extracting payment for debts.

Although the situation in 2008²³ could indicate slowly raising awareness among the public – 697 complaints and two-thirds of them being dismissed – 2009²⁴ brought 879 complaints but more than four-fifths of them were dismissed. The number of investigations has increased from 112 in 2008 to 143 in 2009. In addition, the OPDP dealt with 1,458 complaints regarding unsolicited commercial communications (and investigated 155 cases) in 2008 compared with 2,261 complaints (and 145 cases investigated) in 2009.

Beginning in 2004, the Control Department of the Office for Personal Data Protection, as a rule, no longer addressed the entity against which the petition was aimed. Where the circumstances indicate that a criminal offense was committed, the matter is promptly submitted to the bodies actively engaged in criminal proceedings, and then the Control Department further cooperates with these bodies. The department continues to fully engage in resolving these issues within its responsibility until the criminal proceedings are closed.²⁵

In the course of supervision, the OPDP followed the principle that, as a rule, the identity of the complainant is not disclosed to third persons in the framework of the relevant enquiries; his or her identity is revealed only when necessary and after obtaining his consent. The Control Department also does not refuse to handle anonymous complaints.

Financial penalty for proven misconduct usually accompanies remedial and indemnification measures and it facilitates remediation of the defective state of affairs in the course of the OPDP's supervisory activities. The Personal Data Protection Act distinguishes between misconduct of controllers and processors, who are liable to a fine of up to CZK10 million (€410,000) – CZK20 million (€820,000) for repeated torts – and misdemeanours of natural persons, which are subject to a fine of up to CZK100,000

²² Office for Personal Data Protection Annual Report 2006, at 39, available at http://www.uoou.cz/files/rep_2006.pdf.

²³ Office for Personal Data Protection Annual Report 2008, available at http://www.uoou.cz/files/rep_2008.pdf.

²⁴ Office for Personal Data Protection Annual Report 2009, available at http://www.uoou.cz/files/rep_2009.pdf.

²⁵ Office for Personal Data Protection Annual Report 2006, *supra* at 39.

(€16,300). Natural persons acting as controllers or processors are subject to a fine of up to CZK5 million (€205,000). The Act does not stipulate the applicable amount of fines for individual torts where civil liability (sued in a court proceeding) would apply; however, consideration must always be taken of the general criteria stipulated by the act, including the nature, seriousness, and manner of conduct, degree of fault, duration, and consequences of the misconduct.²⁶

As of 31 December 2007, the OPDP consisted of 92 employees.²⁷ The increase in the number of employees was to enable the OPDP to become fully involved in Schengen cooperation.²⁸ In January 2006, the Department of Complaints and Consultations was established to improve public services. The new Department was charged with responding to telephone inquiries, providing personal consultations, responding to electronic petitions, and assessing complaints. In most cases, the Department was able to respond to inquiries within half of the statutory 30-day deadline.²⁹ At the end of 2009, the OPDP employed 95 employees.³⁰

The OPDP actively engages in making the relevant information about its activities public. The OPDP holds regular press conferences. It also publishes two journals: the official one (five issues per year) includes positions of the OPDP and European documents relevant to personal data protection. A quarterly is designed for the public at large. It provides information on the OPDP's activities, as well as worldwide news concerning personal data protection.³¹

At the end of 2004, a campaign for citizens was launched. It involved publishing leaflets related to the Act on Personal Data Protection, rights and responsibilities of data subjects, and risks that they ought to prevent. About 300,000 issues were distributed (to the regional and local administrative bodies and high schools – with the cooperation of the Ministry of Education). TV, radio stations, and newspapers supported the campaign. The OPDP also cooperated with media (354 publications and broadcasting items through the year 2004).³²

The OPDP reported some gain in public awareness in 2005, illustrated in the increased number of complaints and inquiries since 2004, as well increased media coverage.

²⁶ Act No. 101/2000 Coll., *supra* at Section 46.

²⁷ Office for Personal Data Protection Annual Report 2007, *supra* at 62.

²⁸ Resolution of the Government of the Czech Republic No. 633 of 11 June 2007.

²⁹ Office for Personal Data Protection Annual Report 2006, *supra* at 29.

³⁰ Office for Personal Data Protection Annual Report 2009, *supra* at 71.

³¹ Office for Personal Data Protection Annual Report 2007, *supra* at 59.

³² Office for Personal Data Protection Annual Report 2006, *supra* at 9.

Nonetheless, the OPDP still concluded that overall awareness among controllers and the general public was largely uncultivated.³³

In 2006 the OPDP again focused on raising public awareness of personal data protection. The OPDP acted as co-authors in a 13-part television series on the subject titled *Ignorance does not excuse. Everyone has secrets*. An audience of 160,000 to 310,000 viewed the series. The OPDP's conclusion was somewhat more optimistic in 2006. Citing higher numbers of complaints, consultations, and requests for assistance, the OPDP believed that public awareness of data privacy was constantly increasing³⁴ and statistical data for 2008 and 2009 partially endorsed the tendency, although the unexpectedly higher rate of dismissed complaints in 2009 could mean that the general public might have been overestimating its rights.³⁵

In addition to its supervisory activities, the OPDP focuses on communication and education programmes. The OPDP launched an educational programme called "Protection of Personal Data in Education", supported by the Ministry of Education, Youth, and Sports in 2007; 2009 was the third consecutive year in the framework of further training of pedagogical workers.³⁶

Positive feedback from the campaign aimed at young children accompanied with the competition "My privacy! Don't look, don't poke about!" should emerge as a completely new project in 2011. Similarly, the OPDP also tries to disseminate information on privacy right among seniors in cooperation with Charles University.³⁷

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The relevant case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.³⁸

³³ Office for Personal Data Protection Annual Report 2005, at 2, available at http://www.uoou.cz/files/rep_2005.pdf.

³⁴ Office for Personal Data Protection Annual Report 2006, *supra* at 34.

³⁵ Office for Personal Data Protection Annual Report 2009, *supra*.

³⁶ Joint press release of the Chairman of the Article 29 WP and the President of the Office for Personal Data Protection in the Czech Republic within the framework of the European awareness campaign on Internet and minors, 8 March 2009, available at http://www.uoou.cz/files/wp29_statement.pdf. See also Section "Online youth safety," *infra*.

³⁷ Office for Personal Data Protection Annual Report 2009, *supra* at 65.

³⁸ Cfr. "National databases for law enforcement and security purposes," "Bodily Privacy," "Health & Genetic Privacy," *infra* in this Report.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Electronic surveillance, wiretapping, and the interception of mail by the police are regulated under the criminal process law and require a court order.³⁹ A judge can approve an initial wiretap order for up to four months – the previously applied period of six months shortened in 2008 when criticisms of the extensive use of interception led to the adoption of stricter rules. For example, the authorities are now required to inform any person who was subject to wiretapping about the interception once the case is closed, and such persons have the right, within the six-month period, to ask the Supreme Court to review the legality of the interception.

Although there are special rules for intelligence services (for substantiation of the court order), the wiretapping must be always allowed by a judge of High Court in Prague.⁴⁰

Another state authority that may use electronic surveillance, the tapping of telephones, and the interception of mail if approved by a court is the Customs Administration,⁴¹ due to the fact that Customs may use criminal techniques for the purpose of investigating financial crimes.

There is no comprehensive law on wiretapping; the Criminal Procedure Act is the most detailed and also contains remedies. The absence of proper public control of wiretapping, especially as conducted by intelligence services, is still often discussed as a concerning issue by politicians and media. In practice, the special commission of the Chamber of Deputies⁴² has almost no oversight power to deal with this issue. On the contrary, even such limited oversight is criticised due to the higher risk of leakage of confidential information.⁴³ Unlike the recently strengthened individuals' rights concerning electronic communication interception – as provided in the Criminal Procedure Act (requiring that the subject of telephone interception or remedial procedures with the Supreme Court be subsequently informed) – other types of eavesdropping (such as recording audio and video in public spaces outside an individual's home) need only be approved by the state attorney, and no specific remedy is provided for in this stage of criminal proceeding.⁴⁴

³⁹ Act No. 141/1961 Coll on Criminal Procedure, Section 88.

⁴⁰ Act No. 154/1994 Coll. on the Security Information Service; Act No. 289/2005 Coll. on Military Intelligence Agency.

⁴¹ Act No. 13/1993 Coll. on Customs.

⁴² *Komise pro kontrolu zpravodajské techniky* (Commission for Intelligence Technics Control).

⁴³ Karel Zetocha, "Parliamentary supervision of Intelligence Agencies" (Institute for European Policy, 2008), available in Czech at http://www.europeum.org/doc/pdf/Karel_Zetocha_skupinaII.pdf.

⁴⁴ Act No. 141/1961 Coll. on Criminal Procedure, *supra* at Section 158d.

In 2006 the President of the Office for Personal Data Protection, Igor Němec, cited the expansion in wiretapping surveillance as a factor in the average privacy protection ranking Privacy International conferred on the Czech Republic. Němec stated that he hoped to devote increased resources to the issue of securing access to police documents and ensuring that police recordings were in full accord with the law. He noted that "an alarmingly high number of persons can access police recordings," making it impossible to prevent leaks to the media.⁴⁵

That criticism found support from politicians, and in 2009 a new set of rules⁴⁶ was enacted to strengthen the protection of individuals who were subject to interception. Any unauthorised publishing of wiretapping records (i.e., those that were not publicly heard before a court) was specifically banned. In addition to the criminal sanctions imposed by a court (up to five years, should the leak be considered as a crime of unauthorised personal data handling), the OPDP acquired new power to apply penalties – anyone who breaks the ban may be fined up to CZK1 million (€50,000) or CZK5 million (€205,000) if committed via press, film, broadcasting, Internet, or any other similarly effective means. Given the fact that the OPDP has power to fine the breach only if it is not considered a crime, the maximum penalties are perceived as excessive due to non-discrimination rules between natural persons and companies. Initially the protective measure was nicknamed a “protectionist” measure known as a "muzzle law".⁴⁷ This came about because the measure precludes any journalist from publishing information on serious criminal cases (such as corruption) if such information comes from intercepted communication and no court hearing has yet taken place, thus, according to some legal opinions, restricting freedom of speech. The newest proposals are intended to enable journalists to publish information about participants in criminal proceedings relating to corruption among politicians or other state officials'.⁴⁸

There have been continuous attempts to legalise and expand secret service wiretaps. In 2001, there were attempts to add provisions granting the police and BIS powers to require telecommunications traffic and other information from public bodies to a bill that dealing with asylum law.⁴⁹ This was prepared by members of the Lower Chamber's Security and Defence Committee and apparently coordinated by the secret services. The Senate did not approve this part of the proposed law.

In April 2003, the government proposed an amendment to the Act on Security Information Service (SIS), which would entitle SIS to require information on

⁴⁵ Office of Personal Data Protection Annual Report 2006, *supra* at 3.

⁴⁶ Act No. 52/2009 Coll.

⁴⁷ More details on journalists' protests are available at <http://prisonforjournalists.com/EN/>.

⁴⁸ "Coalition Vows to Soften 'Muzzle Law'," *Prague Daily Monitor*, 24 July 2010, available at <http://www.praguemonitor.com/2010/07/26/coalition-vows-soften-muzzle-law>.

⁴⁹ Document of 30 April 2001, No. 921 of Chamber of Deputies, III election period.

telecommunications traffic, and impose a duty on telecommunications service providers to have wiretapping equipment. The Chamber of Deputies rejected this bill.⁵⁰

Under the 2005 Electronic Communications Act,⁵¹ telecommunication carriers are required to provide secure access to electronic communication information to the Czech Police (or Security Information Service and Military Intelligence Agency) in accordance with Article 88 of the Criminal Procedure Act. Under Section 97 of the Electronic Communications Act, such access includes the means by which the police may decrypt or decode messages (as encryption is used, for example, in GSM technology) in order to tap and record them. Section 97 of the Electronic Communications Act also requires carriers to retain operating and location data for a specified period of time,⁵² as well as a database holding information on all customers, and to permit the Czech police (or Security Information Service and Military Intelligence Agency) access upon legal request (granted by a court). Section 88 of the Electronic Communications Act requires telecommunications carriers to develop multiple means to protect the personal data of their users, and also requires that carriers inform their customers of specific disturbances in network security and, if necessary, ways to remedy data breaches. Without prejudice to Section 97 of the Electronic Communications Act, carriers must render anonymous any user operating and location data pursuant to Sections 90 and 91 once they are no longer necessary for the provision of communication services (unless further processing is necessary for the provision of supplemental services ordered by the user).

A new Police Act prepared during 2007 and adopted in 2008 contains several privacy-intrusive provisions, although fewer than originally proposed.⁵³ The Police Act enables police to exchange personal data with intelligence services. In addition, the new Act fails to provide any improvement on the rules for handling DNA samples. The new act allows police to use video surveillance in public places, again without any rules. The law also broadens the way in which police obtain retained communication data (including 24/7 online access).⁵⁴ A new competence to deactivate electronic communication channels (e.g., a mobile network) was given to the police. Only a last minute amendment made this power (as well as wiretapping and surveillance) subject to parliamentary control.

National security legislation

A document titled *Analysis of Security System of the Czech Republic (Analýza bezpečnostního systému ČR*, here the Analysis) prepared by the Ministry of the Interior

⁵⁰ Document of 29 April 2003, No. 308 of Chamber of Deputies, IV election period.

⁵¹ Act No. 127/2005 on Electronic Communications.

⁵² For more details, see Section "Data Retention", *infra*.

⁵³ Act No. 273/2008 Coll. on Police, available in Czech at <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb08273&cd=76&typ=r>.

⁵⁴ Description of the main features of the Act concerning privacy are available in Czech at <http://www.slidilove.cz/en/node/482>.

and based on the National Anti-terrorist Plan⁵⁵ drafted by the Lower Chamber's Defence and Security Committee, recommends extending the powers of the police and security services. In particular, it calls for an obligation on individuals and companies to provide their personal data to security services. This programme document is to be implemented by legislative proposals. The document also plans for public-private partnership in investments into security projects. The threat of terrorism is stated as the main reason for creating the Analysis. The United Kingdom's "Anti-terrorism, Crime and Security Bill" and the U.S. "Patriot Act" are quoted in the Analysis, as examples of desirable strengthening of investigation powers.

The currently applicable *Strategy against Terrorism* (covering the years 2010 to 2012)⁵⁶ reiterates the lack of necessary competence of law enforcement agencies in the Czech Republic compared to its foreign partner agencies. However, the only explicit proposal is to specify more clearly the obligation of email service providers to retain necessary operational data (but not the content of messages) and to implement the already enacted power granting police online access to data on the use of electronic payment devices (such as credit cards).⁵⁷

Data retention

The Czech Republic adopted data retention legislation in the middle of 2005, in anticipation of new EU legislation. It stipulates a maximum period of data retention for operating and location data of 12 months.⁵⁸ The recent amendment to the Act in the first half of 2008 improved the initial implementation and provided also for a minimum period of data retention of six months. Nevertheless, the implementing regulation providing for the exact retention period kept the original six months' period,⁵⁹ although data on Uniform Resource Identifiers used during the communication are to be stored for only three months. After these obligatory retention periods carriers must destroy the data. However, the wording of the amendment allows use of the databases for purposes other than those specified in the directive. Also, the present form leaves to the Minister of the Interior the decision on the scope of the retained data, which are far above the conditions set by the Data Retention Directive.⁶⁰

In 2007 the Police routinely used the data for investigations (including less serious offences); however, there are no publicly available statistics giving the number of

⁵⁵ Governmental resolution No. 385 of 10 April 2002, available in Czech at http://kormoran.vlada.cz/usneseni/usneseni_webtest.nsf/0/3AE4ABCAC2919A80C12571B6006F37B9.

⁵⁶ *Strategie boje proti terorismu*, available at <http://www.mvcr.cz/soubor/nap-2010-pdf.aspx>.

⁵⁷ *Cfr.* Section "Data Retention," *infra* in this report.

⁵⁸ Act No. 127/2005 Coll. on Electronic Communications, *supra*.

⁵⁹ Regulation No. 485/2005 Coll.

⁶⁰ Helena Svatosova, "Czech Parliament - Close in Implementing Data retention Directive", EDRI-gram, 4 June 2008, available at <http://www.edri.org/edriagram/number6.11/czech-data-retention>.

investigations, neither of accesses nor of the efficiency of the measure,⁶¹ even though the Czech Telecommunication OPDP has received such information from all carriers annually since 2009.

National databases for law enforcement and security purposes

The Bill of law on Protection of Classified Information⁶² granted powers to secret services to require personal data from various public and even private databases (social security system, health insurance institutions, private insurance companies, banks, etc.) for purposes of "security proceedings."⁶³ During 2004, a coalition of NGOs (Iuridicum remedium, Transparency International ČR, and Open Society) raised objections to this provision in the phase of pre-parliamentary proceedings. In February 2005, the unchanged bill was submitted to Parliament. However, the coalition of above-named NGOs prepared proposals to omit these provisions and asked several MPs to raise these proposals in legislative procedure. They were partially successful in the Defence and Security Committee, but Section 58 of the final version of the Bill still permitted all members of the government access to otherwise classified information without a security clearance, although they must still keep the information confidential. The bill also allowed for some technical activities (certification of cryptographic or technical facility or electromagnetic rays measuring in order to qualify equipment to classified information disposal) to be done by private companies and sole entrepreneurs. The Act came into force on 1 January 2006.⁶⁴

The OPDP also expects a continued emphasis on data mining by police and customs groups. The data processing of greatest interest is related to Europol, Eurodac, Schengen Information System (SIS), and technology development work for customs systems.⁶⁵

The OPDP paid particular attention to the processing of DNA-related personal data. A control was carried out in 2008 targeting the Institute of Criminalistics of the Police of the Czech Republic, the operator of the National DNA Database.⁶⁶ Violations of the Act on Personal Data Protection were found, as sensitive data were collected, processed and stored to an extent that went beyond the statutory authorisation. In such cases the law

⁶¹ Filip Pospíšil, Marek Tichý, "Key Privacy Concerns in Czech Republic 2007," EDRI-gram, 30 January 2008, available at <http://www.edri.org/edriagram/number6.2/privacy-czech-2007>.

⁶² Documents No. 880 and 881 of 27 January 2005 of Chamber of Deputies, IV. election period.

⁶³ Proceedings according to Law on Protection of Classified Information, which include screening of person who applied for certificate allowing access classified information.

⁶⁴ Act No. 412/2005 Coll. on the Protection of Classified Information, 2005.

⁶⁵ See E-mail from Ivan Procházka, Head of Department of Foreign Relations for the Office for Personal Data Protection, Czech Republic, to Clifford Chen, Law Clerk, Electronic Privacy Information Center, 11 June 2004, (on file with EPIC). As far as SIS is particularly concerned see also <http://www.uoou.cz/uoou.aspx?menu=133&lang=en>.

⁶⁶ 12th Annual Report of the Art. 29 Data Protection Working Party (2008), 16 June 2009, at 26, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

requires that the consent of the person concerned is obtained, but this had not occurred. One aspect of the control conclusions was the imposition of a fine and a remedy measure, namely the destruction of personal data processed in a manner contrary to the law.⁶⁷

On 1 July 2010, the Act on Basic Registers took effect. The Act on Basic Registers provides for the interconnection of four core registers administered by public authorities (Elementary Register of Inhabitants of the Czech Republic; Elementary Register of Corporate Entities, Natural Persons and Authorities; Elementary Register of Territorial Identification, Addresses and Real Estates; Elementary Register of authorities' agendas and some of their powers and duties) that will be implemented through the special information system. Legislative process leading to adoption of the respective legal measures was unusually swift. Despite the short legislative process, the OPDP was consulted. Some of the comments of the OPDP were incorporated into the Act and the OPDP generally welcomed the final version of the bill.⁶⁸

According to proponents, the new system will prevent some of the dysfunction of the present system of different registers that are used individually by state authorities (fragmentation, ambiguity, and multiplicity in the maintenance of key public administration databases). Thanks to the new system: citizens should be no longer be forced to repeatedly provide their personal data for each different database; the introduction of a system of agenda identifiers of natural persons derived from agenda code and the source identifiers should allow each officer to access only the personal data necessary for administration of his/her agenda; agenda of creation and distribution of the electronic identifiers (ensuring the inability of one authority to access other data relating to a particular individual or company processed by another authority) for basic registers will be administered by the OPDP. The system of basic registers is expected to enter full operational level in July 2012. Practical issues, including privacy concerns, are yet to be tested.

National and international data disclosure agreements

Security interests clashed strongly with privacy interests as the United States began to demand that the Czech air carrier CSA provide data on all its passengers. Terrorism was cited as the rationale for this demand, and there were threats of fines and denial of U.S. landing rights in case of non-compliance. CSA agreed to provide the requested data, but the release was likely to infringe existing privacy laws. CSA had been granted permission from the Data Protection Office to transfer the data, but its validity was limited by the Czech Republic's accession to the European Union in May 2004. CSA has also increased checks of airport property, passengers, luggage and transported goods.⁶⁹

⁶⁷ *Id.*

⁶⁸ Office for Personal Data Protection, Press release, 29 April 2009, available in Czech at <http://www.uoou.cz/uoou.aspx?menu=15&loc=768>.

⁶⁹ United Nations Security Council, Report by the Czech Republic to the Counter-Terrorism Committee, S/2001/1302, 9- 10.

On 26 February 2008, the Czech Minister of Interior and U.S. Homeland Security Secretary signed the Memorandum of Understanding on Passenger Name Records.⁷⁰ In exchange for continued access to the visa waiver programme, Czech authorities agreed to collect, use, analyse, and share Passenger Name Records (PNRs) as well as Advance Passenger Information (API). Neither the procedure nor the amount of data to be provided has been specified. The European Commission drafted the Memorandum independently of the recent EU-USA negotiations on this topic that resulted in sharp criticism. However, similar documents between the USA and five other EU member states, Lithuania, Latvia, Estonia, Slovakia, and Hungary, followed.⁷¹

Cybercrime

Recently, the Government established the Joint Coordination Committee for Security in the Cyberworld, which should deal with various tasks related to cybercrime, mostly on the analysis level.⁷² Due to the very recent formation of the Committee, no output is yet known.

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

The Certain Information Society Services Act was approved at the end of 2004.⁷³ It addresses spam and limits the liability of providers as far the content of communicated information is concerned.

The application of the new supervisory competence of the OPDP in the field of unsolicited commercial communications under the Certain Information Society Services Act, which implements provisions of the EU Directive on Privacy and Electronic Communications,⁷⁴ brought considerable enlargement of the agenda of handled complaints. The Certain Information Society Services Act introduced new duties in the sphere of dissemination of commercial communications. The Act established the Office's Control Department as a supervisory body for commercial electronic communications,

⁷⁰ Memorandum on Understanding between the Ministry of Interior of the Czech Republic and the Department of Homeland Security of the United States of America, 26 February 2008, available at <http://www.poptel.org.uk/statewatch/news/2008/mar/us-czech-mou-visas-etc.pdf>.

⁷¹ *Id.*

⁷² Governmental Resolution No. 380 of 24 May 2010, available in Czech at [http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/17A2B3E12781C958C125773600365557/\\$FILE/380%20uv100524.0380.pdf](http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/17A2B3E12781C958C125773600365557/$FILE/380%20uv100524.0380.pdf)

⁷³ Act No. 480/2004 Coll.

⁷⁴ Email from Ivan Procházka, *supra*. See also Office for Personal Data Protection, Annual Report 2004, *supra* at 41.

including email, faxes, texting, and telemarketing. Such communications must abide by an opt-in principle whereby the messages may only be sent to those who have given prior consent, unless the addressee is already a customer of the sender. An entity sending a commercial communication must be able to demonstrate the consent at any time, such provision not excluding also that the entity has to keep electronic records on obtained consent.

In 2007, the OPDP received 1,569 complaints regarding unsolicited commercial communications. The OPDP dealt with 1,012 complaints concerning 515 subjects. Of these, 466 subjects were asked to implement corrective measures, while 71 subjects were fined a total amount of CZK437,000 (€19,500).⁷⁵ The OPDP found that most commercial entities did not consistently comply with the opt-in principle, nor were their communications clearly and plainly designated as commercial, as required by the Act. In 2008, the OPDP had to deal with 1,458 complaints on unsolicited commercial communications and investigated 155 cases. In 2009 the OPDP dealt with 2,261 complaints and investigated 145 cases. The overall amount of imposed fines rose to CZK797,000 (€32,500).

At the end of 2004 authorities endowed with anti-spam enforcement powers from 13 European countries including the Czech Republic (represented by the OPDP) established the CNSA – Contact Network of Spam Enforcement Authorities – as a common platform for cooperation in investigating complaints about cross-border spam within the EU, and enforcing Article 13 of the Privacy and Electronic Communication Directive 2002/58/EC.⁷⁶ The CNSA meets three to four times per year, and it has set up a cooperation procedure that aims to facilitate the transmission of complaint information or other relevant intelligence between National Authorities. The CNSA is an active member of the StopSpamAlliance.⁷⁷

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

⁷⁵ Jiří Malich, "Spam v Česku: ÚOOÚ si nemyslí, že je to tak hrozné," ("Spam in the Czech Republic: The Office for Personal Data Protection Does Not Find It that Grave,"), Lupa.cz, 6 July 2008, at <http://www.lupa.cz/clanky/spam-v-cesku-uouu-si-nemysli-ze-je-to-tak-hrozne/>.

⁷⁶ See email from Ivan Procházka, *supra*.

⁷⁷ StopSpamAlliance information page, at http://stopspamalliance.org/?page_id=11. The StopSpamAlliance is a joint international effort initiated by APEC, the CNSA, ITU, the London Action Plan, OECD and the Seoul-Melbourne Anti-Spam group.

Online youth safety

As previously mentioned, a programme prepared for teachers by the OPDP, which has received three-year accreditation from the Ministry of Education, Youth and Sports, has also been initiated.⁷⁸ In addition, the second annual art and literature competition for children and young people "My privacy! Don't look, don't poke about!" was held. This time, children from SOS villages in the Czech Republic, Ukraine, Kazakhstan, Russia, and Bosnia-Herzegovina also successfully took part in the competition. The OPDP welcomed this cooperation because it considers it necessary that children preparing for their future life while growing up outside a family are also sufficiently informed about their rights.⁷⁹

TERRITORIAL PRIVACY

Video surveillance

Increasingly, video surveillance - closed circuit television (CCTV) systems - is being used by both private institutions and local governments. Although using CCTV and other camera systems for recording is considered to be processing personal data, few organisations using such systems have registered with the OPDP, although this is a legal duty imposed by the Personal Data Protection Act. The OPDP has very limited capacity for oversight and therefore, does not penalise those routine breaches of law. Although no particular legal duties concerning video surveillance conditions are embodied in any law (e.g., duty of notice, maximum period of storage of records, ban on data attachments, no discrimination on the basis of record), such obligations could be clearly deduced from the general principles stated in the Personal Data Protection Act; of course, it is not as illustrative as a special law or legal provision on CCTV could be.

The OPDP fielded inquiries from a wide variety of sources on the subject, including police bodies, courts, public administration, municipal government, economic entities, trade unions, apartment cooperatives, and many individuals. In 2005, the OPDP levied a fine on a housing co-operative that installed a camera monitoring system in the building without tenants' consent.⁸⁰ The OPDP action was confirmed by a court's decision in 2007⁸¹ stating that the video surveillance connected with electronic entrance system (logging and archiving each entry to a house) was not an appropriate and proportional method for achieving the purpose of the protection of property, although the initial installation of CCTV was driven by a series of vandalism including personal attacks. In January 2006, the OPDP issued Position No. 1/2006, reiterating that the operation of a video recording system is considered personal data processing if it can identify

⁷⁸ *Cfr.* Section "Data Protection Authority," *supra*.

⁷⁹ 12th Annual Report of the Art. 29 Data Protection Working Party (2008), *supra*.

⁸⁰ Office for Personal Data Protection, Decision No. 01428/05-UOOU, 6 May 2005.

⁸¹ Municipal Court in Prague, Case No. 7 Ca 204/2005,, 28 February 2007.

individuals, and thus must serve a legally protected interest and not excessively interfere with an individual's privacy.⁸²

There have been two significant cases where the use of video surveillance has caused a public outrage. In 2006-2007 students of the private *Skvoreckeho* College in Prague launched a public protest against the constant video surveillance at all school premises including classes. Fully supported by their parents and media reports, the students managed to force the school management to remove the CCTV systems.

In 2007, the operator of the municipality CCTV system in Plzen used the cameras for monitoring car traffic that looked into the windows of a private flat opposite. The images were kept online through a public streaming site. The owner of the flat has complained. The case was well covered by the media and condemned as a misuse of the CCTV system. The OPDP launched an investigation.

In 2008, the OPDP released a position on the installation of camera systems in apartment buildings, stating that "[e]ach controller must demonstrate in his or her plan for the use of a camera system that the camera system is: demonstrably suitable for resolving the problem in question, demonstrably necessary for resolving the specific problem, appropriate given, for example, its contribution to security, regularly reviewed to ensure the above points are satisfied, and that it intrudes on privacy demonstrably less than the alternatives."⁸³

In 2009, a representation from the Government's Council on Human Rights led to the adoption of an instruction to the Ministry of the Interior to prepare detailed rules on video surveillance during 2010.⁸⁴

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this section.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The Czech authorities launched a first version of the Czech electronic passport at full scale in September 2006. Issued in compliance with the requirements laid down in the European Union regulation regarding passport security and biometrics,⁸⁵ the passports

⁸² Office for Personal Data Protection, Position No. 1/2006 (January 2006), available at <http://www.uouu.cz/uouu.aspx?menu=22&loc=570>.

⁸³ Office for Personal Data Protection, Position No. 1/2008 (May 2008), available at <http://www.uouu.cz/uouu.aspx?menu=22&loc=575>.

⁸⁴ Governmental Resolution No. 1454 of 30 November 2009, available in Czech at [http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/CFEEC5B0F51F2B43C125768200315CF1/\\$FILE/uv091130.1454.doc](http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/CFEEC5B0F51F2B43C125768200315CF1/$FILE/uv091130.1454.doc).

⁸⁵ Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 13 December 2004, OJ L 385, 29 December 2004, at 1–6, available at http://eur-lex.europa.eu/Result.do?idRoot=4&RechType=RECH_typact&typact=LEG_V111&typihm=Regulations.

include new security features such as intricate designs and complex watermarks, as well as a chip and antenna. The chip stored the electronic facial scan of the owner along with his/her personal details. Facial recognition maps various features on the face, for example, the distances between eyes, nose, mouth and ears. It was planned to add fingerprint details on the chip at a later stage.⁸⁶

As planned, on 1 April 2009, the Czech authorities started rolling out new electronic passports whose chip include, in addition to the existing information, two fingerprint images of the owner.

Since 2007, the project "Opencard" (electronic card used mostly as a ticket for the mass transit in Prague) has been regularly discussed in relation to the protection of personal data that should be used for the operation of the project, the most recent investigation being held in 2009.⁸⁷ Due to the potential of collection of various personal data (including on movement) and the vulnerability of the card itself (RFID technology) the Prague Magistrate finally announced that anonymous cards will be used in the future (at the end of 2009, more than 350 thousand of cards have been issued).⁸⁸

INATIONAL ID& SMART CARDS

In August 2006 the OPDP issued Position No. 08/2006 with regard to the issuance of electronic cards. According to the position, such cards are being increasingly used in many areas of everyday life, including to gain entry to buildings and to obtain discounts and various services. The Position noted that personal data is collected in practically all instances in which such cards are produced, thus certainly bringing such activity within the competence of the OPDP's authority under the Personal Data Protection Act. The Position advised cardholders to exercise caution and card issuers to observe the law regarding privacy protection.⁸⁹

RFID tags

No specific information has been provided under this section.

⁸⁶ ePractice, eGovernment Factsheet – Czech Republic– National Infrastructure (April 2010), available at <http://www.epractice.eu/en/document/288201>.

⁸⁷ Office for Personal Data Protection Annual Report 2009, *supra*.

⁸⁸ "Fotka a jméno: konečně opencard bez zbytečných osobních údajů?" ("Photo and First Name: Last Opencard without Unnecessary Personal Data?"), *Econnect*, 20 July 2010, available at <http://zpravodajstvi.ecn.cz/index.stm?x=2237715>.

⁸⁹ Office for Personal Data Protection, Position No. 8/2006 (2006), available at <http://www.uoou.cz/uoou.aspx?menu=22&loc=573>.

BODILY PRIVACY

In 2005 the OPDP imposed a fine on a state body for scanning biometric data and pictures of fingerprints. The data was acquired in violation of law as a matter of routine.⁹⁰

In 2007, there was a substantial expansion of the number of DNA samples and profiles up to 40,000 records. The amendment to the Police Act and Penal Code adopted in the first half of 2006 introduces new measures that boost the growth of the national DNA database and worsen privacy protection.⁹¹ Although the police had specific powers for DNA sampling since 2001, the amendment of 2006 enabled the use of force to obtain DNA samples (and such provision was kept also in the new Act on Police from 2008⁹²).

Persons charged with criminal activity and prisoners serving sentences for committing deliberate crimes may be subject to DNA sampling for possible future identification. The latter caused new public debate on the extent of involuntary DNA sampling as during 2007, approximately 16,000 prisoners were (in some cases forcibly) coerced into providing their DNA samples. The media have questioned this practice, and the public ombudsman condemned it in his statement.⁹³ The ombudsman questioned the constitutionality of this practice applied on a large scale without proper substantiation (DNA sampling also covered criminals who committed deliberate crimes, including, for example, economic frauds) and also of the very existence of the National DNA Database, which lacks appropriate legal backing. The ombudsman also initiated review of the case by the OPDP and Public Prosecution Office. The OPDP's investigation on the National DNA database led to more systematic activity on the part of the OPDP, including a special seminar on the topic in the Senate (the upper chamber of the Czech Parliament).⁹⁴ The OPDP currently leads an expert working group with the aim of preparing a comprehensive law on handling DNA.⁹⁵ The scientific community is also pursuing demands for a special law on the National DNA database and genetic testing.⁹⁶

WORKPLACE PRIVACY

Employer monitoring of employees' email is an important issue. The Data Protection OPDP issued a legal opinion finding employers' reading of the content of employee's

⁹⁰ See 9th Annual Report of Article 29 Working Party on Data Protection (2005), 14 June 2006, at 29, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

⁹¹ Act No. 321/2006 Coll.

⁹² Act No. 273/2008 Coll. on Police, *supra* Section 65.

⁹³ Statement available in Czech at <http://www.ochrance.cz/stanoviska-ochrance/zasadni-stanoviska/stanoviska-2008/z-odber-vzorku-dna-odsouzenym-a-obvinenym/>.

⁹⁴ Materials from the seminar available at <http://www.uoou.cz/uoou.aspx?menu=15&loc=653>.

⁹⁵ Office for Personal Data Protection, Press release, 21 January, 2010 available in Czech at <http://www.uoou.cz/uoou.aspx?menu=15>.

⁹⁶ E.g., Daniel Vaněk (genetic researcher and former forensic specialist) "Právo a DNA" ("Law and DNA"), *Reflex Weekly*, 28 May 2008.

email to be illegal. However, the OPDP allowed monitoring the subject lines of employees' email correspondence. Scholars and practitioners broadly discussed this issue. The Electronic Communications Act of 2005 stipulates that the location and ownership of electronic equipment cannot compromise an individual's right to confidentiality in communications. However, little debate has occurred to date as to the precise line between an employee's right to privacy and an employer's authority and economic interests.⁹⁷

HEALTH & GENETIC PRIVACY

Medical records

The status of medical registries in the Czech Republic is a privacy issue of continued importance. The Czech Republic maintains a number of medical registries that consolidate information from groups such as oncology patients, expectant mothers, women who undergo abortions, people with professional diseases, and drug addicts.⁹⁸ The legal status of these registries was uncertain, as they had existed on the basis of lower-level legal regulations that could not be maintained after January 2004. The Czech Medical Association advised doctors in February 2004 to refrain from providing data to the national registers to reduce the risk of liability for infringement of privacy laws.⁹⁹ A bill allowing for the continued operation of the registries and use of birth identification numbers passed the Chamber of Deputies but was vetoed by President Vaclav Klaus, who preferred that registry data be entirely anonymous, citing privacy concerns echoed by the Data Protection Office. The Chamber of Deputies overrode President Klaus's veto in March 2004, however, creating the necessary legal basis for the medical registries.¹⁰⁰

In 2009, the OPDP investigated and confirmed the illegal processing of patients' personal data by the State Institute for Drug Control when operating the central archive of prescriptions without proper legal background. Furthermore, the OPDP expressed its concerns regarding a new, related legislative proposal.¹⁰¹ The major objection to the bill was that it would exceed the purpose of the archive (initially intended to reduce the overall consumption or even misuse of drugs) by a wide margin, creating room for the advanced features of the archive to contravene patients' rights.

⁹⁷ European Industrial Relations Observatory Online, "New Technology and Respect for Privacy at the Workplace," 10 April 2007, available at <http://www.eurofound.europa.eu/eiro/2007/02/articles/cz0702029i.html>.

⁹⁸ "Chamber Approves Medical Registers, Overriding Klaus's Veto," CTK National News Wire, 24 March 2004.

⁹⁹ "CLK Appeals to Doctors not to Send Data Statements to Register," CTK National News Wire, 20 February 2004.

¹⁰⁰ Act No. 156/2004 Coll., amending Act on Public Health Care (2004).

¹⁰¹ Document No. 1056 of 24 February 2010, Chamber of Deputies, V. election period. The bill was not adopted.

Genetic identification

Based on complaints and investigations, the OPDP inspected targeted private companies performing genetic paternity and kinship testing for identification for commercial purposes, as well as DNA analysis for research and for the testing of genetically conditioned types of illness and predicting the efficacy of their treatment.¹⁰² Violations of several provisions of the Act (the duty of notification, consent that did not cover all use of data, certain aspects of proportionality, etc.) were found and a fine and remedy measures were imposed.¹⁰³

FINANCIAL PRIVACY

The law-amending Act on Measures against Money Laundering (implementation of EU *acquis*),¹⁰⁴ proposed by the government in March 2003, aimed to limit lawyer-client privilege and obliged solicitors to report their client's "suspicious" financial transactions to the Ministry of Finance. Resistance and lobbying by Czech Bar Association led to a less intrusive text of the Act. Suspicious activities are reported via the Czech Bar Association, which serves as the control body. This wording appears in the final text of the Act, which was approved in April 2004.¹⁰⁵

E-GOVERNMENT& PRIVACY

No specific information has been provided under this section.

OPEN GOVERNMENT

The Parliament approved the Freedom of Information Law in May 1999.¹⁰⁶ The law provides for citizens' access to all government records held by State bodies, local self-governing authorities, and certain other institutions, except for classified information, trade secrets, or personal data.¹⁰⁷ Section 8 of the Law stipulates that information revealing evidence of one's personality and privacy, especially with regard to race, nationality, membership in political parties and movements, religion, health, sexual life, and property, may not be disclosed without prior written consent by the relevant individual or without authorisation by a special law.¹⁰⁸ In 2002, the government rejected a Senate-sponsored amendment to the Law that would have required applicants to pay only

¹⁰² 12th Annual Report of the Art. 29 Data Protection Working Party (2008), *supra*.

¹⁰³ *Cfr.* Section "National databases for law enforcement and security purposes," *supra*.

¹⁰⁴ See Directive 2001/97/EC of the European Parliament and of the Council amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, 4 December 2001, Official Journal L 344, 28 December 2001, at 76–82.

¹⁰⁵ Act No. 284/2004 Coll., amending Act on Measures against Money Laundering and other laws (2004).

¹⁰⁶ Act No. 106/1999 Coll., on Free Access to Information.

¹⁰⁷ "Freedom of Info Clears Last Hurdle," *The Prague Post*, 19 May 1999.

¹⁰⁸ Act No. 106/1999 Coll. *supra*.

for material costs rather than having to pay for the costs associated with searching.¹⁰⁹ Since 2006, the applicants may only be required to pay for costs associated with searching in cases of exceptionally extensive searching.¹¹⁰

A 1998 act governs access to environmental information.¹¹¹ In April 1996, Parliament approved a law that allows any Czech citizen to obtain his or her file created by the Communist-era secret police (StB). Non-citizens are not allowed to access their records. The Interior Ministry holds 60,000 records, but it is estimated that many were destroyed in 1989.

In 2003, the Interior Ministry decided to publish a list of Communist StB secret service collaborators. The Office for the Protection of Personal Data, which offered comments on the original legislation that allowed for the release of the information, stated that such a release would not be in conflict with the law on the protection of personal data.¹¹²

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

Iuridicum Remedium (IuRe) is an NGO in the Czech Republic specialised in the field of digital rights and privacy.¹¹³ Its activities are wide-ranging in scope, covering both lobbying at the stage when laws are being drafted and campaigning against existing and actual threats.

Since April 2007, IuRe has campaigned against the irresponsible use of RFID chips in the new multifunctional municipal cards in Prague (Opencard). IuRe proved that in the initial stage of the project, it was possible to harvest personal data from its chip simply with the knowledge of publicly accessible security key. Since that time, the issuer of the Opencard ceased storing data on the chip, enabling IuRe to concentrate on criticising discrimination against those who wish to use the card anonymously.

In June 2008, IuRe succeeded in proposing significant changes to the proposed Police Act. IuRe helped, for example, to set up stricter rules for police concerning local disturbance of the mobile and computer networks and police legally based access to

¹⁰⁹ "Czech Cabinet Rejects Legislation Facilitating Access to Information," CTK News Agency, 5 August 2002.

¹¹⁰ Act No. 106/1999 Coll., *supra* at Section 17(1).

¹¹¹ Act No. 123/1998 Coll. on the Right to Information About the Environment.

¹¹² "Internet Publication of Czech Communist Era Agents' Names Legal," CTK news agency, 17 March 2003.

¹¹³ Iuridicum Remedium's Web site, at <http://www.iure.org/>.

media in case of emergency. However, campaign activities continue as the Police Act leaves unclear the conditions of use for police CCTVs.¹¹⁴

The Czech Big Brother Awards (organised by Privacy International and IuRe) announced the 2007 winners.¹¹⁵ The Ministry of the Interior received the Lifetime Menace award for having ignored basic citizen privacy protection rights in establishing the National Action Plan of Fighting Terrorism (NAP). The plan also includes the establishment of a national database of biometric data for verification of travel documents. The NAP for 2007 to 2009 period also contains concepts for further spreading of camera systems and for wider access to data, access to location data, and further telecommunication data.¹¹⁶

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

The Czech Republic announced its succession to the International Covenant on Civil and Political Rights and to its First Optional Protocol establishing an individual complaint mechanism on 22 February 1993.¹¹⁷

The Czech Republic is a member of the Council of Europe and in 1992 signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms, which entered into force on 1 January 1993.¹¹⁸ The Czech Republic also signed and ratified the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data¹¹⁹ and its Additional Protocol regarding supervisory authorities and transborder data flows.¹²⁰ Although the Czech Republic became a signatory to the European Council's Convention on Cybercrime in February 2005, it has not yet ratified the treaty.¹²¹

¹¹⁴ IuRe, "EDRI Welcomes 5 New Members", EDRI-Gram - No 3.16, 10 August 2005, available at <http://www.edri.org/edrigram/number3.16/newmembers>.

¹¹⁵ Filip Pospisil, "Czech Republic Big Brother Awards 2007," EDRI-Gram - No 5.24, 19 December 2007, available at <http://www.edri.org/edrigram/number5.24/bba-czech-republik>.

¹¹⁶ Czech Big Brother Awards 2007, in Czech at http://www.slidilove.cz/zpravy/nejvetsi_slidilove_opet_odhaleni.html.

¹¹⁷ Czechoslovakia had signed the International Covenant on 7 October 1968 and ratified it on 23 December 1975. It acceded to the Optional Protocol on 12 March 1991. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹¹⁸ Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS No. 105). Text and other relevant information concerning all the Conventions adopted within the Council of Europe are available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

¹¹⁹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), signed on 8 September 2000, ratified on 9 July 2001 and entered into force 1 November 2001.

¹²⁰ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows (ETS No. 181), signed on 10 April 2002, ratified on 24 September 2003 and entered into force on 1 July 2004.

¹²¹ Convention on Cybercrime (ETS No. 185).

The Czech Republic is also a member of the Organisation for Economic Cooperation and Development (OECD). It has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In April 2010, the Privacy and Data Protection Commissioners' Conference took place in Prague. The OPDP undertook to make an inventory of the projects and campaigns organised or initiated by the European Data Protection Authorities so as to facilitate the exchange of experience and to intensify cooperation between all the data protection authorities.¹²² The conference was concluded by adopting four resolutions: on use of body scanners on airports, on the planned EU-USA agreement on privacy standards in the police and judicial cooperation in criminal matters, on future development of privacy protection, and on common steps towards better awareness and education of young people on European and international level.¹²³

* Updates to the Czech Report published in the 2010 edition of EPHR have been provided by: Richard Otevřel, Havel & Holásek, Czech Republic.

¹²² Joint press release of the Chairman of the Article 29 WP and the President of the Office for Personal Data Protection in the Czech Republic within the framework of the European awareness campaign on Internet and minors, *supra*.

¹²³ Minutes from the conference and text of the resolutions are available in Czech at <http://www.uoou.cz/uoou.aspx?menu=15&loc=689>.

KINGDOM OF DENMARK

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Danish Constitution of 1953 contains two provisions relating to privacy and, indirectly, to data protection. Section 71 provides for the inviolability of personal liberty. Section 72 states, "The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute."¹ Section 72 also applies to all kinds of telecommunication and electronic data. The European Convention on Human Rights (ECHR)² was ratified in 1953 and was formally incorporated into Danish law in 1992.³

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Act on Processing of Personal Data (the Act or PPD) entered into force on 1 July 2000.⁴ The Act implements the European Union (EU) Data Protection Directive 1995/46/EC into Danish law. It replaces the Private Registers Act of 1978, which governed the private sector,⁵ and the Public Authorities' Registers Act of 1978, which governed the public sector.⁶ The law divides personal information into three categories: ordinary, sensitive, and semi-sensitive, and provides different conditions for the processing of each.⁷ According to Section 2 (2), the Act shall not be applied if doing so is contradictory to the freedom of expression and information as stipulated in Article 10 of the European Convention on Human Rights. An exemption from the Act is provided for the Danish Security Intelligence Service (*Politiets Efterretningstjeneste* or PET) and the Danish Defence Intelligence Service (*Forsvarets Efterretningstjeneste* or FE).

According to PPD Section 7 (1) there may be no processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union

¹ Constitution of Denmark 1953, available at http://www.servat.unibe.ch/icl/da00000_.html.

² Convention for the Protection of Human Rights and Fundamental Freedoms CETS No. 005.

³ Act No. 285 of 29 April 1992.

⁴ *Lov om behandling af personoplysninger* (Act on Processing of Personal Data), Act No. 429 of 31 May 2000, available at <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/>.

⁵ *Lov nr 293 af 8 juni 1978 om private registre mv* (Private Registers Act of 1978), in force 1 January 1979.

⁶ *Lov nr 294 af 8 juni 1978 om offentlige myndigheders registre* (Public Authorities' Registers Act of 1978), in force 1 January 1979.

⁷ Peter Blume et al., *Nordic Data Protection 19-20* (DJOEF Publishing Copenhagen 2001).

membership, or data concerning health or sex life. Exceptions can be allowed under certain conditions.

Private controllers must in most cases obtain the authorisation of the Danish Data Protection Agency before processing data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sexual relations, criminal offences, serious social problems, or other purely private matters.

An exemption from the Act is provided in Section 2, subsections 5 and 11, for processing performed on behalf of *Folketinget* (the Danish Parliament) and its related institutions, the Danish Security Intelligence Service and the Danish Defence Intelligence Service. According to Chapter 17 of the PPD, the Danish Court Administration supervises the processing of data carried out on behalf of Danish courts. According to Section 2, subsection 4, some of the rules in the Act do not apply to the processing of data that is performed on behalf of the courts, the police or the prosecution in the area of criminal law.⁸

The PPD and the Act on Public Administration were amended by Act No. 503 of 12 June 2009. From 1 July 2009 the PPD, Section 1(3), also regulates the manual transfer of personal data between public authorities. Before this date this processing operation was regulated by Act on Public Administration, Section 28(1-3). Transfer of confidential and non-confidential personal information between public authorities has been somewhat expanded (PPD Section 8(2) No. 3), since the amended PPD now allows for the transfer of sensitive information if it is necessary for case-handling for the receiving authority.⁹

⁸ Chapter 8 (information given to the data subjects) and Chapter 9 (the data subject's right of access to data) as well as Sections 35-37 (e.g. provisions about the data subject's right to object and the controller's duty to rectify, erase, or block data in some cases) and Section 39 (provision about the data subject's possibility to object against decision which produce legal effects concerning him/her or significantly affecting him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects) do not apply for processing of data, which is performed on behalf of the courts in the area of criminal law. Further, chapter 8 as well as Sections 35-37 and 39 do not apply for processing of data, which is performed on behalf of the police or the prosecution in the area of criminal law.

⁹ See *Datatilsynets årsberetning 2008 og 2009* (DPA Annual Report 2008 and 2009), at 20-21, available in Danish at http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/AArsberet_2008_og_2009.pdf

Sector-based laws

Rules on data protection are a part of many Danish statutes¹⁰ among which there are: the Penal Code,¹¹ the Statute on Financial Institutions,¹² the Public Administration Act,¹³ the Act on the Central Personal Data Register,¹⁴ the Act on Social Services,¹⁵ the Marketing Act,¹⁶ the Act on the DNA Profile Register,¹⁷ and the Administration of Justice Act.¹⁸ Sectoral laws also provide special protections for medical information,¹⁹ information about customers of financial businesses²⁰ and payment services details,²¹ and lay down restrictions on direct marketing (including spam).²² If they are in accordance with Denmark's international obligations, these sectoral laws take priority over the general Data Protection Act.²³

DATA PROTECTION AUTHORITY

The Danish Data Protection Agency (*Datatilsynet* or DPA) enforces the Act. The DPA is an independent public body consisting of a council and a secretariat. The Minister of Justice appoints the members of the council. Section 56 of the PPD states that the DPA shall act with complete independence in executing the functions entrusted to it. Neither the Ministry of Justice nor any other public body has instructive authority over the DPA, but the agency is attached to the Ministry of Justice regarding recruitment of staff and

¹⁰ See Peter Blume, Country Studies: A.2 – Denmark, in Douwe Korff (Ed.), *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, European Commission DG JFS, May 2010, at 2, available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A2_denmark.pdf.

¹¹ Act No. 1068 of 6 November 2008.

¹² Act No. 897 of 4 September 2008.

¹³ *Lov 2007-12-07 nr. 1365 Forvaltningslov* (Act No. 1365 of 7 December 2007).

¹⁴ Act No. 1134 of 20 November 2006.

¹⁵ Act No. 58 of 18 January 2007.

¹⁶ Act No. 1389 of 21 December 2005.

¹⁷ Act No. 434 of 31 May 2000.

¹⁸ Act No. 1069 of 6 November 2008.

¹⁹ *Lov 2010-07-13 nr. 913 Sundhedsloven* (Act No. 913 on Danish Health of 13 July 2010).

²⁰ *Lov 2010-09-23 nr. 1125 om finansiel virksomhed* (Act No. 1125 on Financial Business of 23 September 2010).

²¹ *Lov 2009-05-25 nr. 385 om betalingstjenester* (Act No. 385 on Payment Services of 25 May 2009).

²² *Lovbekendtgørelse 2009-08-31 nr. 839 om markedsføring* (Consolidated Act on Marketing Practices No. 839 of 31 August 2009).

²³ Peter Blume *et al.*, *supra*.

budgetary issues.²⁴ Furthermore, the Minister of Justice appoints the members of the data council.

The DPA supervises registries established by public authorities and private enterprises in Denmark. It ensures that the conditions for registration, disclosure, and storage of data on individuals are complied with. It mainly deals with specific cases based on inquiries from public authorities or private individuals, or cases taken up by the agency on its own initiative. Staff of the DPA is allowed to enter any premise where a file is operated without a court order. Section 58 of the Act on Processing of Personal Data states that the DPA shall see to it that the processing of personal data is carried out in compliance with the provisions of Act and that any regulations issued are in accordance with the Act. The DPA also has competence to conduct unannounced inspections. Decisions²⁵ made by the DPA are final and may not be appealed to any other administrative body. They may, however, be brought before the courts.

As reported above, private controllers must in most cases obtain the authorisation of the DPA before processing sensitive or semi-sensitive data. The latter are certain kinds of data that are regulated in such a way that they are almost viewed as sensitive. These are data on criminal offences, serious social problems, and other data of a clearly private nature.²⁶

According to the PPD, the DPA is required to give an opinion before any new laws or regulations that have an impact on privacy are issued.²⁷ The DPA has examined the Act on Prohibition of Video Surveillance and assessed whether this type of surveillance complies with the PPD.²⁸

In 2009 the staff of the DPA was around 35 and its budget of the DPA was DKK20.4 million (approximately. €2,738 million) – governmental funding – plus DKK513,000 (€68,859) – external funding.²⁹

In 2009, the DPA received 1,468 inquiries and complaints, and the DPA initiated 170 cases of its own accord and carried out 83 inspections. Of the 1,468 inquiries and

²⁴ The DPA consists of a Counsel and an independent Secretariat who is only answerable to the Counsel. The Counsel, which is set up by the Minister of Justice, is composed of a chairman, who is a legally qualified judge, and of six other members. The Council decides in leading cases. The day-to-day business is attended by the Secretariat, which currently counts around 30 employees including: one director, 19 legal advisors, five IT security consultants and administrative staff. See <http://www.datatilsynet.dk/om-datatilsynet/medarbejdere/>.

²⁵ Information is available at <http://www.datatilsynet.dk/afgoerelser/>.

²⁶ Peter Blume, Country Studies, *supra* at 3.

²⁷ *Datatilsynet*, at <http://www.datatilsynet.dk/> "; English version available at <http://www.datatilsynet.dk/english/> .

²⁸ *Lov om behandling af personoplysninge* (Act on Processing of Personal Data), Chapter 6(a), *supra*.

²⁹ See http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsrapporter/aarsrapport_2009_-_Datatilsynet.pdf.

complaints, 960 concerned private entities, and 508 concerned public bodies. Private entities filed 2,077 notifications of registration of personal information; public bodies filed 375. Of the 4,859 cases in total, other topics of interest are: issues of security (30), legislative preparation (329), and international cases (157).³⁰ The issues of digital surveillance as a crime prevention measure and security in relation to the transfer of personal information on the Internet have been central to many of the inquiries and statements.

The DPA issues opinions every year including in 2005, when it issued an interesting and critical opinion on reporting to the Schengen Information System (SIS).³¹ The Danish DPA criticised the National Commissioner of Police in Denmark for an unacceptably high number of errors in reporting to the SIS database personal data that had been passed to another EU Member State or to a third country. The SIS database provides access to alerts on individuals, including immigration, on public order or national security grounds. "[A]n investigation by the Danish Data Protection Agency in June 2005 found 68 errors out of a base of 443 Article 96 'alerts'³² on the Schengen Information System (SIS) entered by Denmark."³³ According to DPA, 11 people had incorrectly been declared "undesirable" in Denmark. The DPA concluded that *Rigspolitiet* (the National Commission of the Danish Police) had violated PPD Section 5 (4). The DPA stated that dealing with personal data shall be organised in a manner that allows for necessary updates. In addition, necessary control measures must be initiated to secure that the information is not misleading or wrong. Information which is found to be wrong or misleading must be erased or corrected.³⁴

On 3 April 2009 the DPA sent a list of questions to Facebook.³⁵ The agency questioned Facebook about whether the network is registered in an EU country and how and whether it adheres to Danish legislation on personal data protection.³⁶ On 18 December 2009 the DPA received a reply in which Facebook thanked the DPA for making it aware of the

³⁰ *Datatilsynets årsberetning 2008 og 2009* (DPA Annual Report 2008 and 2009), *supra*.

³¹ See *Journalnummer: 2003-851-0048 "Undersøgelse af indberetninger i henhold til Schengen-konventionens"* ("Examination of Reporting Pursuant to the Schengen Convention"), 10 June 2005, available in Danish at http://www.datatilsynet.dk/index.php?id=325&tx_ttnews%5Btt_news%5D=219&no_cache=1.

³² I.e. blocking third-country nationals from entering Schengen territory.

³³ Tony Bunyan, "Statewatch Analysis. EU Data Protection in Police and Judicial Cooperation Matters: Rights of Suspects and Defendants under Attack by Law Enforcement Demands," October 2006, <http://www.statewatch.org/news/2006/oct/eu-dp.pdf>.

³⁴ *"Undersøgelse af indberetninger i henhold til Schengen-konventionens"* ("Examination of Reporting Pursuant to the Schengen Convention"), *supra*.

³⁵ Letter from Janni Christoffersen, Director, The Danish Data Protection Agency to Chris Kelly, Chief Privacy Officer, Facebook, "Facebook's Processing of Personal Data," 3 April 2009, available at http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook.pdf.

³⁶ *Id.*

DPA's guidelines following the resolution of the 30th International Conference of Data Protection and Privacy Commissioners and explained some of the improvements made to the privacy settings on Facebook.³⁷

The DPA provides information and views regarding legislative proposals, and has a useful Web site where journalists and others can obtain information on specific issues, cases, and press briefs. In 2009 the DPA focused on TV surveillance and published, in cooperation with other stakeholders, material for school children.³⁸ The aim was to raise awareness among youngsters about the protection of their own and others' personal information.

Major Privacy & Data Protection Case Law

In 2006 the Eastern High Court of Denmark decided a case concerning a company that had posted on a Web site two individuals' social security numbers for a period of seven days.³⁹ Signing a mortgage contract, which they knew would be registered, could not be regarded as explicit consent to publication of the social security numbers, and was therefore found to be a violation of the PPD Act, Section 11, subsection 3. The defendant company was found to be responsible and was fined DKK3,000 (€400) according to the PPD, Section 70, subsection 5, No. 1.

The DPA was asked to give an opinion regarding the request of ATP⁴⁰ to transfer personal data to third countries.⁴¹ The DPA was then informed that by the end of 2006, ATP had a total of almost 4.5 million members and approximately 150,000 contributing employers, coming from both the public and private sectors.⁴² The information processed by ATP included information such as name, address, other contact information, civil registration number, employer, occupation, and education.⁴³ ATP wished to transfer this data about members and contributing employees to data processors in India and South America, for the purposes of the security of supplies.⁴⁴

³⁷ Letter from Chris Kelly, Chief Privacy Officer, Facebook, to Janni Christoffersen, Director, Danish Data Protection Agency, 18 December 2009, available at http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Breve/FacebookDanishDPADec09.pdf.

³⁸ See <http://www.dubestemmerselv.dk>.

³⁹ U.2007.334Ø, *Østre Landsret* (Eastern High Court of Denmark).

⁴⁰ ATP is an independent institution, established by Act No. 46 of 7 March 1964, for the purpose of paying supplementary pensions to wage earners etc.

⁴¹ 11th Annual Report of the Article 29 Data Protection Working Party (2007), 24 June 2008, Chapter Two, Main Developments in Member States: Denmark, European Commission, at 31-33.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

The DPA, when asked to comment on this informed ATP of Section 41(4) of the Act on the Processing of Personal Data which states in part that: "As regards data which are processed for the public administration and which are of special interest to foreign powers, measures shall be taken to ensure that they can be disposed of or destroyed in the event of war or similar conditions" The Act therefore prevented ATP from transferring personal data to India and South Africa.⁴⁵ The DPA stressed that both personal data from the centralised civil register and personal data about citizens' education were covered by Section 41(4) when the Act on the Processing of Personal Data was adopted.⁴⁶

Other relevant case law concerning privacy and data protection is categorised and discussed under the corresponding section.⁴⁷

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The Criminal Code regulates wiretapping.⁴⁸ In 2001, the Danish Parliament adopted an amendment to the Act on Administration of Justice which increased the police surveillance mandate by allowing access to a list of all active mobile phones near the scene of a crime at the time the crime was committed. This law was approved by the Parliament in June 2001.

Statistical data on the interception of communications by the police show that the courts approved the vast majority of requests prior to the interception. The majority of requests were related to drug crimes (943 requests); some were related to human trafficking (Section 125 (a) of the Criminal Code) and violation of the Aliens Act (17 requests); most requests involved telephone tapping (2,658); and a significant number (1,823) dealt with the "requiring of information from telecommunication providers (*Teleoplysning*)."⁴⁹

An act on the activities of the police was adopted in 2004,⁵⁰ establishing a common foundation for the work of the police. The act regulates procedures for the use of force, and for police interception and investigations, which are not regulated by other legislation. One issue, which has been criticised in relation to this act, is the lack of

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Cfr.* Section "Data Protection Authority," *supra* and Sections "Cybercrime," "E-commerce," "International Obligations & International Cooperation," *infra* in this report.

⁴⁸ Criminal Code at Section 263.

⁴⁹ The Danish Police, *Politiets Årstabel 2008* (Annual Statistical Report 2008), in Danish at <http://www.politi.dk/NR/rdonlyres/807C15C7-901A-4347-9C33-7AAF2B1A6877/0/PolitietsÅrstabel2008.pdf>.

⁵⁰ *Lov 2004-06-09 nr. 444 om politiets virksomhed* (Act on Police Activities No. 444 of 9 June 2004).

regulation regarding the use of electronic tracking devices on vehicles as a means of police surveillance.⁵¹

National security legislation

On 8 June 2006, an Act amending the Administration of Justice Act, the Act Prohibiting Video Surveillance etc., and the Act on Air Traffic (Strengthening of the efforts to fight terrorism etc.) was adopted in Parliament (Act No. 542 of 8 June 2006).⁵² The amendment to the Administration of Justice Act gives the Police Intelligence Service increased powers to exchange information with the Defence Intelligence Service and to collect information from other public authorities, e.g. hospitals, schools, libraries, social services etc. without a court order. The amendment of the Act Prohibiting Video Surveillance gives the police increased powers to demand that public offices and private parties install and conduct video surveillance. The amendment of the Air Traffic Act obliges airline companies to register and keep data on passengers and crews for one year and to provide the Police Intelligence Service with electronic access to the data without a court order.

In 2006 the government decided not to propose legislation concerning phone scanning. The report, entitled "Danish society's initiatives against and preparedness for terror", was prepared in October 2005 and contained a recommendation that it be made legal for police to scan the contents of telecommunications within a defined area. The Standing Committee on Administration of Criminal Justice delivered its remarks on the recommendation in September 2006. Among its conclusions, the Committee found that phone scanning amounts to a particularly serious intrusion into the secrecy of correspondence, since this measure would also entail sweeping access to communication among individuals who are not suspected of any criminal wrongdoing. The Police Intelligence Service was informed that the Committee had established that phone scanning can in fact be undertaken according to existing legislation based on the principle of emergency law. The government subsequently decided not to propose legislation on phone scanning.⁵³

Data retention

An administrative order from the Ministry of Justice followed the "anti-terrorism package", which was passed in June 2002 despite vocal opposition to increased data retention and the enlarged surveillance powers it embraced. The order extending the scope of Section 786(4) and Section 786(6) of the Administration of Justice Act was

⁵¹ Christoffer Badse, The Use of Electronic Tracking Devices Should Be Regulated, (*Pejling bør reguleres*) *Lov og Ret* No. 8, December 2004, (27-32).

⁵² L 217 (2005) *Forslag til lov om ændring af straffeloven, retsplejeloven og forskellige andre love* (Draft Bill to Amend the Criminal Code, the Administration and Various other Laws).

⁵³ The Ministry of Justice, Press statement of 21 December 2006.

approved in September 2006, with an implementation deadline of September 2007.⁵⁴ The ministerial order regulates in more detail the obligations of the Danish telecommunications providers (small, private Internet Service Providers, or ISPs, excluded), specifying how they must assist the Danish police to interfere with the secrecy of communication, what data should be retained, and how it should be done. During the drafting period the proposal was heavily criticised by ISPs, cooperative housing associations, and non-governmental organisations for being disproportionate and inconsistent, *e.g.* letting private entities store huge amounts of personal information while at the same time being easy to evade because of the many exemptions, such as libraries and universities not being included.

The administrative order further implements the EU directive on data retention, adopted February 2006. Danish telecommunications providers are obliged to retain data for one year for use in the investigation and prosecution of criminal offences.

National databases for law enforcement and security purposes

The Act concerning the Central DNA Profile Register.

National and international data disclosure agreements

On 18 June 2008 Act No. 479 of 18 June 2008 amending the Act concerning the Central DNA Profile Register, the Administration of Justice Act, and the Act concerning Registration of Vehicles was adopted by the Danish Parliament. It aims to transpose the so called EU "Prüm" Decision into the Danish legal order.⁵⁵ Although approved in 2008, Act No. 479 of 18 June 2008 is not in force yet. The amendment to the Act concerning the Central DNA-Profile Register gives EU member states' judicial authorities carrying out a criminal investigation the right to use electronic search to compare a DNA profile relevant to the investigation with DNA profiles in the Central-Profile Register. The amendment to the Administration of Justice Act gives the EU member states' judicial authorities carrying out criminal investigations the right to use electronic search to compare fingerprints relevant to the investigation with fingerprints in the Central Finger and Handprint Register. The amendment to the Act concerning Registration of Vehicles gives the Danish National Commissioner the right to give the judicial authorities of other EU member states access to carry out electronic searches of information from the Danish Vehicle Register that has been disclosed to the Danish Police for the purpose of a concrete criminal investigation or a concrete case about maintaining the public safety.

⁵⁴ *Cfr.* Administrative Order bkg 2006 No. 986.

⁵⁵ Council Decision 2008/615/JHA, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008, OJ L 210, 6 August 2008, at 1–11, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:01:EN:HTML>.

On 18 March 2009, Parliament adopted Act No. 188 of 2009 amending the Act on Processing of Personal Data.⁵⁶ The amendment to the Act on Processing of Personal Data gives the Minister of Justice powers to lay down rules about protection of personal data processed in the framework of police and judicial cooperation in criminal matters in the EU.⁵⁷ The Minister of Justice has not yet laid down such rules.

Cybercrime

Also in 2001, Denmark amended its laws on search and seizure in accordance with its obligations under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) and under pressure from the US software industry. The Administration of Justice Act now authorises physical searches for copyright infringement without "prior notification of the defendant if it is assumed that the notification would cause a risk of removal, destruction, or modification of objects, documents, information in computer systems, or anything else that are comprised by the petition for investigation."⁵⁸

Following a complaint by IFPI (International Federation of the Phonographic Industry), on 4 February 2008 a Danish bailiff's court issued an injunction ordering Tele2, one of Denmark's major ISPs, to block access to The Pirate Bay's domains.⁵⁹ IFPI asked the court for this injunction because most of the materials linked from The Pirate Bay are copyrighted and the exchange of these materials between Pirate Bay users is illegal.⁶⁰ The injunction of the bailiff's court was subsequently upheld by the Danish High Court, and the decision by the Danish High Court was upheld by the Danish Supreme Court on 27 May 2010.⁶¹

Critical infrastructure

No specific information has been provided under this section.

⁵⁶ The purpose of the act is to implement Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

⁵⁷ Section 72(a) of the Act on Processing of Personal Data.

⁵⁸ "Denmark Enacts Anti-Piracy Search and Seizure Law," Cluebot, 20 July 2001.

⁵⁹ "Pirate Bay--Blocked in Denmark," EDRI-Gram, 13 February 2008, available at <http://www.edri.org/edrigram/number6.3/piratebay-denmark>.

⁶⁰ *Id.*

⁶¹ Order of 27 May 2010 by the Danish Supreme Court (U 2010.2221 H).

INTERNET & CONSUMER PRIVACY

E-commerce

Since July 2000, spamming has been forbidden under the Marketing Practices Act (*Markedsføeringsloven*).⁶² Article 13 of the EU Privacy and Electronic Communications Directive⁶³ was transposed into Danish law on 10 June 2003,⁶⁴ and changed Denmark's legal data protection framework on spam. According to the directive, people who have already given their address to companies in connection with the companies' sale of products or services can now be spammed with advertisements for "similar services" ("soft opt-in"), which the Marketing Practices Act did not previously allow.⁶⁵

The Danish Consumer Ombudsman has published guidelines for industry regarding spamming and Section 6 of the Marketing Practices Act. Also, the Danish Consumer Ombudsman has established email addresses where consumers can file complaints regarding spam.⁶⁶

During the recent years, the Danish Maritime and Commercial court has convicted companies for spamming. Companies have been fined up to DKK2,000,000 (approx. €269,000) for sending out unsolicited advertising material.⁶⁷ The size of the fine also depends on other violations of the Marketing Practices Act.⁶⁸

⁶² Section 6.

⁶³ Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002, Article 13, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>.

⁶⁴ Law No. 450 concerning the change of Law of Competition and Consumer Regulation of the Telecommunications Market, 10 June 2003.

⁶⁵ According to Section 6(2) of the Marketing Practices Act, a company may send advertising via electronic mail without the customer's prior consent if the customer, has already given his electronic mail address to the company in a previous purchase transaction. According to Section 6(2), it is a pre-condition that the customer is given the option, free of charge, and in an easy manner, of declining such communication both when giving his contact details to the company and in the event of subsequent communications. This means that the customer must express dissent to avoid getting spammed (opt out), which is a change compared to the former regulation where the customer also under such circumstances had to positively express his wish to receive advertising material (opt in). The amendment entered into force on 25 July 2003.

⁶⁶ The Guidelines can be downloaded (in Danish) from www.forbrugerombudsmanden.dk and complaints can be filed at "dansk@spamklage.dk" and "int@spamklage.dk".

⁶⁷ See judgment of 14 March 2005 of the Danish Maritime and Commercial Court in case M-1-04. The fine of DKK2,000,000 also involved improper comments about competitors.

⁶⁸ *Lovbekendtgørelse 2009-08-31 nr. 839 om markedsføring* (Consolidated Act on Marketing Practices No. 839 of 31 August 2009).

Cybersecurity

In June 2008 the DPA published requirements and recommendations concerning transfer of personal data via the Internet in the private sector.⁶⁹ According to these requirements and recommendations the DPA demands sensitive personal data and social security numbers being transferred via Web sites must be encrypted.

In May 2010, the DPA decided not to take judicial action against Google for collecting pieces of email correspondence and other electronic communications from private persons when recording photographs and Internet addresses for Google Street View. Google had informed the DPA that it did not intend to collect this data and that the company had not used this data.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

The Danish Data Protection Agency's Web site publishes guidelines for young computer users.⁷⁰ These guidelines concern (1) what young users can write on the Internet, (2) when they can publish pictures on the Internet, (3) how they can remove something from the Internet, (4) how they secure their data on the Internet and (5) what they should be aware of, when they are on the Internet.

TERRITORIAL PRIVACY

Video surveillance

In June 2007 the Act on TV Surveillance⁷¹ and the PPD were amended.⁷² The amendments to the Act on TV Surveillance give private enterprises such as banks, gas stations, hotels, and shops extended powers to perform surveillance on areas related to their property. TV surveillance is defined as systematic and continuous surveillance of persons via remote-controlled or automatic cameras. The Act applies whether or not the

⁶⁹ See <http://www.datatilsynet.dk/nyheder/nyhedsarkiv/artikel/datatilsynets-krav-og-anbefalinger-i-forbindelse-med-overfoersel-af-personoplysninger-via-internettet/> (in Danish).

⁷⁰ See <http://www.datatilsynet.dk/borger/boern-og-unge/> (in Danish).

⁷¹ *Lov 2007-10-11 nr. 1190 om tv-overvågning* (Act No. 1190 of 11 October 2007 on TV Surveillance).

⁷² *Lov 2007-06-06 nr. 519 om ændring af lov om forbud mod tv-overvågning m.v. og lov om behandling af personoplysninger – Udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i forbindelse med tv-overvågning* – (Act No. 519 of 6 June 2007 Amending the Law Prohibiting Television Surveillance, etc. and Act on Processing of Personal Data – Extension of Access to Television Surveillance and Strengthening of Legal Protection in Handling Personal Information in Connection with CCTV).

pictures are stored or recorded. As a starting point, it is prohibited to establish TV surveillance where there is ordinary public traffic; however, exceptions are provided for in the act, e.g. for crime prevention. According to the Act there is a duty to inform people via signs that there is TV surveillance in the area. There is no longer a duty to notify the DPA prior to installing surveillance equipment.⁷³ Both analog and digital TV surveillance is now covered by the PPD and the requirements in the PPD for storage and protection against the abuse of information must be observed. This was not the case before the amendment.⁷⁴

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this section.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The Danish National Police started issuing electronic passports in October 2006. These new, secure e-Passports feature a polycarbonate data page containing a contactless microprocessor chip running the highly secure operating system. The chip not only features the information identity already laser-engraved on the first page, but also contains the passport holder's digitised photograph.⁷⁵

NATIONAL ID& SMART CARDS

Danish citizens do not have an identification card but all citizens are provided with a Central Personal Registration (CPR)⁷⁶ number, which is used to identify them in public registers. The information in the CPR register includes: name, address, municipality, prior addresses, place and date of birth, gender, nationality, membership information regarding the Danish National Church, information on family ties, guardians, information on marriage, and information on job positions. The Ministry of the Interior can hand over information for purposes of statistics or research. According to Section 38 of the Act, private entities can gain access to information⁷⁷ on a larger group of persons identified individually.⁷⁸ A condition for access is that the private entity has a legitimate purpose.

⁷³ Section 26(c) of the Act on Processing of Personal Data. See http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Breve/Orienteringsbrev_20fra_20Datatilsynet_20DOK11925.pdf (in Danish).

⁷⁴ Cfr. *Lovforslag af 28. februar 2007 om ændring af lov om forbud mod tv-overvågning etc. og lov om behandling af personoplysninger*, pkt. 3.2.1 (LSF 162/2006) (Draft Bill No. 162 of 28 February 2007 Amending the Law Prohibiting Television Surveillance, etc., and Act on Processing of Personal Data, Section 3.2.1).

⁷⁵ ePractice, eGovernment Factsheet – Denmark – National Infrastructure (June 2010), available at <http://www.epractice.eu/en/document/288210>.

⁷⁶ As regulated in *Lovbekendtgørelse 2009-09-14 nr. 878 om Det Centrale Personregister* (Consolidated Act on Central Personal Registration, No. 878 of 14 September 2009).

⁷⁷ The information accessible includes primarily: name, address, job position, death, and disappearance.

⁷⁸ Identified by either CPR number, date of birth and name, or address and name.

According to the Act an individual can upon request be granted name and address protection lasting one year in relation to private entities.⁷⁹

RFID tags

No specific information has been provided under this section.

BODILY PRIVACY

According to the Aliens Act,⁸⁰ immigration authorities may require DNA samples from applicants for residency or persons with whom the applicant claims family ties for the purposes of residency. In its October 2001 report, the United Nations Human Rights Committee expressed concern about the privacy implications of this practice and called on Denmark to ensure that such testing is used only when "necessary and appropriate to the determination of the family tie on which a residence permit is based."⁸¹

WORKPLACE PRIVACY

In 2008, the Copenhagen Maritime and Commercial Court rendered a decision in a case where a store employee was subjected to approximately half an hour to 45 minutes' video surveillance by his employer from the employer's private residence.⁸² The surveillance was not motivated by work or safety reasons. The surveillance led to the collection of information (images) of the employee for purposes other than those the employee was aware of. According to the Court, the collection was therefore in breach of the PPD, Section 5, subsection 1 concerning good practices for the processing of data and Section 5, subsection 2 which states that data must be collected for specified, explicit and legitimate purposes. Compensation for moral damages was DKK25,000 (€3,332).

HEALTH & GENETIC PRIVACY

Medical records

The National e-Health portal is a Internet-based solution collecting and providing information on, and access to, all Danish health care services.⁸³ By bringing the entire health care sector together on the Internet and providing integration for some of the central registers and solutions in this sector, the portal supports a common infrastructure while offering a setting for citizens and healthcare professionals to meet and efficiently exchange information. Citizens can access their personalised health page via their digital

⁷⁹ The Consolidated Act on Central Personal Registration, Section 28.

⁸⁰ *Lovbekendtgørelse* 2010-08-18 nr. 1061 *Udlændingelov* (Consolidated Aliens Act No. 1061 of 18 August 2010).

⁸¹ Report of the Human Rights Committee, A/56/40, Volume 1, 26 October 2001, available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/602/26/PDF/N0160226.pdf?OpenElement>.

⁸² U.2008.727/2S, *Sø- og Handelsretten* (Copenhagen Maritime and Commercial Court).

⁸³ *Cfr.* Section "E-Government & Privacy", *infra*.

signature. Among other available citizen services are: electronic booking of appointments, access to one's own medical records, prescription renewals, and health appointment calendars.⁸⁴ The portal gathers together all electronic patient records that are stored in each individual hospital. Health care professionals have easy access to the latest patient information from most hospitals and laboratories in the country while being enabled to exchange information with other professionals. Access to patients' personal data requires special security certificates.⁸⁵

The Danish e-Health portal contributed to making Denmark the world leader in the area of national health care information exchange. In this respect, the country has been chosen as the testing ground for a new standardised electronic health record-keeping system.⁸⁶

Genetic identification

No specific information has been provided under this section.

Financial privacy

No specific information has been provided under this section.

E-GOVERNMENT

First launched in January 2007, "www.borger.dk" is the e-Government portal for citizens. It is a single Internet entry point to the public sector's information and e-Services to citizens, regardless of the origin of the public authority. "Borger.dk" results from a merger between the previous "danmark.dk" and "netborger.dk" sites (the former a local eGovernment services portal). The platform is operated in cooperation between State and local authorities. The Citizen portal provides information on public authorities and a common public e-Service channel for citizens. The portal features a range of "self-service" sections, thus allowing citizens to manage their communications with the public sector in a more efficient way.⁸⁷ The target is for all public sector bodies to integrate their digital information and services for citizens into the portal in 2012 at the latest. It is to be noted that "borger.dk" forms the framework for developing cross-governmental standards and principles of digital service applicable to all authorities.

A new, updated version of "borger.dk" went live in October 2008. It contains the first version of the "My Page" section, which gives a personal overview of one's relation to the public authorities. In addition, a single sign-on solution allows citizens to receive and access information and services from several agencies without having to log on multiple times.⁸⁸ Further updates were scheduled to take place. Among other things, citizens will

⁸⁴ ePractice, eGovernment Factsheet – Denmark – National Infrastructure, *supra*.

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

gain the opportunity to opt for SMS reminders and to communicate by means of secure emails with the public authorities via "My Page". Several other public self-services will be added, together with new franchises.⁸⁹

OPEN GOVERNMENT

Other laws regulating the processing of personal information by the public sector include the Public Administration Act of 1985,⁹⁰ the Publicity and Freedom of Information Act of 1985,⁹¹ and the Act on Public Records of 2002.⁹² These laws set out basic data protection principles and determine which data and governmental records are accessible to the public and which should be kept confidential.⁹³

Other recent factual developments

There is a continuous focus on privacy issues. For example, the Information Technology Security Committee (IT-sikkerhedskomiteen) was established by the Ministry of Science in 2008. In October 2009 it hosted a public event "Privacy in the Information Society" (*Privatliv i informationssamfundet*) to discuss privacy, biometrics, RFID tags, and social networks.⁹⁴

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

No specific information has been provided under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

On 6 January 1972, Denmark ratified the UN International Covenant on Civil and Political Rights and the Optional Protocol allowing the UN Human Rights Committee to receive and consider communications from individuals.

Denmark is a member of the Council of Europe and has ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.⁹⁵ Denmark signed the Convention on Cybercrime on 22 April 2003, and ratified it on 21

⁸⁹ *Id.*

⁹⁰ Lov 2007-12-07 nr. 1365 *Forvaltningslov, supra.*

⁹¹ Lov 1985-12-19 nr. 572 *om offentlighed i forvaltningen.*

⁹² Lov 2007-08-21 nr. 1035 *Arkivlov.*

⁹³ Peter Blume *et al., supra.*

⁹⁴ Press release concerning the event "*Privatliv i informationssamfundet*," "*Pressemeddelelse: It-sikkerhedskomitéen i 'privacy streetfight'*" ("Press release: IT security Committee in 'Privacy Street Fight'", 6 October 2009, in Danish at <http://www.itst.dk/nyheder/nyhedsarkiv/2009/it-sikkerhedskomiteen-i-201dprivacy-streetfight201d> .

⁹⁵ Signed 28 January 1981; ratified 23 October 1989; entered into force 1 February 1990.

June 2005. The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems was signed in February 2004, and ratified in June 2005.

In May 2006, a decision on admissibility was taken by ECtHR in a case against Denmark. In a dispute over inheritance, the complainant claimed that it would be a violation of the Act on Processing of Personal Data to exhume his father in order to administer a DNA test. The Court reiterated that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. However, the Court found that it would stretch the reasoning developed in this case law too far to hold in a case like the present one that DNA testing on a corpse constituted interference with the Article 8 rights of the deceased's estate. Consequently, ECtHR found the application inadmissible and partly manifestly ill-founded.⁹⁶

In relation to the development of international jurisprudence, the Danish Institute for Human Rights (DIHR) assessed in relation to the European Court of Human Rights (ECtHR) judgment in *S. and Marper v. UK* (4 December 2008) that Denmark could lose a case before ECtHR since Danish legislation was comparable to the UK.⁹⁷ The Ministry of Justice came to the same conclusion as DIHR. Based on the judgment against the UK, an amendment was put forward in September 2009 limiting the retention of fingerprints, DNA profiles, and DNA samples to ten years for acquitted persons, which is probably still problematic in relation to the ECtHR.⁹⁸

There has also been a focus on stop and search procedures conducted by the police, especially whether the regulation was in accordance with human rights standards after the ECtHR judgment of *Gillan and Quinton v. UK* of 12 January 2010.⁹⁹ It is the assessment of the DIHR that the legal provisions are not adequate and run the risk of being arbitrary. Therefore DIHR recommended that the legal provision in the Act on Police matters (*Lov om Politiets Virksomhed*) regulating the so-called zones of visitation (*visitationszoner*) should be amended to avoid any risk of conflict with the newest jurisprudence from ECtHR. The Ministry of Justice issued a statement in March 2010¹⁰⁰ briefly stating that

⁹⁶ ECtHR, „Application No. 1338/03, 15 May 2006, *Estate Of Kresten Filtenborg Mortensen v. Denmark*. Decision.

⁹⁷ ECtHR (Grand Chamber), Applications No. 30562/04 and No. 30566/04, 4 December 2008, *S. and Marper v. The United Kingdom*, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=MARPER&sessionid=57426852&skin=hudoc-en>.

⁹⁸ See <http://menneskeret.dk/nyheder/arkiv/nyheder+2009/ministerium+retter+ind+efter+menneskerettighedsdom> (in Danish).

⁹⁹ ECtHR (Fourth section), Application No. 4158/05, 12 January 2010, *Gillan and Quinton v. The United Kingdom*, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=GILLAN&sessionid=57427195&skin=hudoc-en>.

¹⁰⁰ See http://www.justitsministeriet.dk/pressemeddelelse+M5699c5d96c7.html?&tx_ttnews%5Bpointer%5D=3.

the minister did not find that the Danish stop and search procedures should be changed by an amendment in legislation.¹⁰¹

Denmark is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Denmark has been a member of the EU since 1973. It ratified the EU Treaty of Lisbon in accordance with Section 19 of the Danish Constitution according to which international agreements can only be entered into with the consent of the Parliament.. The ratification bill was passed on 24 April 2008 by a majority of 90 votes for, 25 against, and no abstentions. Thereby the EU Charter of Fundamental Rights (including in particular Articles 7 – Respect for private and family life – and 8 – Protection of personal data – was made legally binding for Denmark from the day the Treaty of Lisbon entered into force (1 December 2009).

GREENLAND

The original (un-amended) Danish Public and Private Registers Acts of 1978 and Guidelines regarding Notification of Data Processing Bureaus of 1979 continue to apply within Greenland, a self-governing territory. The Danish Data Protection Agency oversees compliance with the law. The 1988 amendments that brought Denmark into compliance with the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data do not apply to Greenland. Furthermore, Greenland is not part of the European Union and therefore has not adopted any of the EU Data Protection legal instruments. Greenland's data protection requirements are much less stringent than those of Denmark and the other member states of the European Union.

* Updates to the Danish Report published in the 2010 edition of EPHR have been provided by: Christoffer Badse, Danish Institute for Human Rights, Denmark; Michael Hopp, Attorney-at-Law at Plesner Law Firm, Denmark.

¹⁰¹ Christoffer Badse, "13-4-2010 *Advokaten* 3/2010 - Klokken er mange... og nu skal du kropsvisiteres" (13-4-2010 Attorney 3/2010 - The Time Many ... and Now You Searched) *Advokaten*, at <http://www.advokatsamfundet.dk/Default.aspx?ID=11687&M=News&PID=0&NewsID=12843>.

REPUBLIC OF ESTONIA

I. STATE'S PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The 1992 Estonian Constitution recognizes the right of privacy, secrecy of communications, and data protection. Article 26 states, "Everyone has the right to the inviolability of private and family life. State agencies, local governments, and their officials shall not interfere with the private or family life of any person, except in the case and pursuant to the procedure provided by law to protect the health, morals, public order, or the rights and freedoms of others, to combat a criminal offence, or to apprehend a criminal offender." Article 42 states, "State agencies, local governments, and their officials shall not gather or store information about the beliefs of Estonian citizens against their free will." Article 43 states, "Everyone shall be entitled to secrecy of messages transmitted by him or to him by post, telegram, telephone, or other generally used means. Exceptions may be made on authorisation by a court, in cases and in accordance with procedures determined by law in order to prevent a criminal act or for the purpose of establishing facts in a criminal investigation." Police must obtain a warrant in order to intercept communications. Illegally obtained evidence is not admissible in court.¹ Article 44 (3) of the Constitution states, "An Estonian citizen has the right to access information about himself or herself held in state agencies and local governments and in state and local government archives, pursuant to procedure provided by law. This right may be restricted pursuant to law to protect the rights and freedoms of others, or the confidentiality of a child's parentage, and in the interests of preventing a criminal offence, apprehending a criminal offender, or ascertaining the truth in a criminal proceeding."²

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The *Riigikogu*, Estonia's Parliament, enacted the first Personal Data Protection Act (PDPA) in June 1996. It was superseded by a second version of the law to bring Estonia into full compliance with the 1995 EU Data Protection Directive. That law was enacted in February 2003 and entered into force on 1 October 2003. As of February 2007, a third version of the PDPA was enacted and came into force on 1 January 2008.³ The aim of the current PDPA is to protect the fundamental rights and freedoms of natural persons upon

¹ The Human Rights Report submitted to the United States Congress by the United States Department of State, Section 1f, available at <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136029.htm>.

² Constitution of Estonia, available in English: <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136029.htm>.

³ Personal Data Protection Act RT I 2007, 24, 127, available at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete+kaitse>.

the processing of their personal data, and above all the right to inviolability of their private life.⁴

The PDPA removes the category of "private personal data," thereby removing the government's duty to notify data processing. Instead the law divides personal data into "personal data", "sensitive personal data", and "genetic data", a subcategory of "sensitive personal data".⁵ It defines "personal data" as any data concerning an identified natural person or a natural person to be identified, regardless of the form or format in which such data exists.⁶ The processing of sensitive personal data is more strictly regulated, since it includes the requirement to register such processing with data protection authorities or to appoint a person responsible for the processing of sensitive personal data. The PDPA classifies as "sensitive personal data" the following categories of personal data: data revealing political opinions, or religious or philosophical beliefs, except data relating to membership with a legal person in private law and registered pursuant to a lawful procedure; data revealing a person's ethnic or racial origin; data on his state of health or disability; data on his genetic profile; a person's biometric data – above all fingerprints, palm prints, iris images and genetic data; information on his sex life or trade union membership; information regarding the commission of an offence or falling victim to an offence before a public court hearing, and information with respect to a decision in the matter of the offence or a termination of the court proceedings in the matter.⁷

Pursuant to the PDPA, processors of personal data⁸ must ensure that personal data is processed in accordance with the following principles: personal data shall be collected only in an honest and legal manner; shall be collected only to achieve specific and lawful objectives, and shall not be processed in a manner not compatible with the objectives of data processing; shall be used for other purposes only with the data subject's consent, or with the competent authority's authorisation; shall be up-to-date, complete and necessary to achieve the purpose of data processing; security measures shall be applied in order to protect them from involuntary or unauthorised processing, disclosure or destruction; the data subject shall be notified of data collected concerning him, shall be granted access to the data concerning him, and has the right to demand the correction of inaccurate or misleading data.⁹

⁴ *Id.* at § 1(1).

⁵ Article 29 Working Party on Data Protection, Eleventh Annual Report (2008) at 34, available @@@

⁶ *Id.* at § 4(1).

⁷ *Id.* at § 4(2).

⁸ The Estonian PDPA differentiates between "chief processors" and "authorised processors", however the law refers to both by using the general term "processors of personal data".

⁹ *Id.* § 6.

Processing of personal data is generally permitted only with the data subject's consent,¹⁰ although it is permitted without the data subject's consent if the personal data is to be processed on the basis of law; for the performance of a task prescribed by an international agreement or directly applicable legislation of the European Union; in individual cases for the protection of the data subject's life, health, or freedom if obtaining his consent would be impossible; for the performance of a contract entered into with the data subject or in order to ensure the performance of such contract, unless the data to be processed is sensitive personal data.¹¹

If the rights of a data subject have been violated upon processing of their personal data, the data subject has the right to demand compensation of the damage.¹² Violation of the obligation to register the processing of sensitive personal data, violation of the requirements regarding security measures to protect personal data, or violation of other requirements for the processing of personal data is punishable by a fine in misdemeanour proceedings amounting to a maximum of approximately €1,150.¹³ For the same act, if committed by a legal person, the fine can be set to a maximum of approximately €31,956.¹⁴

In April 1997, the *Riigikogu* passed the Databases Act (DA). However, as of January 2008 this act is void and a chapter on databases has been appended to the Public Information Act (PIA).¹⁵ The purpose of the PIA is to ensure that the public and every person have the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law, and an open society, as well as to create opportunities for the public to monitor the performance of public duties. Pursuant to the PIA, databases shall be accessible to the public while personal data in such databases shall not be made public unless the requirement to publish such data arises by law.¹⁶

Sector-based laws

The Credit Institutions Act¹⁷ is one of the few sector-based laws that directly confront the general regulation of the PDPA. It contains a controversial provision which enables credit

¹⁰ *Id.* § 10(1).

¹¹ *Id.* § 14(1).

¹² *Id.* at § 23.

¹³ *Id.* at § 42(1).

¹⁴ *Id.* at § 42(2).

¹⁵ Public Information Act RT I 2000, 92, 597. A slightly outdated version is available in English at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40095K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=avaliku+teabe+seadus>.

¹⁶ *Id.* at § 43(8).

¹⁷ The Credit Institutions Act RT I 1999, 23, 349, currently valid version is available in Estonian at <https://www.riigiteataja.ee/ert/act.jsp?id=13330780>.

institutions to unilaterally obtain the consent required from data subjects in order to process their personal data. The credit institutions may obtain such consent by unilaterally amending their standard terms.¹⁸

The Electronic Communications Act transposes to the Estonian legal system the ePrivacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC.¹⁹

Other relevant legal acts related to the processing of personal data and liability are the Administrative Procedure Act, Investment Funds Act, Official Statistics Act, Insurance Activities Act, Population Register Act, Punishment Register Act, etc. However, these acts do not include a specific sector or subject matter-related data protection regulation, but rather refer to the PDPA and the requirement to adhere to its provisions.

DATA PROTECTION AUTHORITY

The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA and the PIA. On February 14, 2007, the DPI was reorganised: it was moved from an agency operating under the authority of the Ministry of Internal Affairs, and has become an independent agency operating under the Ministry of Justice. The DPI's goal is "to help design a society that values the right of an individual to privacy and transparency of the state's activities."²⁰ The agency can conduct investigations and request documents, impose fines, and administrative sanctions. The DPI has three departments and approximately 20 officials.²¹ The Estonian Government appoints the head of the Data Protection Inspectorate for a term of five years at the proposal of the Minister of Justice and after having heard the opinion of the Constitutional Committee of the Estonian Parliament. As of April 2009, DPI's inspectors are divided between two specialised departments. The first one deals with "soft" issues (the economy, communications, welfare, education, media, the Internet, and spam), while the second one deals with "hard" issues (legal protection and state defence, security service companies, finance, statistics, population accounting, and local government).²² The Control Department exercises control over the processing of personal data and the access to public information, issues precepts, and is the body conducting extra-judicial proceedings. Two departments supervise processing personal data and provide access to public information in various areas of activity.

¹⁸ *Id.* at § 89 (2)2.

¹⁹ Electronic Communications Act, RT I 2004, 87, 593, current Estonian version available <https://www.riigiteataja.ee/ert/act.jsp?id=13333950>.

²⁰ DPI Web site at <http://www.aki.ee/eng/>.

²¹ See generally Estonian Data Protection Inspectorate: Structure, available at <http://www.aki.ee/eng/?part=html&id=95>.

²² Estonian Data Protection Inspectorate. Executive Summary of Annual Report 2009, available <http://www.aki.ee/eng/systematic/files.php?id=1641>, at 2.

Based on requests for explanations and complaints, personal data protection is predominantly connected with the following problems: the misuse of personal data in social media and social networking Web sites (including identity theft), intrusive advertising offers in consumers' mailboxes – especially the issue of the lawfulness of the collection of contact details – the prohibited publication of personal data (including the publication of debtors' personal data); excessive requests for personal data (including when clients are applying for credit cards).

During the period from October 2005 to September 2006, the DPI received 414 registration applications and registered 229 processors of sensitive data.²³ From October 2005 to September 2006, the DPI performed 48 on-site verification visits to determine compliance with the PDPA.²⁴ The DPI also held 34 training sessions on personal data protection in various locations.²⁵

As can be seen from the table below, there has been a significant increase in DPI's workload since then:²⁶

In 2009, the DPI received 306 complaints and challenges based on PDPA violations. This resulted in 49 precepts and 46 misdemeanour proceedings.²⁷ Fines or penalties were imposed in 12 cases; 1,429 registration applications were reviewed by the DPI and 459 precepts were made to data processors for fulfillment of the registration obligation. The same year, the DPI launched a help line that received 851 calls in 2009.

The DPI has changed its policy concerning the supervision of compliance with the Public Information Act. Instead of the predominantly complaint-based response previously used, the DPI is doing their best to influence the implementation of the law. Important tools are comparative monitoring, instructions, and raising awareness. The DPI has introduced comparative monitoring as a new form of work that is designed to identify good and bad practices, cover many subjects, and have a greater impact than supervision proceedings conducted on a subject-by-subject basis. All monitored entities²⁸ are notified of the results. On the basis of monitoring, the DPI initiates separate supervision proceedings for major violations and elaborate instruction materials for recurring problems.²⁹

²³ *Id.* at 6.

²⁴ *Id.* at 14.

²⁵ *Id.* at 6.

²⁶ *Id.* at 3 and Statistics, available at available in English at <http://www.aki.ee/est/?part=html&id=23><http://www.dp.gov.ee/document.php?id=169/>

²⁷ Data Protection Inspectorate, Statistics, at <http://www.aki.ee/est/?part=html&id=23>.

²⁸ "Monitored entities" means the organisations or companies subject to particular monitoring by the DPI, usually all organisations and companies that belong to a particular sector under scrutiny, e.g., all state agencies.

²⁹ *Id.* at 4.

The monitoring of state agencies' Web sites, which the DPA conducted in autumn 2009, confirmed that compliance with the Public Information Act is irregular and not uniform. Application of the law is too often left in the hands of officials without the necessary training. In December 2009 a memorandum was sent to the Secretary of State concerning clarification of responsibilities in the area of public information. It was proposed that in all state agencies an individual with sufficient authority be assigned to take responsibility to coordinate compliance with the Public Information Act, and supervise those guaranteeing compliance.³⁰

The DPI maintains close relations with the data protection authorities (DPAs) in other central and eastern European countries. In December 2001, the data protection commissioners from the Czech Republic, Hungary, Lithuania, Slovakia, Estonia, Latvia, and Poland signed a joint declaration agreeing to closer cooperation and assistance. The commissioners agreed to meet twice a year in the future, to provide each other with regular updates and overviews of developments in their countries, and to establish a common Web site for more effective communication.³¹

The DPI participates in the e-PRODAT project, which includes DPAs, universities and regional/city governments from Spain, Italy, Greece, and Estonia. The main goals of e-PRODAT are to share knowledge and experiences related to personal data protection in public bodies of different European countries; to create an Internet-based "European e-government data protection observatory"; identify best data protection practices already in use for e-government and other public services, and to make recommendations to improve data protection standards in the public sector.³²

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In 2004, the DPI was involved in two cases which found their way to the Supreme Court. Both of them dealt with access to public information. The first one concerned the DPI and the Estonian Tax and Customs Board.³³ The case involved the Board's register of documents and restrictions on access.³⁴ The Supreme Court upheld the previous decisions made by the administrative court and circuit court. According to them, the complaint made by the Board is not within the sphere of competence of the administrative court. Thus, the decision made by the DPI (that the restriction is illegal) was not upheld by the

³⁰ *Id.* at 7.

³¹ Email from Karel Neuwirt, President, Office for Personal Data Protection, Czech Republic, to Sarah Andrews, Research Director, Electronic Privacy Information Center, 15 May 2002 (on file with EPIC).

³² Estonian Data Protection Inspectorate: Main, *supra* at <http://www.aki.ee/eng/>.

³³ Supreme Court case no. 3-3-1-38-04, available in Estonian at <http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-38-04.html>.

³⁴ *Id.*

courts. In November 2004, the restriction on access was made legal with the alteration of the Taxation Act.³⁵

Another key case involves the DPI and a private individual.³⁶ The case was about the complaint made by a private person regarding the DPI's decision on appeal. According to the DPI's challenge, the private person (who was a member of a city council) had no right to request information about the wages and salaries of employees of the institutions administered by the city, because these employees are not officials. The Supreme Court decided that the private individual wanted to get information as a member of the City Council and, because of that, it was not even considered a request of information for the purposes of the Public Information Act.³⁷ The Supreme Court repealed previous decisions made by the administrative court and circuit court, and concluded the proceeding because the employees of the institutions administered by the city are not officials, and their salaries and wages are not public. The DPI's decision was upheld.

In 2007, the Supreme Court issued a ruling regarding the right to have the court judgment kept confidential due to the personal data included in it.³⁸ The accused stated that the victims might be recognised and associated with him. The court ruled that the accused, as a person whose personal data are processed, may in general submit such a claim. However, the court found that no sensitive personal data about the accused was included in the court's decision. The sensitive data on the victims would have been anonymised in any case under the Code of Criminal Procedure (the victims were under age). The Supreme Court confirmed the principle recognised in criminal procedures that the disclosure of the defendant's identity in the court's decision is not a violation of his rights.

The definition of "private life" was analysed by the Supreme Court in 2009.³⁹ Pursuant to the Penal Code⁴⁰ the disclosure of information obtained in the course of professional activities and relating to the health, private life, or commercial activities of another person by an individual who is required by law to maintain the confidentiality of such information, is punishable by a fine.⁴¹ In this case, the accused, as a police inspector, gave information about the victims' place of residence, registered vehicles and violations

³⁵ Amendment of the Taxation Act, available in Estonian at <https://www.riigiteataja.ee/ert/act.jsp?id=901885>.

³⁶ Supreme Court case no. 3-3-1-55-04, available in Estonian at <http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-55-04.html>.

³⁷ Public Information Act, *supra* <http://www.esis.ee/ist2004/106.html>

³⁸ Supreme Court case no. 3-1-1-35-07m, available in Estonian at <http://www.nc.ee/?id=11&tekst=222504645>.

³⁹ Supreme Court case no. 3-1-1-81-08, available in Estonian at <http://www.nc.ee/?id=11&tekst=RK/3-1-1-81-08>.

⁴⁰ Penal Code RT I 2001, 61, 364, available at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30068K8&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusseadustik>.

⁴¹ *Id.* at § 157.

of law to a third person. The police inspector claimed that the forenamed data was neither private nor sensitive⁴² personal data. The Supreme Court held that "private life" includes the whole sphere of personal life, meaning that it also includes information on an individual's place of residence, registered vehicles, and violations of law.

In 2008, the Supreme Court deliberated over whether a request about one's state of health can be considered as "processing" personal data.⁴³ An imprisoned person requested a doctor but, in response to the prison guard's question about the nature of his complaint, refused to disclose the exact ailment. The complainant found that, pursuant to the PDPA, information about one's state of health is confidential, and that the prison guard's request was therefore not legitimate. The Supreme Court upheld the previous decisions made by the administrative and circuit court. It agreed that as the prison guard only made a reasoned request on the nature of the complainant's complaint, no personal data was processed, and therefore the PDPA does not apply. The Supreme Court also agreed that in order to decide whether the need for a doctor is inevitable, the prison guard is entitled to know the grounds of the imprisoned person's request for a doctor.

Another case that involved the DPI found its way to the Supreme Court in 2010. A former political party leader filed a request with a newspaper in 2008 to take down an online article published in 2004. As the publisher (the newspaper) declined, the plaintiff turned to the DPI. The latter compelled the newspaper to take down the online version of the article. The newspaper, in turn, found that the article and personal data it included had been published under the then newly elected party leader's consent, and that the PDPA allows the processing and disclosure of personal data for journalistic purposes even without the data subject's consent, provided that there is a predominant public interest and it is in accordance with the principles of journalism ethics. As the Supreme Court did not find any grounds to hear the matter, the decision of the circuit court entered into force. The circuit court ruled that the public interest in a former party leader remains after the data subject has finished his or her political activity. The court found that the need to preserve already published news for educational and historical purposes gives rise to a predominant public interest that outweighs the interests of the data subject.

⁴² The PDPA gives a list of personal data that is considered to be "sensitive", the list of which is wider than its scope under Art. 8 of the Directive 95/46/EC.

⁴³ Supreme Court case no. 3-3-1-1-09, available in Estonian at <http://www.nc.ee/?id=11&tekst=RK/3-3-1-1-09>.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The 1994 Surveillance Act regulates the interception of communications, covert surveillance, undercover informants, and police and intelligence databases.⁴⁴ Surveillance activities are permitted only if the desired purpose cannot be achieved in a manner that less violates individuals' fundamental rights.⁴⁵ Surveillance can be approved by a "reasoned decision made by the head of a surveillance agency." Surveillance agencies have the right to conduct the following surveillance activities: covert collection of information by persons who are engaged in surveillance activities; covert collection of comparative samples and the covert and initial examinations of documents and objects; covert surveillance and covert examination and replacement of objects; covert identification; collection of information concerning the fact of messages being communicated via telecommunications networks, duration, manner and form of communication thereof, and personal data and location of senders and receivers of such messages.⁴⁶ Obtaining information by wiretapping or covert observation of messages, or other information transmitted by a public electronic communications network, is allowed only in a criminal proceeding, and only with the permission of a preliminary investigation judge. In 2008 and 2009 the court accepted approximately 99 percent of prosecuting authorities' requests and issued 1,804 permits for telephone interception.⁴⁷ Evidence is collected through surveillance activities by a police authority, the Security Police Board, and in some cases also by the Tax and Customs Board, at their own initiative or at the request of an investigative body.⁴⁸ Illegally obtained evidence is not admissible in court. Unlawful surveillance activities, or unlawful and covert collection of information, unlawful concealment or destruction of information collected by surveillance activities or covertly, if conducted by a person with the right arising from law to engage in surveillance or covert collection of information, are punishable by a fine or up to three years' imprisonment.⁴⁹ The legality of surveillance and the activities of the Security

⁴⁴ Surveillance Act, 1994, RT* I 1994, 16, 290 (1994), available in English at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30011K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=j%E4litustegevuse>.

⁴⁵ *Id.* at § 5(5).

⁴⁶ *Id.* at § 12(1).

⁴⁷ Veiko Pesur, "Glikman: jlitustegevuseks antud lubade hulk jahmatab", *Postimees*, 4 March 2010, available in Estonian at <http://www.postimees.ee/?id=232656>.

⁴⁸ *Id.* at §§ 112(2).

⁴⁹ Penal Code at § 315.

Police are monitored by the Security Authorities Surveillance Select Committee, which consists of Parliament members.

National security legislation

There is no update to report under this Section.

Data retention

On 1st January 2005, the new Electronic Communications Act⁵⁰ came into force. The Act replaced the Telecommunications Act and is in accordance with EU legislation. Since January 2008 electronic communications companies are required to preserve traffic and location data as defined by the Data Retention Directive (2006/24/EC) for one year. With respect to communications data relating to Internet access, Internet telephony, and Internet email, electronic communications companies have been required to retain such data since March 2009. Electronic communications companies must only retain such data that becomes known to them in the course of providing communications services. Electronic communications companies must also provide the surveillance agency or security authority with the information at their disposal.⁵¹ Also, electronic communications companies have to grant surveillance agencies and security authorities access to their communications network to conduct surveillance activities or to restrict the right to confidentiality of correspondence.⁵²

National databases for law enforcement and security purposes

The official publication "Official Announcements"⁵³ may represent a problem in the area of personal data protection. Namely, there exists no legal basis for terminating the publication of notices published via a computer network and found via search engines (cache) after the objective of the publication has been fulfilled. Especially serious problems are related to notices that have become misleading insofar as, for example, they incorrectly refer to a person as a debtor, suspect or offender.⁵⁴

The "Punishment Register" is a general national register containing data concerning individuals punished and their punishments. Currently, individuals processing the data in that register, or issuing register notices, are required to maintain the confidentiality of the information they have learned in the course of their official duties. Persons entitled to

⁵⁰ Electronic Communications Act, RT I 2004, 87, 593 (2007), available in English at <http://www.legaltext.ee/text/en/X90001K2.htm>.

⁵¹ *Id.* at § 111(4) and § 112(1).

⁵² *Id.* § 113(1).

⁵³ (in Estonian "*Ametlikud Teadaanded*").

⁵⁴ DPI Annual Report 2008 Summary, available in English at http://www.aki.ee/download/1231/Eess%C3%B5na%202008%20aastaraamat_eng%20280709.pdf.

receive data from the register are enumerated in the Punishment Register Act.⁵⁵ However, draft legislation⁵⁶ that makes the data in the Register public, with some exceptions, is being deliberated by the Parliament. According to the explanatory memorandum of the Act,⁵⁷ pursuant to the PDPA the decisions of misdemeanour and criminal proceedings are not sensitive personal data.

Since 2001 there is a database codenamed "KAIRI" under the jurisdiction of the Ministry of the Interior, with limited public access, and maintained by police authorities. In 2002, the Director General of the Police enacted rules about the maintenance and usage procedure of the database. The rules are confidential. However, according to the media, the purpose of the database is to collect and maintain information about surveillance activities (including photos and operational information) of suspects and fugitives, as well as grant access to other information systems and databases.⁵⁸ The database has approximately 4,500 users, of whom approximately 1,300 have the right to access surveillance information.

A uniform Population Register contains the personal data of Estonian citizens and foreigners with Estonian residence permits, and is administered and developed by the Ministry of the Interior. The data in it is used for performing the tasks assigned under the law to officials of state and local government institutions. Legal entities (companies, NGOs) and individuals have access to its data only if they show a legitimate interest. The administration and issuance of Population Register data has to comply with the requirements of the protection of personal data.⁵⁹

⁵⁵ Punishment Register Act § 13 and § 17, available in English <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X60042K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=karistusregistri>.

⁵⁶ Draft legislation of the Punishment Register Act, available in Estonian at [http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=1034813&file_name=Karistusregistri%20seadus%20\(766\).rtf&file_size=160130&mnsent=762+SE&fd=16.07.2010](http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=1034813&file_name=Karistusregistri%20seadus%20(766).rtf&file_size=160130&mnsent=762+SE&fd=16.07.2010).

⁵⁷ Explanatory memorandum of the draft legislation of the Punishment Register Act, available in Estonian at [http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=1034814&file_name=Karistusregistri%20seadus%20seletuskiri%20\(766\).rtf&file_size=148477&mnsensk=762+SE&fd=2010-07-16](http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/rtf&file_id=1034814&file_name=Karistusregistri%20seadus%20seletuskiri%20(766).rtf&file_size=148477&mnsensk=762+SE&fd=2010-07-16).

⁵⁸ Janar Filippov and Tarmo Vahter, "Politsei salajane andmebaas pälvis poliitikute viha," *Eesti Ekspress*, 16 October 2009, available in Estonian at <http://paber.ekspress.ee/viewdoc/03406B5D67CA83E8C225764F0040E06B>.

⁵⁹ The Population Register contains the following information on Estonian citizens and foreigners with Estonian residence permits: given name and surname, personal ID code, gender, residence data, birth data (date and place of birth), citizenship, existence of foreigners' residence, work permits and term thereof, death data (date and place of death). The following data on individuals is also entered in the Population Register: marital status, information on spouse and children, guardianship, restrictions of active legal capacity, statistical or testimony-based data (nationality, native language, education, field of professional activity), data on documents issued to the individual (number, time of issue and validity of identity card, passport, driver's license, birth certificate, marriage certificate, etc.). Ministry of the Interior, available in Estonian at <http://www.siseministeerium.ee/35796/>.

National and international data disclosure agreements

Estonia joined the Schengen information system on 30 March 2008,⁶⁰ and is a member of Interpol.⁶¹

Cybercrime

The bulk of cyber offences committed in Estonia are computer-related fraud, the manufacture of works involving child pornography, or making child pornography available.⁶² Computer-related fraud formed 0.444 percent of all criminal offences against property in 2003, 0.464 percent in 2007 and 1.299 percent in 2008.⁶³ Therefore, an increase in computer-related fraud can be seen. In 2008, 52 cases of manufacture of works involving child pornography or making child pornography available were registered.⁶⁴ The Parliament has stated in its approval of development trends of criminal policy until 2018⁶⁵ that the fight against cybercrime has to focus on the prevention of sexual abuse of minors, major computer-related fraud, and the spreading of computer viruses. Also, the Parliament has declared that cooperation with the private sector in crime prevention is needed in order to raise the awareness of potential victims. Therefore, the existence of a sufficient number of IT specialists in law enforcement authorities has to be assured.

The Cyber Security Strategy Committee is focused on preventing and combating cyber threats at a state level. The Committee is led by the Ministry of Defence. Estonia hosts the Cooperative Cyber Defence Centre of Excellence (CCD COE) that was formally established on 14 May 2008, in order to enhance NATO's cyber defence capability. In the spring of 2010, the Ministry of the Interior submitted Estonia's official proposal to host the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.⁶⁶

⁶⁰ Estonia: Schengen expanded to airports, available at <http://www.schengenspace.com/taxonomy/term/39>.

⁶¹ European Police and Justice Systems, available at <http://www.interpol.int/Public/Region/Europe/pjsystems/Estonia.asp>.

⁶² Timo Reinthal, "Kuritegevuse kohtupraktika Eestis", in Estonian available at <http://www.riigikohus.ee/vfs/899/Kyberkuritegevus%202009.pdf>.

⁶³ *Id.*

⁶⁴ Explanatory memorandum of the approval of development trends of criminal policy until 2018, in Estonian available at [http://www.just.ee/orb.aw/class=file/action=preview/id=50604/Seletuskiri+\(kriminaalpoliitika+arengusuunad+aastani+2018\).pdf](http://www.just.ee/orb.aw/class=file/action=preview/id=50604/Seletuskiri+(kriminaalpoliitika+arengusuunad+aastani+2018).pdf).

⁶⁵ Approval of development trends of criminal policy until 2018, in Estonian available <http://www.just.ee/orb.aw/class=file/action=preview/id=50603/Kriminaalpoliitika+arengusuunad+aastani+2018.pdf>.

⁶⁶ Estonia bidding to host the IT Agency in the field of justice and home affairs, 29 April 2010, available at <http://www.siseministeerium.ee/estonia-bidding-to-host-the-it-agency-in-the-field-of-justice-and-home-affairs/>.

Critical infrastructure

The collection and processing of information concerning activities aimed at changing the constitutional order or territorial integrity of the state by force, and the prevention and blocking of terrorism and its financing is in the hands of the Security Police Board.⁶⁷ It collects and processes information, including personal data, insofar as is necessary for performing its functions.⁶⁸ The exact measures used for performing them are not known. However, the Security Police Board can only use the measures that are necessary for performing its functions.⁶⁹ In case there is a choice between several measures, the authority shall use the measure that causes the minimum level of restrictions to individuals' fundamental rights in connection with the performance of its functions: a measure may be used only if the restrictions it causes to an individual's fundamental rights are not disproportionate to the objective the Security Police Board aims to achieve. This authority may restrict an individual's right to the confidentiality of the messages he sends or receives by post, telephone or other commonly used means.

INTERNET & CONSUMER PRIVACY

E-commerce

Pursuant to the Trading Act, "e-trade" means the offer for sale, or sale of goods or services, on the Internet without the parties being simultaneously present.⁷⁰ As the processing of personal data is permitted only with the data subject's consent, unless otherwise provided by law, commercial emails to physical persons can be sent to emails given by the addressees. Pursuant to the Law of Obligations Act, an offer may be communicated to the consumer by facsimile, telephone answering machine, or electronic mail only with the consumer's prior consent.⁷¹ Furthermore, commercial emails can be sent only with the addressee's prior consent ("opt-in"), whereby the addressee has to have the possibility to prohibit such use of his or her contact data in the future.⁷² Violation of this obligation is punishable by a fine in misdemeanour proceedings amounting to

⁶⁷ Security Authorities Act § 6(1) and § 6(21), available at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X50038K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=julgeolekuasu>.

⁶⁸ *Id.* at § 3(1).

⁶⁹ *Id.* at § 3(2).

⁷⁰ Trading Act § 2, available at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X80015K1&keel=en&pg=1&ptyyp=RT&tyyp=X&query=kaubandustegevus>.

⁷¹ Law of Obligations Act § 60, available at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30085K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=v%F51a%F51gusseadus>.

⁷² Electronic Communications Act § 1031(1) and § 1031(3), *supra* at 106.

approximately €1,150.⁷³ For the same act, if it is committed by a legal person, the fine may go up to approximately €31,956.⁷⁴

Cybersecurity

Dissemination of spyware, malware, or computer viruses is punishable by a fine or up to three years' imprisonment.⁷⁵ The same act, if it is committed at least twice, or if it causes significant damage, is punishable by a pecuniary punishment or up to five years' imprisonment.⁷⁶

Online behavioural marketing and search engine privacy

There are no laws in Estonia that expressly regulate online behavioural marketing or search engine privacy. However, the DPI has issued guidelines about the privacy risks of search engines.⁷⁷ In general, digital data can be tracked and linked to a particular person on a case-by-case basis due to data retention obligations imposed on telecommunications companies and Internet service providers. These entities are, for example, compelled to retain the real names and addresses of their customers, to whom an IP address, a user name, or a number has been allocated, as well as the exact period of Internet sessions, etc.⁷⁸ However, such data can only be made available to the surveillance or security authorities, the Financial Supervision Authority, and the courts.⁷⁹

Online social networks and virtual communities

According to a survey conducted in December 2009, the most popular social network in Estonia is Orkut, which is used on a monthly basis by 26 percent of respondents.⁸⁰ Also, there are approximately 255,000 Facebook users in Estonia (or roughly one-fifth of the population), of whom 57.7 percent are females and 63.3 percent are between 18 and 34 years old.⁸¹ Other social networks, such as Twitter, MySpace, and LinkedIn, are used by approximately 5 percent of the population.

⁷³ *Id.* at § 1842(1).

⁷⁴ *Id.* at § 1842(2).

⁷⁵ Penal Code § 208(1), *supra* at 93

⁷⁶ *Id.* at § 208(2).

⁷⁷ The Estonian Data Protection Inspectorate. Risks of Web searches, available in Estonian at http://www.aki.ee/download/933/Ohud%20ehk%20v%C3%B5imalused%20veebiotsingu%20maailmas%20_121208.pdf.

⁷⁸ Electronic Communications Act § 1111(3), *supra* at 106.

⁷⁹ *Id.*, § 1111(11).

⁸⁰ "GfK uuring: lõviosa noori regulaarselt Orkutis, Twitteris veel mitte," January 2010, available <http://www.gfk.lv/et/node/399>.

⁸¹ At <http://www.checkfacebook.com/>.

The DPI has posted on its Web site an Estonian translation of the International Working Group on Data Protection in Telecommunications' "Report and Guidance on Privacy in Social Network Services", most likely to use it as a tool to interpret the data protection requirements in this field.⁸²

Online youth safety

Estonian children have excellent access to the Internet. According to a survey carried out in 2008, 93 percent of children in the 6 to 16 age group use the Internet. However, in contrast to other EU countries,⁸³ only 22 percent of parents expressed concern that their child might be the victim of online grooming.⁸⁴ In March 2008, a 16-year-old boy committed suicide, it was presumed due to an online molester who threatened to publish indecent photographs of the victim that he had gathered. Apparently 43 Estonian minors were molested by the same person, who is currently in prison for preliminary investigation. This incident brought the importance of online youth safety acutely into the spotlight. In 2009, the Ministry of Social Affairs summoned a children's online safety working group, which it has been coordinating ever since.⁸⁵ The same Ministry also represents Estonia in the EU Safer Internet Programme. The Estonian Union for Child Welfare has also been actively involved in the process of promoting online safety. Since 15 March 2010, online grooming is punishable by a fine or up to three years' imprisonment.⁸⁶ According to the explanatory memorandum of the Penal Code the purpose of the amendment is to prevent the sexual abuse of minors.⁸⁷

⁸² Available at <http://www.aki.ee/download/816/Sotsiaalv%C3%B5rgud.pdf>.

⁸³ In the European Union, 60 percent of parents were very or rather worried that their child could become a victim of online grooming. European Commission, *Eurobarometer*, Toward safer use of the Internet for children in the EU – A parents' perspective, December 2008, available at http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2008.pdf.

⁸⁴ Explanatory memorandum of the draft legislation of the amendment act of the Penal Code, available in Estonian at [http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=854794&file_name=KarS%20muutmine%20seletuskiri%20\(643\)%20seksuaalkuritegu.doc&file_size=101888&mnsensk=640+SE&fd=2010-04-22](http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=854794&file_name=KarS%20muutmine%20seletuskiri%20(643)%20seksuaalkuritegu.doc&file_size=101888&mnsensk=640+SE&fd=2010-04-22).

⁸⁵ Available in Estonian at <http://www.sm.ee/sinule/lapsele/turvaline-internet/koostoogrupp.html>.

⁸⁶ Penal code § 1781(1), *supra* at 93.

⁸⁷ Explanatory memorandum of the draft legislation of the amendment act of the Penal Code, available in Estonian at [http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=854794&file_name=KarS%20muutmine%20seletuskiri%20\(643\)%20seksuaalkuritegu.doc&file_size=101888&mnsensk=640+SE&fd=2010-04-22](http://www.riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&file_id=854794&file_name=KarS%20muutmine%20seletuskiri%20(643)%20seksuaalkuritegu.doc&file_size=101888&mnsensk=640+SE&fd=2010-04-22).

TERRITORIAL PRIVACY

Video surveillance

Pursuant to the PDPA,⁸⁸ surveillance equipment transmitting or recording personal data may be used for the protection of persons or property only if this does not excessively damage the justified interests of the data subject, and the collected data is used exclusively for the purpose for which it is collected. In such a case, sufficiently clear communication of the fact of the use of the surveillance equipment and of the data processor's name and contact details substitutes for the consent of the data subject. Private (legal) persons are not allowed to monitor or record images from the public space. However, in cases where an entrance to the premises is being filmed, the recording of public space to some extent is inevitable. According to the Security Act, which provides the conditions and procedure for the activities of companies providing security services, a security agent is required to observe individuals' constitutional rights while using video technology.⁸⁹ Pursuant to the Police and Border Guard Act, the police is authorised to use surveillance equipment that transmits or records images from public spaces only if the public has been previously informed about the surveillance.⁹⁰ The same principle is also reflected in the draft legislation of the Maintenance of Law and Order Act that is currently being deliberated by the Parliament.⁹¹ The use of CCTV cameras in Estonia is increasing but because of the lack of official data the exact scope of video surveillance cannot be adequately estimated.

The DPI has held that webcast security camera images, where the activities of a data subject may be observed in detail without his or her knowledge, constitute a breach in the right to privacy. However, webcams that only show a street view or scenery at a wide angle are permitted.⁹²

Location privacy (GPS, mobile phones, location based services, etc.)

The regulation of technologies that link an individual to a physical location is subject to the same rules as any other surveillance activity.

⁸⁸ Personal Data Protection Act § 14(3), *supra* at 4.

⁸⁹ Security Act § 33 5), RT I 2003, 68, 461, available in English at <https://www.riigiteataja.ee/ert/act.jsp?id=13249880>.

⁹⁰ Police and Border Guard Act § 720, RT I 2009, 26, 159, available in Estonian at <http://www.aki.ee/est/?part=events&id=47>.

⁹¹ Draft legislation of the Maintenance of Law and Order Act, available in Estonian at http://riigikogu.ee/?page=pub_file&op=emsplain&content_type=application/msword&u=20100827112826&file_id=505953&file_name=49%20SE%20II-2%20tekst%20p%C3%A4rast%20katkestamist%2017.12.2008.doc&file_size=210944&mnsent=49+SE&fd=22.04.2010.

⁹² The Estonian Data Protection Inspectorate, available in Estonian at <http://www.aki.ee/est/?part=events&id=47>.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

Biometric data is sensitive personal data.⁹³ Since 22 May 2007, the Republic of Estonia has been issuing biometric passports for Estonian citizens, putting the holder's biometric data onto a chip.⁹⁴ Pursuant to the Identity Documents Act, the biometric data of the holder of a document may be processed only in the cases and under the conditions provided by law.⁹⁵ The Government has established a database for identity documents⁹⁶ for internal use only, with limited access.

NATIONAL ID & SMART CARDS

Pursuant to the Identity Documents Act, identity (ID) cards are mandatory for all Estonian citizens over the age of 15 and resident aliens. In Estonia, an identity card is an internal document held by an Estonian citizen or an alien staying permanently in Estonia.⁹⁷ The following personal data may be entered on it concerning its holder: name; date and place of birth; personal identification code; photo or facial image; sex; citizenship; fingerprint images; signature or image of signature; iris images; hair colour; other personal data as prescribed by an international agreement, a law, or other legislation of general application established on the basis thereof.⁹⁸ The first Estonian ID Card was issued on 28 January 2002. All ID cards enable the electronic identification of individuals and the digital signing of documents. As of 6 September 2010, there are over 1.1 million active ID cards, whereas the population of Estonia is 1.3 million. Over 37 million electronic signatures have been provided and more than 63 million electronic authentications have been made using the ID card since its launch in 2002.⁹⁹

Under the General Part of the Civil Code Act, digitally signed documents have the same probative value as documents with written signatures.¹⁰⁰ The use of the digital signature is mandatory for public sector institutions. Digital signatures are used throughout the Estonian court system for communications between parties and by the Estonian Tax Board when receiving tax documents from individuals or businesses, and in order to

⁹³ Personal Data Protection Act § 4(2), *supra* at 4.

⁹⁴ Available at <http://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/eesti-kodaniku-pass/index.dot>.

⁹⁵ Identity Documents Act § 92(5), RT I 1999, 25, 365, available in English at <https://www.riigiteataja.ee/ert/act.jsp?id=13276890>.

⁹⁶ *Id.* at § 152(1).

⁹⁷ *Id.* at § 19(1).

⁹⁸ *Id.* at § 9(3).

⁹⁹ ID.ee Web site, available at <http://id.ee/>.

¹⁰⁰ General part of the Civil Code Act, RT I 2002, 35, 216, § 80 (1), available in English at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30082K2&keel=en&pg=1&ptyyp=RT&tyyp=X>.

conclude loan agreements with online banks.¹⁰¹ A personal identification number (PIN) is used to activate the card.¹⁰² For resident aliens with valid documents, the ID card also contains residence and work permit data.¹⁰³ Any Estonian citizen over 14 years of age residing permanently in Estonia shall hold an identity card.¹⁰⁴ In the same way, any alien residing permanently in Estonia on the basis of a valid residence permit or right of residence shall hold an identity card.¹⁰⁵

The ID-card can be used to get access to Internet-based services provided by the state as well as by private companies. Some of the services this card provides are: digital signatures, encryption, electronic voting, online banking, electronic tickets for public transportation, iPatient (an online patient information portal of the East Tallinn Central Hospital), online filing of tax forms with the Tax Board, registration of company-related information with the Company Registration Portal, etc.

The police are authorised to check the identity of a person on the basis of his identity card for safety reasons.¹⁰⁶ Also, businesses selling alcoholic beverages are authorised to request an identity card from the individuals they sell them to who look like minors.¹⁰⁷ Since May 2007 a "Mobile-ID service" gives customers the ability to identify themselves by using their mobile phone.¹⁰⁸ The user enters into a contract to use the Mobile-ID services, swaps out his old SIM card for a new one and "gets the usual PIN and PUK keys plus additional codes needed for Internet-based personal identification and issuance of digital signatures."¹⁰⁹

RFID tags

There is neither specific legislation nor reliable data or information regarding the use of RFID tags. However, the general data protection framework is applicable to the processing of personal data through RFID technology.

¹⁰¹ Terms of Use for the National ID Card Certificates, available in English at http://www.pass.ee/index.php/pass/eng/id_card/terms_of_use_for_the_national_id_card_certificates.

¹⁰² *Id.*

¹⁰³ Benefits Today and Tomorrow at http://www.pass.ee/index.php/pass/eng/id_card/benefits_today_and_tomorrow.

¹⁰⁴ *Id.* at § 5(1).

¹⁰⁵ *Id.* at § 6(1).

¹⁰⁶ Police and Border Guard Act § 7¹⁸(1), *supra* at **Error! Bookmark not defined.**

¹⁰⁷ Alcohol Act, RT I 2002, 3, 7, available in English at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40060K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=alkohol>.

¹⁰⁸ idBlog, "EMT Launches the Mobiil-ID Service," 2 May 2007 http://www.id.ee/blog_en/?p=20.

¹⁰⁹ *Id.*

BODILY PRIVACY

Pursuant to the Police and Border Guard Act¹¹⁰ the police are entitled to use direct coercion to conduct invasive procedures – as long as it is inevitably necessary and complies with the law – such as compelling individuals to provide bodily fluid samples, DNA, or fingerprints. This has been a hugely controversial subject that has generated a lot of media attention.

WORKPLACE PRIVACY

Since 1 July 2009 the Employment Contracts Act¹¹¹ contains a provision pursuant to which an employer is required to respect employees' privacy and verify the performance of their duties in a manner that does not violate the employee's fundamental rights. However, there is neither regulation nor case law regarding the employer's specific rights with respect to monitoring its employees' Internet browsing, phone use, etc. Therefore, today the most efficient way to regulate the monitoring of employees' activity in the workplace is through an employment contract.

HEALTH & GENETIC PRIVACY

Health privacy

According to the Health Care Services Organisation Act,¹¹² from 1st January 2009 all medical institutions will have to record health data in the general Electronic Health Record System (EHRs). It is not possible for a patient, as a data subject, to oppose the recording of his health record in the health information system. However, the patient may block access to some or all of the health data recorded about him through a patient portal¹¹³ or during a visit to a medical institution. Patients can access all data recorded about them in the EHRs themselves but, if it is necessary to protect the patient's life or health, the healthcare provider may, upon entering the patient's health record in the EHRs, restrict the patient's access to some of his health record or limit access to only a health care provider.

Genetic privacy

On 13 December 2000, the Estonian Parliament approved the Human Genes Research Act.¹¹⁴ The Act created a national genetic database to be used for research into diseases.

¹¹⁰ Police and Border Guard Act § 7¹⁹, 7²⁶, 7²⁷.

¹¹¹ Employment Contracts Act RT I 2009, 5, 35, available in English at <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX042&keel=en&pg=1&ptyyp=RT&tyyp=X&query=t%F6%F6leping>.

¹¹² RT I 2001, 50, 284.

¹¹³ At <http://www.digilugu.ee>.

¹¹⁴ Human Genes Research Act, RT I 2000, 104, 685, available in English at <http://www.legaltext.ee>.

The database is owned and controlled by the Estonian Genome Project Foundation.¹¹⁵ However, the Estonian government provides only 20 percent of the funding for the project. A United States registered company, EGeen International Corporation, has agreed to provide the remaining financing.¹¹⁶ The focus of the Estonian database is different than that of the Icelandic database. Rather than looking for genes that cause disease, as in Iceland, the Estonian project is focusing on how genes influence individual responses to medicines.¹¹⁷ The main project is underway after successful completion of pilot programmes in three regions.¹¹⁸

Privacy protection for donors is included in the project design. Doctors who collect samples and medical histories for the project must register their databases with the DPI before they can participate. Individual data is stored in coded form on computers that are not connected to any network. The rights of donors and the consent form they have to sign before donating their samples are publicly available on the Web site of the Estonian Genome Project Foundation.¹¹⁹ These rights include: voluntary consent, anonymity, the right to obtain one's own information or give one's doctor the ability to obtain the information, and the right to have all data removed and deleted from the database.¹²⁰

The DPI has expressed concern over the lack of pharmacy service providers – there are approximately 300 of them in Estonia – registering for processing sensitive information.¹²¹ Each healthcare provider must have a method for registering complaints, their resolution methods, patient feedback, sending on-time notifications to patients on waiting lists about transfers to different healthcare specialists, or about substitutions for their health care professionals.¹²²

FINANCIAL PRIVACY

Pursuant to the Credit Institutions Act¹²³ a credit institution is, upon entry into a contract or a transaction, required to identify his client or the client's representative. If the institution has already identified either one in an earlier transaction, it is authorised to

¹¹⁵ See generally, *Eesti Geenivaramu* at <http://www.geenivaramu.ee/index.php?lang=eng>.

¹¹⁶ "Estonian Genome Foundation Signs Pilot Project Financing Accords," Baltic News Service, 2 January 2002.

¹¹⁷ Mark Frary, "Estonian Genome Project ahead of Schedule," Estonian Genome Foundation, 23 December 2002 *here*.

¹¹⁸ A. Metspalu et al., "The Estonian Genome Project in the Context of European Genome Research," Estonian Genome Foundation, 30 April 2004 *here*.

¹¹⁹ Gene Donor Consent Form *here*.

¹²⁰ Gene Donor Consent Form, Regulation No. 125 (17 December 2001), available in English *here*.

¹²¹ Data Protection Inspectorate, *supra* *here*.

¹²² RTL 2004, 158, 2376, 28 December 2004.

¹²³ Credit Institutions Act § 89(21), RT I 1999, 23, 349, available in English *here*.

require additional identification, and also has the right to verify the validity of identity documents and to obtain personal data from databases of the state agencies that issued the documents. The standard terms of the agreement between the credit institution and the client may include a consent clause by which the client agrees to have the institution process his personal data.¹²⁴

The criminalisation of identity theft through complementary provisions of the Penal Code entered into force on 15 November 2009. According to Article 157² of the Penal Code, the illegal use of another person's identity is punishable by a fine or up to three years' imprisonment.¹²⁵

E-GOVERNMENT & PRIVACY

The Estonian Parliament first allowed e-voting on 28 June 2005. E-voting is provided for in the Local Government Council Election Act (§ 50), the Riigikogu Election Act (§ 44), the European Parliament Election Act (§ 43), and the Referendum Act (§ 37). The infrastructure enabling secure electronic personal authentication and electronic ID cards (e-ID cards) was in place before the adoption of the Law on Personal Identity Documents. E-voting is secret and takes place four to six days before Election Day.¹²⁶ The system uses asymmetric cryptography, and contains a system key pair to guarantee voting secrecy.¹²⁷ A voter may change his vote either by voting electronically or by casting a paper ballot at a polling station. The last vote is the one that is counted.

The Estonian e-voting system, which uses the Estonian e-ID card to identify voters, was developed for the Estonian National Electoral Committee. In order to vote online, voters need first to access the election Web site, then identify themselves with their e-ID card. The Voter Forwarding Server (VFS) then checks the voter's personal identification code from the voter list database, verifies the voter's eligibility, then identifies the constituency. The VFS notifies the voter if he has already voted. The voter selects the candidate and is asked to confirm his selection. Then the vote is encrypted and signed using the voter's digital signature.

OPEN GOVERNMENT

The Public Information Act was approved by the Parliament and entered into force on 1 January 2001. Supervision and enforcement of the Act will be conducted by the DPI. The law includes significant provisions on electronic access. Government departments and

¹²⁴ *Id.* at § 89(22).

¹²⁵ "The forwarding of, enabling access to or using information which identifies, or enables to identify, another person, without the person's consent, for the purpose of knowingly creating a misleading image of the person by pretending to be him or her, and provided that it damages the other person's rights or interests protected by law, or for the purpose of hiding a criminal offence, is punishable by a pecuniary punishment or up to three years' imprisonment." Article 157² of the Penal Code, RT I 2009, 51, 348.

¹²⁶ Estonian E-Voting System at http://www.vm.ee/estonia/kat_340/pea_172/7025.html.

¹²⁷ *Id.*

other holders of public information will have a duty to post information on the Web, and email requests must be treated as official requests for information.¹²⁸ During the period from October 2005 to September 2006, the DPI received 99 complaints, requests for explanation or memoranda based on the Public Information Act. This resulted in eight misdemeanour proceedings.¹²⁹ The majority of the complaints stemmed either from government Web sites violating provisions of the PIA or failure of the Web site owner to comply with requests for information.¹³⁰

In 2006, the Centre of Registers of the Ministry of Justice was merged with the Ministry of Justice's IT division, becoming the Centre of Registers and Information Systems of the Ministry of Justice.¹³¹ The purpose of the agency is to develop and administer the registers and infosystems in the Ministry of Justice and to provide communication and IT services.¹³² The regulation enacts usable information systems and related security measures systems in the maintenance of state and local governments' databases. The security measures system consists of the regulation of specifying security requirements and the description of data's organisational, physical, and technical security measures. The regulation comprises the description of security classes and levels. Security classes are divided into four components: time criticality, severity of consequences of delay, integrity, and confidentiality. A new information policy action plan, taking into account the objectives and priorities of the EU information strategy, i2010, is currently under discussion in the Ministry of Economic Affairs and Communications.¹³³

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

No updates.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Estonia is a member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹³⁴ In November 2001, Estonia ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (Convention No.

¹²⁸ Public Information Act, *supra* here.

¹²⁹ Data Protection Inspectorate, *supra* at 11 here.

¹³⁰ *Id.*

¹³¹ Ministry of Economic Affairs and Communications, "Information Technology in Public Administration of Estonia Yearbook 2005," 2006 at 78, available in English at http://www.riso.ee/en/pub/yearbook_2005.pdf.

¹³² *Registrite ja infosüsteemide keskus* at http://www.eer.ee/index_eng.phtml.

¹³³ Ministry of Economic Affairs and Communications, *supra* at 78, available at http://www.riso.ee/en/pub/yearbook_2005.pdf.

¹³⁴ Signed 14 May 1993; ratified 16 April 1996; entered into force 16 April 1996.

108).¹³⁵ Also in November, Estonia signed and ratified the CoE Convention on Cybercrime.¹³⁶

On 1 December 2009, when the Treaty of Lisbon entered into force, the Charter of Fundamental Rights became binding upon the Republic of Estonia.

¹³⁵ Signed 24 January 2000; ratified 14 November 2001; entered into force 1st March 2002.

¹³⁶ Signed 23 November 2001; ratified 5 December 2003; entry into force 1st July 2004.

REPUBLIC OF FINLAND¹

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Section 10 of the Constitution of Finland, entitled "The right to privacy", states: "Everyone's private life, honour, and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony, and other confidential communications is inviolable. Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual, society, or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act."² Additionally, Section 12 of the Constitution, titled "Freedom of expression and right of access to information," provides that "documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings."³

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Personal Data Act of 1999 (PDA)⁴ went into effect on 1 June 1999. The PDA replaced the 1987 Personal Data File Act⁵ to make Finnish law consistent with the EU Data Protection Directive.⁶ The PDA was amended by the Act on the Amendment of the Personal Data Act, effective 1 December 2000, to incorporate provisions on policy and

¹ The EPHR 2010 "Finland" report has been updated first in June 2009 by Amie Stepanovich (Electronic Privacy Information Center, Washington, DC, USA), then, in September 2010, by Ilona Teräkivi (LMR Attorneys Ltd., Helsinki, Finland) and Eija Warma (Castrén & Snellman Attorneys Ltd, Helsinki, Finland).

² Constitution of Finland (unofficial translation), available at <http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf>.

³ *Id.*

⁴ Personal Data Act (523/99) (unofficial translation), available at <http://www.tietosuoja.fi/uploads/hopxtvf.HTM>.

⁵ Personal Data Files Act (Law No. 471/87).

⁶ See Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

effects of the European Commission's decision-making.⁷ Under the PDA, everyone has the right of access to the data files on him or her or to notice that the file contains no such data. If a data controller refuses to rectify an error at the request of a data subject, the data subject may inform the Data Protection Ombudsman (DPO) of the matter. The DPO may order a data controller to recognize the data subject's right of access or to rectify an error. The PDA does not apply to processing of personal data for a private or purely personal use. Activities of "the media, the arts and literary expression" are also excluded from its scope. Exemptions for defense and public security are included in separate provisions of the PDA.

The PDA introduces the concept of informed consent and self-determination into Finnish law, giving data subjects the rights to access or correct their data, or to prohibit their use for stated purposes. The previous act regulated the use and disclosure of information in a personal data file but did not generally require the individual's consent or provide for the same level of notice and access.⁸ Processing without consent may still occur under the new system – for example, if there is "assumed consent", or the Data Protection Board (DPB) has granted permission, or if the matter concerns publicly available data on the "status, duties or performance" of a public figure.⁹ The PDA lays down civil and criminal sanctions (including imprisonment of up to one year)¹⁰ for unlawful processing.^{11, 12}

Sector-based laws

Telecommunications privacy is regulated by the Act on the Protection of Privacy in Electronic Communications ("Electronic Communications Act"), which entered into force on 1 September 2004.¹³ The Electronic Communications Act is broad in scope, covering all telecommunications, including emails and communications on the Internet.¹⁴ Together with Section 10 of the Constitution of Finland,¹⁵ the Electronic

⁷ Amendment of the Personal Data Act (986/2000) (unofficial translation), available at <http://www.tietosuoja.fi/uploads/p9qzq7zr3xxmm9j.rtf>.

⁸ Peter Blume *et al.*, *Nordic Data Protection* 49 (DJOF Publishing 2000).

⁹ *Id.*

¹⁰ See Finland Penal Code 1389/99, Chapter 38, § 9 (unofficial translation), available at <http://www.finlex.fi/pdf/saadkaan/E8890039.PDF>,

¹¹ Personal Data Act (523/1999), *supra*.

¹² The latest amendment to the PDA relates to the processing of identity numbers, adding companies offering payment services to the list of operations that are allowed to process identity numbers in their business. Amendment (294/2010) of 1 May 2010 to the Personal Data Act (523/99), available in Finnish at <http://www.finlex.fi/fi/laki/alkup/2010/20100294>.

¹³ Act on the Protection of Privacy in Electronic Communications (516/2004) (unofficial translation), available at <http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf>.

¹⁴ *Id.*

¹⁵ See Chapter Constitutional Privacy Framework, *supra*.

Communications Act ensures a right to confidential communications: all messages, identification data and location data are confidential, unless the Electronic Communications Act or another act provides otherwise.¹⁶ The confidentiality means that the messages and identification data can be processed only for the purposes set out in the law. The protection includes all messages transmitted in the communications network, this including for instance so called “pre-paid” connections. There is, however, an important exception to the main confidentiality rule described above: where a message has been transmitted to be universally received, it is not considered confidential. The identification data associated with such message is, however, confidential.¹⁷ Practically, this means that everyone is entitled to express his opinion in various social networks and discussion forums. The administrators of such forums are not, however, entitled to disclose any identification data, such as IP addresses.¹⁸

The Electronic Communications Act also clarifies rules for processing confidential identification and location data: except in an emergency, telecommunications users aged 15 years or older may not be located without their prior consent.¹⁹ The DPO oversees the processing of location data. *(See more details under the "Location Privacy" section.)*

The Electronic Communications Act provides new means to prevent unsolicited commercial emails ("spam") and viruses. Previous legislation banning the sending of spam failed to protect against messages sent from outside Finland; thus, the Act permits telecommunications operators and corporate and association subscribers to block email and to remove malicious content in order to protect against security infringement or to ensure communications access.²⁰ The Electronic Communications Act prohibits direct marketing through email or mobile telephone except with the user's prior consent.²¹

The Finnish government has enacted special ordinances that apply to particular personal data systems. These include those operated by the police such as criminal information systems,²² the National Health Service, passport systems, population registers,²³ farm

¹⁶ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 2, § 4 (1).

¹⁷ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 2, § 4 (2).

¹⁸ Sanna Helopuro, Juha Perttula, Juhapekka Ristola: Sähköisen viestinnän tietosuoja (Talentum, Helsinki 2004), pp. 45-47.

¹⁹ Finland Ministry of Transport and Communication, "New Means to Improve Data Protection and Information Security—Act on Data Protection in Electronic Communications to Enter into Force on 1st September," Press release, 16 June 2004, available at <http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=113506>.

²⁰ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 5, § 20.

²¹ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 7, § 26.

²² Criminal Records Act (770/93).

²³ Act on Population Information (1993/507).

registers, and motor vehicle registers.²⁴ In January 2001, a new law on the status and rights of social welfare clients came into force and includes data protection provisions relating to the use of social services.²⁵

On 1 October 2004, the Act on the Protection of Privacy in Working Life took effect.²⁶ The Act determines the legality of several privacy issues in the workplace, such as psychological, genetic, and drug tests; the processing of medical histories and health information; and the use of video and audio surveillance devices. The main principle of the Act is that the employer shall collect personal data about the employee primarily from the employee himself. In order to collect personal data from elsewhere, the employer must obtain the employee's consent.²⁷ (*See more details under the "Workplace Privacy" section.*)

DATA PROTECTION AUTHORITY

The Data Protection Ombudsman (DPO) enforces the Personal Data Act of 1999 (PDA) and receives complaints. The DPO's primary tools for compliance with legislation are direction and guidance. Under the PDA, the DPO provides direction and guidance on the processing of personal data and supervises the processing to achieve the objectives of the statute. Before bringing charges of a violation of the PDA, the public prosecutor must hear from the DPO. In such cases, the court affords the DPO an opportunity to be heard.²⁸

The number of new cases brought before the DPO increased by approximately 20 percent from 2004 to 2005.²⁹ Every complaint directed at the public sector was matched by nearly two complaints directed at the private sector. The DPO explains that this development is probably because while public authorities are usually regulated by law, private companies often try to test the boundaries of legal protections. The change in proportion between public and private sector complaints represents a deterioration in the private sector rather than an improvement in the public sector. The number of complaints against the public sector has remained fairly static.³⁰ When comparing the latest figures,

²⁴ Jorma Kuopus, *Data Protection Regulatory System - Data Transmission and Privacy* (D. Campbell & J. Fisher, eds., Martinus Nijhoff Publishers 1994).

²⁵ Act on Experiments with Seamless Service Chains in Social Welfare and Health Care Services and with a Social Security Card (811/2000) (unofficial translation), available at <http://www.finlex.fi/pdf/saadkaan/E0000811.PDF>.

²⁶ Act on the Protection of Privacy in Working Life (759/2004), available at <http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf>.

²⁷ Article 4.

²⁸ Personal Data Act (523/1999), Chapter 9, § 41.

²⁹ Article 29 Working Party on Data Protection, Ninth Annual Report (2006) at 34, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf.

³⁰ Review 2005 Of The Data Protection Ombudsman, available at <http://www.tietosuoja.fi/uploads/q0vwlft5.rtf>.

the number of unprompted cases brought before the DPO increased by 232 percent from 2008 and 2009, and the number of statements issued by the DPO increased by 55 percent.³¹ As of July 2010, there were 20 staff employed by the Data Ombudsman's office.³² Each DPO inspector specialises in a particular field, including education, social services, working life, and credit issues.³³

The Data Protection Board (DPB) resolves disputes and hears appeals of decisions rendered by the DPO and, under the PDA, grants permissions for the processing of personal data.³⁴ The DPB consists of a chair, a deputy chair, and five members, and they are required to be familiar with the operations of the register. The Board is appointed by the Council of State for a term of three years.³⁵ At the DPO's direction, the DPB drafts regulations for the processing of personal data. The DPO must be heard during the preparation of legislative or administrative reforms that may affect individual privacy rights.³⁶ In 2009, the DPO issued 72 (against 45 in 2005) statements on legislative matters related to the protection of personal rights or freedoms in the processing of personal data and 39 (as opposed to 20 in 2005) on administrative reform projects.³⁷

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In May 2005 the Helsinki District Court handed down suspended sentences to five defendants in a case involving unauthorized use of mobile telephone records by executives of telecommunications service provider Sonera.³⁸ The court found there had been extensive misuse of telecommunications information at Sonera from 1998 to 2001.³⁹ The case was appealed, and the Court of Appeals affirmed the sentences in March 2007, also increasing the amount of monetary damages and court costs. The Supreme Court did not grant permission to appeal the case, making the decision final.⁴⁰ (*See more details under the "Location Privacy" section.*)

³¹ The DPO Annual Report of 2009, available at <http://www.tietosuoja.fi/uploads/dr3ecvra.pdf>.

³² *Tietosuojavaaltuutetun Toimisto*, available at <http://www.tietosuoja.fi/>.

³³ *Tietosuojavaaltuutetun Toimisto*, *supra*.

³⁴ Personal Data Act (523/1999), Chapter 9, § 38.

³⁵ Statutory Order on the Data Protection Board and Data Protection Ombudsman (3.6.1994/432) (no English translation available), available at <http://www.finlex.fi/fi/laki/ajantasa/1994/19940432>.

³⁶ Personal Data Act (523/1999), Chapter 9, § 41.

³⁷ Article 29 Working Party on Data Protection, Ninth Annual Report (2006), *supra* at 35.

³⁸ "Five Get suspended Sentences in Sonera Telephone Record Case," *Helsingin Sanomat* International Edition, 30 May 2005, available at <http://www.hs.fi/english/article/1101979719153>.

³⁹ *Id.*

⁴⁰ "Court of Appeals Affirms Sentences in Sonera Snooping Case," *Helsingin Sanomat* (International Edition), 16 March 2007, (English translation) available here.

In February 2007, the Supreme Administrative Court agreed that the right of access extends to data on a bank client's own loan transactions and their associated interest rates. (See more details under the "Financial Privacy" section.)

The demand for instant loans requested via mobile phone or over the Internet has dramatically increased in Finland in recent years. In March 2007 the Data Protection Board (DPB), at the request of the Data Protection Ombudsman (DPO), ordered an instant loan company to change their authentication process pertaining to loan applicants. The DPB required that creditors identify their clients in order to ensure the accuracy of any personal data processed. The case proceeded to the Supreme Administrative Court, which gave its ruling in January 2010 in accordance with the decision of the Data Protection Board.⁴¹ (See more details under the "Financial Privacy" section.)

On 17 July 2008, in *I v. Finland*,⁴² the European Court of Human Rights (ECtHR) decided a case on the issue of an individual's right to find out, on the basis of log data, who had had access to his patient records. However, the hospital's data system had been implemented in such a way that the administration of access rights and log files did not allow the tracking of the individuals who had accessed the patient's health records. As a result, and by applying the principle of obligatory prosecution, the Finnish court could not convict any specific person of a crime. The ECtHR stated that a lack of protection had resulted, caused by the functional characteristics of a data system that was not controlled as provided by law, and in which the protection of the individual's personal life, as guaranteed by Article 8 of the European Convention on Human Rights, had been violated.

On 2 December 2008, the European Court of Human Rights (ECtHR) announced its judgment in the case of *K.U. v. Finland*, regarding the violation of the right to private life protected under Article 8 of the European Convention of Human Rights (ECHR) in a case where a minor's personal information was placed online without the minor's consent.⁴³ The ECtHR held that Finland was in breach of its obligations under Article 8 of the ECHR, because it did not provide effective criminal sanctions for serious privacy infringements on the Internet or enabling the means of identifying the offenders.⁴⁴

In 2009, the Supreme Administration Court made a ruling according to which the company Satakunnan Markkinapörssi Oy had violated the Personal Data Act by

⁴¹ Summary of the Supreme Administrative Court ruling of 8 January 2010, available in Finnish at <http://www.tietosuoja.fi/49514.htm>.

⁴² ECtHR, *I v. Finland* (20511/03) 17 July 2008, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Finland%20%7C%2020511/03&sessionid=63707926&skin=hudoc-en>

⁴³ "ECHR Rules on Identifying Serious Privacy Infringers," number 6.24, 17 December 2008, available at <http://www.edri.org/edri-gram/number6.24/echr-privacy-ku-finland>. ECtHR, *K.U. v. Finland* (2872/02), 2 December 2008, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=4&portal=hbkm&action=html&highlight=Finland&sessionid=63708122&skin=hudoc-en>

⁴⁴ *Id.*

publishing data concerning the taxation of Finnish citizens in a publication named *Veropörssi*.⁴⁵ (See more details under the "Financial Privacy" section.)

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The powers available to the Finnish law enforcement authorities for the investigation of certain serious crimes are mainly provided for in the Coercive Measures Act passed in 1987.⁴⁶ The Coercive Measures Act contains provisions on telecommunications interception and monitoring, acquisition of identification data showing the location of mobile communications devices, and technical surveillance (technical listening, viewing, and homing⁴⁷). A general condition for the use of these methods is that the information obtained can be assumed to be of great relevance for the investigation of the offence.

A court can give permission to perform electronic surveillance or tap the telephone lines of a suspect ("telemonitoring") and obtain his account information if the suspect is liable to imprisonment for any of the crimes that are exhaustively listed in the Coercive Measures Act.⁴⁸ The latest update to the list was made in June 2010, when suspicion of crimes of, e.g., trafficking and hostage taking, were added to the list of suspected crimes that justified electronic surveillance and telephone tapping.⁴⁹ The conditions for performing coercive measures depend on the measure in question. For example, transactional data of a suspect's telecommunications activity can be obtained if the suspect potentially faces at least four years of imprisonment. Telecommunications monitoring is possible, with the permission of the court, if the suspect is accused of a drug-related crime or a crime that can be punished with more than four years of imprisonment.

The Electronic Communications Act⁵⁰ broadens police access to telecommunications information in criminal cases. In addition to permanent Internet protocol (IP) addresses

⁴⁵ Notice by the Supreme Administrative Court of the ruling of 23 September 2009, available in Finnish at <http://www.kho.fi/47999.htm>.

⁴⁶ Available in Finnish at <http://www.finlex.fi/fi/laki/ajantasa/1987/19870450?search%5Btype%5D=pika&search%5Bpika%5D=pakkokeinolak>.

⁴⁷ The process of determining the location of something, sometimes the source of a transmission, and going to it.

⁴⁸ See Collection of Laws for Electronic Access, World Intellectual Property Organization <http://www.wipo.int/clea/en/fiche.jsp?uid=fi039> (full text not available online).

⁴⁹ Coercive Criminal Investigation Means Act, available at <http://www.finlex.fi/fi/laki/ajantasa/1987/19870450>.

⁵⁰ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 5, § 20.

and telephone numbers, police now have the right to obtain dynamic IP addresses and international mobile equipment identity (IMEI) codes of mobile telephones. The FICORA is responsible for ensuring compliance with the Electronic Communications Act and regulations issued under it, while the DPO monitors the processing of location data and provisions on direct marketing.⁵¹

Data retention

Following minor amendments, the EU approved a Directive⁵² on mandatory data retention in December 2005.⁵³ The Directive requires Internet Service Providers (ISPs) and phone companies to keep data on every electronic message sent and every phone call made for between six months and two years. The directive has been criticised as a threat to the personal privacy of European citizens. Finland originally postponed the entry into force of mandatory retention on the Internet to Spring 2009 at the earliest.⁵⁴ Under the Act on the Protection of Privacy in Electronic Communications,⁵⁵ amended on 1 June 2008⁵⁶ to comply with the Directive, ISPs and phone companies must retain their customers' traffic data for a period of 12 months from the date of the communication. Such data may be used only for the purposes of investigating and resolving crimes, and the consideration of charges for criminal acts referred to in the Coercive Measures Act.⁵⁷ The retention obligation does not apply to the contents of a message or identification data generated through Internet browsing, but only information on, for example, the time and location of certain electronic communications.⁵⁸

National databases for law enforcement and security purposes

In October 1999, the government amended the law and granted the police a new high-tech means of enforcing traffic fines, which in Finland are based on the driver's income. Whereas previously the police would simply ask violators for their income and calculate the fine manually based on that information, they now use cellular phones to access the

⁵¹ Act on the Protection of Privacy in Electronic Communications, (516/2004), Chapter 8, § 31 and § 32.

⁵² See Directive 2006/24/EC, Official Journal of the European Union, 15 March 2006, available at www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf.

⁵³ "Finland: Internet Data Retention to Start in 2009?" eFinland, 28 February 2006, available at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=48378>.

⁵⁴ *Id.*

⁵⁵ Act on the Protection of Privacy in Electronic Communications, 516/2004 (unofficial translation), available at <http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf>.

⁵⁶ Amendment to the Act on the Protection of Privacy in Electronic Communications, 343/2008 (no English translation available), available at <http://www.finlex.fi/fi/laki/alkup/2008/20080343>.

⁵⁷ Chapter 5 a, Section 3, The Coercive Measures Act, available in Finnish at <http://www.finlex.fi/fi/laki/ajantasa/1987/19870450?search%5Btype%5D=pika&search%5Bpika%5D=pakkokeinolaki>.

⁵⁸ Government's bill HE 158/2007, available at <http://www.eduskunta.fi/valtiopaivaasiat/he+158/2007>.

official tax records. Within seconds the driver's reported income appears on the device along with a calculation of the appropriate fine.⁵⁹

National and international data disclosure agreements

Nothing to report under this section.

Cybercrime

Nothing to report under this section.

Critical infrastructure

Nothing to report under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

On 1 September 2009, the Act on Strong Electronic Identification and Electronic Signatures (617/2009) went into effect. The Act revokes the 2003 Act on Electronic Signatures.⁶⁰ The purpose of the Act of 2009 is to create ground-level legislation on strong electronic identification of natural persons and the provision of products and services related to them, as well as to promote data protection and data security of electronic commerce and electronic communications. Further, the purpose of the act is to set "ground rules" for the entities acting in the field of electronic commerce. FICORA has authority to ensure, through monitoring and auditing, that certification service providers that issue qualified certificates comply with the Act.⁶¹ FICORA also issues regulations governing information supplied by certification service providers and handles customer complaints.⁶²

Presently services using strong electronic identification directed at consumers are offered by banks and by the Population Register Centre. The most commonly used strong identification method is the *Tupas-identification* developed by the Federation of Finnish Financial Services (*Pankkiyhdistys*). The main part of all identification transactions made by consumers are located on Internet banks (over 500 million identification annually) or the electronic payment services they offer. Moreover, identification methods utilising the Citizen Certificate and that were developed for the Population Register Centre, are used in a couple of services, but the identification method has not reached the expected level

⁵⁹ Steve Stecklow, "Finnish Drivers Don't Mind Sliding Scale, but Instant Calculation Gets Low Marks," *Wall Street Journal*, 2 January 2001, available at http://www.stayfreemagazine.org/public/wsj_finland.html.

⁶⁰ Act on Strong Electronic Identification and Electronic Signatures (unofficial translation), available at <http://www.finlex.fi/en/laki/kaannokset/2009/en20090617>.

⁶¹ See *Id.*

⁶² Finnish Communications Regulatory Authority, Regulation on Certification Authorities' Obligation to Notify FICORA, 29 January 2003, at <http://www.ficora.fi/attachments/englanti/1156489107542/Files/CurrentFile/FICORA072003M.pdf>.

of popularity: only about 150,000 chip ID cards utilising the Citizen Certificate have been issued thus far and its usage has been further constrained by the small amount of reader devices.⁶³ It is presumed that new service providers will emerge on the market for strong identification in the near future. The mobile certification system, currently being developed by several major mobile phone operators, will presumably fulfil the requirements for strong electronic identification in the future.⁶⁴ The certification authority for the mobile authentication system is the Population Register Centre.

Cybersecurity

On 4 September 2003, the Finnish government submitted a resolution on the National Information Security Strategy. The Strategy aims to increase citizens' and companies' trust in the information society and formulates the efforts of the government, trade, and industry organisations, and private citizens into common information security objectives. The Strategy, one of the first proposals in the world that concerns the development of information security in the whole society, was praised as the best European security guidelines at the International RSA Information Security Conference held in Amsterdam in November, 2003.⁶⁵

In October 2003, the Finnish Ministry of Transport and Communications appointed the National Information Security Advisory Board to oversee implementation of the National Information Security Strategy.⁶⁶ The Board began its work in spring 2004 and continued through May 2007. On 14 December 2004, the Board submitted to the government a progress report that provided an overview of the state of information security in Finland. The report also outlined four primary projects for 2005: adoption of a programme on information-secure electronic services, analysis of national information security risks, assessing and remedying cybercrime, and organising the nation's second annual National Information Security Day, which was held on 8 February 2005.⁶⁷ The Strategy was updated in December 2008 and is entitled "Everyday Security in the Information Society – a Matter of Skills, not of Luck." The Strategy's vision is that people and businesses will

⁶³ "Sähköisen tunnistamisen kehittämisryhmän. 1. väliraportti arjen tietoyhteiskunnan neuvottelukunnalle" (The First Temporary Report of 2008 on the condition of the Development Group of Electronic Identification in Finland to the Information Society Advisory Board), 15 January 2008, available at http://www.arjentietoyhteiskunta.fi/files/36/Sahkoisen_tunnistamisen_nykytila_lopullinen_080115.pdf.

⁶⁴ "Sähköisen Tunnistamisen Kehittämisryhmä. Vahvan Sähköisen Tunnistamisen Kansalliset Linjaukset Suomessa" (The National Policy Definitions of the Development Group of Electronic Identification in 2008), available at http://www.arjentietoyhteiskunta.fi/files/89/Sahkoisen_tunnistamisen_kansalliset_linjaukset_080926_lopullinen.pdf.

⁶⁵ Email from Reijo Aarnio, *supra*, and Timo Poropudas, "Finnish Information Security Strategy Receives an Award," *Mobile Monday*, 5 November 2003, available at <http://www.mobilemonday.net/news/finnish-information-security-strategy-receives-an-award>.

⁶⁶ Ministry of Transport and Communications Finland, Creating a Safer Information Society: National Information Security Advisory Board Report Submitted to the Government on 14 December 2004 17 (2004), available at <http://www.lvm.fi/files/creating%20a%20safer%20information%20society.pdf>.

⁶⁷ *Id.* at 9.

be able to trust that their information is secure when it is processed in information and communications networks and related services. The three priority areas of the Strategy are: 1) basic skills in the ubiquitous information society, 2) information risk management and process reliability, and 3) competitiveness and international network cooperation.⁶⁸

FICORA's Computer Emergency Response Team (CERT-FI) reported in its 2006 annual review that distributing spyware to hacked computers in Finland became common in 2006.⁶⁹ CERT-FI reported that spyware software activities, which can hijack personal data, user identification, passwords, and credit card numbers, were "large-scale and systematic".⁷⁰ The agency reports, however, that it received word of only a few cases where information about Finnish users of electronic services had fallen into the wrong hands.⁷¹ FICORA's CERT-FI reported in its information security review of April 2009, that there had been a few cases reported where access to confidential information of Finnish organisations were accidentally available on Web sites.⁷² After preparing an international survey, they concluded that slip-ups were fairly common worldwide.⁷³ FICORA's CERT-FI's Annual Review of 2009 reported on the computer worm Conficker, which spread to millions of computers in 2009. Also during 2009, a Trojan was reported to interfere with Finnish online banking sessions and make several unauthorised bank transfers. The annual report states further that international information security communities and authorities tightened their cooperation over the course of the year. In addition to dealing with the Conficker worm, that cooperation ensured that certain companies offering malicious content have been shut off from the Internet. The report notes that CERT-FI completed a research on European CERT organisations during 2009. The operation of 11 CERT units was compared in the research. This research was the first of its kind in Europe, and its results were met with international interest. The report notes further that a new Act concerning signals intelligence in Sweden (the Signals Intelligence Act) came into force on 1 December 2009. The Act gives the Swedish National Defence Radio Establishment (*Försvarets Radioanstalt*) the right to perform signals intelligence activities on fixed networks for national defence purposes. But such monitoring also applies to electronic communication traffic going to and passing through Sweden, thereby including Finnish communications. The new Swedish law emphasises telecom operators' responsibility to inform their customers of information security threats targeting services

⁶⁸ The Strategy for 2009-2015, available at <http://www.lvm.fi/web/fi/julkaisu/view/821188>.

⁶⁹ CERTI-FI, "Annual Review 2006", 5 January 2007, available at http://www.cert.fi/attachments/5mfKbZPac/5mW7X6Cdx/Files/CurrentFile/CERT-FI_situation_report_4-2006.pdf.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² CERTI-FI, "Information Security Review 1/2009," 4 March 2009, available at http://www.cert.fi/attachments/tietoturvakatsaukset/5gmoCIS9f/CERT-FI_information_security_review_1-2009.pdf.

⁷³ *Id.*

implemented abroad, but offered to Finnish customers. This notification responsibility is further detailed in the Act on the Protection of Privacy in Electronic Communications.⁷⁴

The Ministry of Finance broadly oversees the coordination of information security for the Finnish Government and for this purpose set up the Government Information Security Management Board "VAHTI" for steering and developing government information security.⁷⁵ On 15 June 2004, VAHTI appointed a working group to develop and prepare propositions to privacy in administration and electronic surveillance. The issues that the working group is dealing with include biometrics, electronic identification, and electronic surveillance. The working group will further consider privacy when dealing with data security and develop cooperation in administration which is related to privacy issues.⁷⁶ In 2009, VAHTI launched a new development programme for preparing the public administration information security during the period 2010 to 2015. In 2010, the development programme will be put into action, coordinated, and supervised by VAHTI. In 2009, VAHTI also issued the first provisional instructions for ICT issues aimed to the public administration, published a report on data security assaults, and supervised the data security instructions regarding local area networks and system development.⁷⁷

Online behavioural marketing and search engine privacy

Nothing to report under this section.

Online social networks and virtual communities

CERT-FI's information security review of July 2010 was focused on security problems in social networks, specifically in Facebook where worms have spread through malicious links or applications (the so-called "likejacking" problem). The malicious link takes the user to a Web site containing program code that hijacks the mouse cursor in the user's browser. Further, in the same information security review, it was reported that a very popular social network site, "Suomi24," had been hacked in April 2010. The hackers managed to steal the Web site's user data: usernames and passwords.⁷⁸

Online youth safety

In August 2005, the Minister of Transport and Communications announced a voluntary scheme asking Finnish ISPs to block a list of Web pages suspected of containing child

⁷⁴ CERT-FI, Annual Review of 2009, available at http://www.cert.fi/attachments/tietoturvakatsaukset/5nd5tTQ00/CERT-FI_annual_review_2009.pdf.

⁷⁵ Ministry of Finance, Information Security and Management by Results, January 2005, available at http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20060320Inform/94247.pdf.

⁷⁶ Email from Reijo Aarnio, *supra*.

⁷⁷ VAHTI, Annual Report 2009, available at http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20100416VAHTIn/name.jsp.

⁷⁸ CERT-FI, "Information Security Review 2/2010," 7 July 2010, available at http://www.cert.fi/attachments/tietoturvakatsaukset/5sdU8rPUt/CERT-FI_information_security_review_2_2010.pdf.

pornography.⁷⁹ Critics have denounced the plan, saying it may be unconstitutional, could block legitimate Web sites, and might not advance its goal of preventing access to child pornography.⁸⁰

Authorised by an Act Against Distribution of Child Pornography, entered into force on 1 January 2007, the Finnish Police Authority is entitled to maintain and update a confidential list of Web sites containing child pornography. ISPs are allowed, not compelled, to censor the child pornography Web sites on the list. The purpose of the law is to prevent access to foreign Web sites that contain child pornography.⁸¹ Upon the Police Authority's discretion, the list can be disclosed to telecommunications companies. A telecommunications company receiving such list has a confidentiality obligation provided by law.⁸²

In May 2009, the Helsinki Administrative Court decided that being added on the list of child pornography Web sites is not an action subject to appeal.⁸³ The case concerned the censorship of a Web site that listed the full censorship list.⁸⁴ By publishing the list, the police determined that the Web site was acting as a "portal" to child pornography content.⁸⁵ However, the Supreme Administrative Court gave a decision in September 2010 repealing the decision and remitting the case to the lower court.⁸⁶

⁷⁹ "Finnish ISPs Must Voluntarily Block Access, EDRI-gram newsletter, number 3.18, 8 September 2005, available at <http://www.edri.org/edri-gram/number3.18/censorshipFinland>.

⁸⁰ *Id.*

⁸¹ Electronic Frontier Finland, "Effi: Finnish Police Censors A Critic of Censorship," 12 February 2008, available at <http://www.effi.org/julkaisut/tiedotteet/lehdistotiedote-2008-02-12-en.html>.

⁸² Act Against Distribution of Child Pornography (1.12.2006/1068), (no English translation available) available at <http://www.finlex.fi/fi/laki/ajantasa/2006/20061068>.

⁸³ "Finland: Complaints Not Allowed For the Police Child-Porn Censorship List," number 7.12, 17 June 2009, available at <http://www.edri.org/edri-gram/number7.12/lapsiporno-trial-finland>.

⁸⁴ *Id.*

⁸⁵ "ENDitorial: Finnish Web Censorship," number 6.4, 27 February 2008, available at <http://www.edri.org/edri-gram/number6.4/finland-web-censorship>.

⁸⁶ At <http://www.kho.fi/paatokset/51802.htm>.

TERRITORIAL PRIVACY

Video surveillance

The Act on the Protection of Privacy in Working Life⁸⁹ contains new regulations on camera surveillance: it is allowed as long as no employee is singled out and employees are informed how and when such monitoring is to be conducted).⁹⁰

Location privacy (GPS, mobile phones, location based services, etc.)

The Electronic Communications Act clarifies rules for processing confidential identification and location data: except in an emergency, telecommunications users aged 15 years or older may not be located without their prior consent.⁸⁹ However, parents or guardians of children under 15 years old may decide on the use of location services, a change in the law that was made in response to a 2003 proposal to allow parents to track the whereabouts of their young children through the use of mobile phones.⁹⁰ Finland's leading mobile operators, TeliaSonera and Elisa, offer such positioning services, which are based on user proximity to base stations.⁹¹ In an emergency situation, positioning is always possible.⁹² The DPO oversees the processing of location data.

In May 2005 the Helsinki District Court handed down suspended sentences to five defendants in a case involving unauthorised use of mobile telephone records by executives of telecommunications service provider Sonera.⁹³ The court found there had been extensive misuse of telecommunications information at Sonera from 1998 to 2001.⁹⁴ The case was appealed, and the Court of Appeals affirmed the sentences in March 2007, also increasing the amount of monetary damages and court costs. The Supreme Court did not grant permission to appeal the case to the Supreme Court making the decision final.⁹⁵ After the scandal, Sonera was merged with Swedish telecommunications operator Telia,

⁸⁸ *Id.*

⁸⁹ Finland Ministry of Transport and Communication, "New Means to Improve Data Protection and Information Security – Act on Data Protection in Electronic Communications to Enter into Force on 1st September," Press release, 16 June 2004, available at <http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=113506>.

⁹⁰ Associated Press, "Finns Ready Cellphone Tracking Law," MSNBC, 17 October 2003, available at <http://msnbc.msn.com/id/3226848/>.

⁹¹ *Id.*

⁹² Finland Ministry of Transport and Communication, "New Means to Improve Data Protection and Information Security – Act on Data Protection in Electronic Communications to Enter into Force on 1st September," Press release, 16 June 2004, available at <http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=113506>.

⁹³ "Five Get suspended Sentences in Sonera Telephone Record Case," *Helsingin Sanomat* International Edition, 30 May 2005, available at <http://www.hs.fi/english/article/1101979719153>.

⁹⁴ *Id.*

⁹⁵ "Court of Appeals Affirms Sentences in Sonera Snooping Case," *Helsingin Sanomat* (International Edition), 16 March 2007, (English translation) available at <http://www.hs.fi/english/article/Court+of+Appeals+affirms+sentences+in+Sonera+snooping+case/1135225870463>.

creating TeliaSonera.⁹⁶ At the time of the scandal, the Finnish state was a majority shareholder in Sonera.⁹⁷ Sonera's security department was suspected of having misused telecommunications logs of at least 100 people, among them journalists, in an attempt to discover who was responsible for information leaks that had been troubling the company.⁹⁸ One journalist commented at the time, "Communications privacy in Finland, as elsewhere, is seen as a sacred right. The strong suspicion that this privacy has been shamelessly violated has prompted talk of an Orwellian society."⁹⁹

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Finland made biometric passports available in 2006¹⁰⁰ by enacting a new Passport Act in July 2006 and amending it in June 2009. The Ministry of the Interior reports that the introduction of biometric passports is a joint project of all EU member states to fight passport fraud and forgery.¹⁰¹ According to the Ministry, biometrics will improve the efficiency of identification and help fight illegal immigration and terrorism.¹⁰² The biometric passports introduced by the Passport Act of 2006 included a microchip that stores a digital facial image, personal data, and passport data on the data page of the passports.¹⁰³ Along with the amendment of the Act in 2009, fingerprints were also added to the biometric passports. The fingerprints constitute a personal data register that authorities suggested be made available for police criminal investigation. The suggestion has been widely criticised in the media due to the risk of misuse.¹⁰⁴

⁹⁶ Kyösti Karvonen, "Finland's Intelligence Service Shaken by SUPOgate," *Virtual Finland*, 23 September 2004, available at <http://www.finland.fi/netcomm/news/showarticle.asp?intNWSAID=28174&intIGID=&intCatID=607&CatTypeNumber=3&LAN=EN&contlan=&Thread=&intThreadPosition=0>.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ Press Release, Ministry of the Interior, "New Biometric Passports to be Introduced on 21 August 2006," 31 May 2006, available at <http://www.intermin.fi/intermin/bulletin.nsf/HeadlinesPublicEng/A4C2738C1289CCF2C225717F00213A38>.

¹⁰¹ *Id.*

¹⁰² "Biometric Passports Possibly in May 2005," eFinland, 9 March 2004, at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=21813>.

¹⁰³ *Id.*

¹⁰⁴ "The Police Wants to Use Passport Fingerprints for Criminal Investigation", Helsingin Sanomat, 21 February 2008, available at <http://www.hs.fi/kotimaa/artikkeli/Poliisi+haluaa+passien+sormenj%C3%A4ljet+rikostutkijoille/1135234251356>.

NATIONAL ID & SMART CARDS

National identification numbers have long been in use in Finland. Since the 1970s, all citizens have been issued a national identification number consisting of their date of birth and four other characters. The number is used extensively in the public and private sectors. It is included on passports, driving licences, and other personal data files held by the public administration.¹⁰⁵ Identity cards are delivered by the Finnish Police, and consist of standard identity cards, minors' ID cards, and temporary ones.¹⁰⁶

The Finnish government in December 1999 began issuing new national ID cards (FINEID) based on smart card technology.¹⁰⁷ A "Citizen Certificate" could originally be incorporated into a chip ID card issued by the police, a bank card or the Subscriber Identity Module (SIM) card of a mobile phone.¹⁰⁸ As of December 2008, that choice is no longer available due to, among other things, a lack of demonstrated interest.¹⁰⁹ This certificate can be used for secure identification in e-transactions, email, and document encryption and as an electronic signature.¹¹⁰ The cards include digital signatures to communicate online with government agencies and companies. The Citizen Certificate can also be used on different platforms and is channel-independent and not bound to the ID Card issued by the Finnish government.¹¹¹ The Finnish Population Register Centre operates as the digital signature certificate authority.

The Identity Card Act was passed in early 1999 to regulate the adoption and use of digital ID cards.¹¹² As of June 2003, cardholders have been able to have their cards imprinted with their social security data. The card can be used as a travel document in EU member states, and about 50 services use the card. The citizen certificate can also be used on different platforms and is channel-independent.

¹⁰⁵ Peter Blume *et al.*, *supra*.

¹⁰⁶ See Finnish Police, "Identity Cards," available at <http://www.poliisi.fi/poliisi/home.nsf/pages/F082D8AB29097DB5C2256C29002BA66C>.

¹⁰⁷ See, Finnish Population Register Centre's homepage <http://www.vaestorekisterikeskus.fi/>.

¹⁰⁸ See Press Release, Population Register Centre, "Finnish Government Employees Get Chip ID Cards," October 5, 2006, available at <http://www.fineid.fi/vrk/bulletin.nsf/fineidbd/A25EC94E8F7395B0C22571FD004232A4?opendocument>.

¹⁰⁹ Finland Population Register Centre, "Cooperation regarding to the mobile Citizen Certificate between Population Register Centre, Elisa Corporation and TeliaSonera Finland Oyj has ceased," available at <http://www.vaestorekisterikeskus.fi/vrk/bulletin.nsf/PFBD/6E1C17B303B6B96CC225753D002CCECB?opendocument>.

¹¹⁰ *Id.*

¹¹¹ Finnish Population Register Centre, "FINEID" Web site: <http://www.fineid.fi/vrk/fineid/home.nsf/pages/4DC96862A6BFA292C2256FFF00379DE9>.

¹¹² The Identity Card Act (28.7.1999/829), (no English translation available) available at <http://www.finlex.fi/fi/laki/ajantasa/1999/19990829>.

Beginning in June 2004, medical insurance data could be put into identification cards on a voluntary basis, thus replacing social security (KELA) cards issued by the Social Security Institution of Finland.¹¹³ As of May 2007, 34,300 people had integrated their health insurance information into their ID cards.¹¹⁴ The Population Register Centre reported in 2006 that chip ID cards are being adopted for Finnish government employees.¹¹⁵ The ID cards contain a Government Employee Certificate that is part of the same Finnish certificate infrastructure as the Citizen Certificates.¹¹⁶ The certificate on the government ID cards enables identification and to log into information networks, to authenticate network users and their usage rights, encrypt email, and use electronic signatures.¹¹⁷

In May 2009 a Finnish ID card was used to register a business in Estonia, without the founders of the company ever having to leave their desks.¹¹⁸ The company is the result of the Estonian e-Commercial Register Portal, opened to Finnish ID cards for the first time in December 2008.¹¹⁹

RFID tags

In late 2002, VTT Technologies, a government research centre, developed a new type of high-frequency (900 MHz) Radio Frequency Identification (RFID) tag that can be read with a transceiver up to four metres away. The signal can also penetrate obstacles. In 2004, the city library of Kauhajoki was the first in Finland to implement RFID technology, which was introduced to help manage collections, cut losses, speed up customer service, and increase self-service. RFID technology is widely used for theft prevention in libraries.¹²⁰

In the Helsinki region, the most familiar application of RFID technology is the green travel cards provided by Helsinki Region Transport. The travel cards are contactless integrated circuit cards, or proximity cards, that are based on the ISO 14443 A

¹¹³ "Social Security Data on Electronic ID Cards," eFinland, 2 June 2004, at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=24579>.

¹¹⁴ Press Release, Population Register Centre, "By the end of May, Citizen Certificates Had Been Issued to a Total of 145,200 People," *supra*.

¹¹⁵ Press Release, Population Register Centre, "Finnish Government Employees Get Chip ID Cards," *supra*.

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ Epractice, "EU: Finnish ID Card Used for the First Time to Create a Company in Estonian e-Commercial Register," 15 May 2009, available at <http://www.epractice.eu/en/news/290131>.

¹¹⁹ *Justiitsministeerium*, "Company Registration Portal Now Open to Finns," 3 December 2008, available at <http://just.ee/39621>.

¹²⁰ "Using RFID in the Libraries," at <http://www.toptunniste.fi/index.php?id=rfid-kirjasto&L=3>.

standard.¹²¹ They replaced paper tickets in the area's public transport system by the end of 2002. Partners in the project were the Helsinki Metropolitan Area Council (YTV), Helsinki City Transport, and the railway company VR. The use of travel cards is recorded in a database. This information can be accessed to aid transport capacity planning. The movements of travel card users are saved and can be accessed for later retrieval. The data from the transport system has been used for crime investigations in serious cases.¹²² YTV records the customer information it needs for customer service and consumer protection in the Travel Card System. Then, YTV municipal service point employees and the people in charge of the system have the right to browse and update the customer data recorded in the system, as well as the data stored in the central processing unit, concerning travel periods and the amount of money a passenger has loaded into his/her card and where the card was last used. It is not possible to browse the travel data at the point of service.¹²³ The travel card received heavy public criticism after its introduction, since it was theoretically possible to connect a specific traveler's identity with travel route information. After the DPO made the issue public, YTV changed its policy.¹²⁴

BODILY PRIVACY

The Act on the Protection of Privacy in Working Life¹²⁵ contains new regulations on camera surveillance and drug testing. Camera surveillance is allowed as long as no employee is singled out and employees are informed how and when such monitoring is to be conducted. Drug testing is widely allowed at work, provided such testing is legally justified, as when the job requires accuracy or the ability to react quickly.¹²⁶

WORKPLACE PRIVACY

On 1 October 2004, the Act on the Protection of Privacy in Working Life took effect.¹²⁷ The Act determines the legality of several privacy issues in the workplace, such as psychological, genetic, and drug tests; the processing of medical histories and health information; and the use of video and audio surveillance devices. The main principle of the Act is that the employer shall collect personal data about the employee primarily from

¹²¹ "Millaiset ovat matkakortin tekniset ominaisuudet?," available at <http://www.hsl.fi/FI/matkustajanopas/faq/Matkakortti/Sivut/Millaisetovatmatkakortinteknisetominaisuudet.aspx>.

¹²² Privacy International, Privacy, Technology, and Europe: A report for Japan's Ministry of Public Management, Home Affairs Postal and Telecommunications 373 (March 2003), available at http://personal.lse.ac.uk/hosein/pets/japan_pets.pdf.

¹²³ *Id.* at 374.

¹²⁴ *Id.* at 374.

¹²⁵ Act on the Protection of Privacy in Working Life (759/2004), available at <http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf>.

¹²⁶ *Id.*

¹²⁷ Act on the Protection of Privacy in Working Life (759/2004), available at <http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf>.

the employee himself. In order to collect personal data from elsewhere, the employer must obtain the employee's consent.¹²⁸ The Act also delineates procedures by which employers may, in their employees' absence, open email messages sent to or from employees' work email addresses.¹²⁹ Previously, the Telecommunications Privacy Act prevented Finnish employers from monitoring the contents of employees' email messages.¹³⁰

The statute also contains new regulations on camera surveillance (allowed as long as no employee is singled out and employees are informed how and when such monitoring is to be conducted) and drug testing (widely allowed at work, provided such testing is legally justified, as when the job requires accuracy or the ability to react quickly).¹³¹

One of the latest amendments to the Act in 2008 concerns the employer's right to receive and process credit status information on the job applicant for evaluating his reliability if the job applied for includes tasks requiring a particular reliability, e.g. tasks relating to making decisions about financial commitments on the employer's behalf.¹³²

In November 2006, the Finnish Data Protection Ombudsman (DPO) ruled that the Act barred employers from researching prospective employees using Internet search engines without the employees' consent.¹³³ Media reports indicate that the "Ombudsman's decision may make life more difficult for Human Resources personnel, as employers may not be permitted to even check the reliability of a job applicant's CV from publicly available sources available through the Internet without first obtaining the applicant's permission."¹³⁴

From June 2009, a new amendment to the Electronic Communications Act, generally known publicly as "*Lex Nokia*",¹³⁵ entered into force. It allows companies and

¹²⁸ Article 4.

¹²⁹ Act on the Protection of Privacy in Working Life, *supra*.

¹³⁰ Peter Blume *et al.*, *supra* at 71.

¹³¹ *Id.*

¹³² Amendment (511/2008), 1 September 2008 to the Act on the Protection of Privacy in Working Life, available at <http://www.finlex.fi/fi/laki/alkup/2008/20080511>.

¹³³ *RoschierRaidla News*, "The Internet and Privacy in the Workplace," November-December 2006, available at http://www.roschier.com/monthlybriefs/RoschierRaidla/December2006/RRnewsletter_December2006.htm.

¹³⁴ *Id.*

¹³⁵ The Act on Protection of Privacy in Electronic Communications (125/2009) (the unofficial translation is available at <http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf>, the main amendment of the Act or *Lex Nokia* was inserted into the Act; precisely, the Act's Chapter 3, new Sections 13a-13h. In addition to the new sections dealing with the corporate's or organisation's right to process data in case of misuse, certain minor adjustments were made to other sections of the Act.

associations ("association subscribers")¹³⁶ who suspect that business secrets are being leaked or that communication networks are being misused, to process "identification data"¹³⁷ in order to prevent such disclosure of business secrets or investigate their potential disclosure,¹³⁸ but under the supervision of the DPO.¹³⁹ Association subscribers may process identification data for producing and consuming services, for invoicing, marketing, and technical developing, detecting a technical defect or error, and for carrying out information security tasks.¹⁴⁰ Association subscribers are not, however, allowed to read the content of employees' messages themselves; the right to process identification data explicitly concerns electronic communications and does not apply to, e.g., telephone and mobile phone communications. During the legislative process, the "*Lex Nokia*" gained an enormous amount of publicity and criticism, critics claiming that it would encourage association subscribers to "snoop" on their employees, and could also be construed to allow snooping on any IP-based telecommunications.¹⁴¹ This amendment was, however, approved by the Parliament and association subscribers may exercise that new right as of 1 June 2009. Before commencing any actions, the association subscriber has to notify the Finnish Data Protection Ombudsman (DPO) (notification is payable).¹⁴² In 2009, the DPO did not receive any notification from association subscribers and as of 2010 none of them had used the right to process identification data as intended in the amendment.¹⁴³ The true added value of that new right therefore remains to be seen in the coming years.

¹³⁶ "Association subscribers" are "companies and associations that process confidential messages, identification data or location data of their users". An "association subscriber" is defined as a company, a cooperative, a university, a governmental agency or an association of almost any kind. DPO, Association Subscribers' Right to Process Identification Data, 1st June 2009, available at http://www.tietosuoja.fi/uploads/luke8tvsw85r2gg_1.pdf.

¹³⁷ "Identification data" is defined as "all information that is possible to combine to a specific user or a subscriber of the communication service at issue, e.g. the time and place of the electronic communication". DPO, Association Subscribers' Right to Process Identification Data, 1st June 2009, available at http://www.tietosuoja.fi/uploads/luke8tvsw85r2gg_1.pdf.

¹³⁸ Act on Protection of Privacy in Electronic Communications (125/2009), Chapter 3, § 13a-13b.

¹³⁹ DPO, Association Subscribers' Right to Process Identification Data, 1st June 2009, available at http://www.tietosuoja.fi/uploads/luke8tvsw85r2gg_1.pdf.

¹⁴⁰ DPO, Guidelines for Processing Identification Data, 4 June 2010, available at http://www.tietosuoja.fi/uploads/pw6n3m6_1.pdf.

¹⁴¹ "Snooping Law, 'Lex Nokia,' Proceeding Slowly but Surely in Finland," EDRI-gram newsletter, number 6. 24 17 December 2008, available at <http://www.edri.org/edri-gram/number6.24/nokia-law-finland-snooping>.

¹⁴² The blank notification form is available (in Finnish) at <http://www.tietosuoja.fi/46872.htm>.

¹⁴³ Government's bill HE 48/2008, available at <http://www.eduskunta.fi/valtiopaivaasiat/he+48/2008>.

HEALTH & GENETIC PRIVACY

Health privacy

Privacy in health care is protected by the Act on the Status and Rights of Patients, which became effective in 1993. Under the Act, health care must be administered in a way that does not violate human dignity and that protects the patient's convictions and privacy. In general, medical records may not be released without the patient's written consent, except when otherwise provided by law.¹⁴⁴ In addition, the Medical Research Act, in force since 1 November 1999, prohibits disclosure of patient information including health status, personal circumstances, or financial situation by medical research workers and ethics committee members.¹⁴⁵

Genetic privacy

Nothing to report under this section.

FINANCIAL PRIVACY

In February 2007, the Supreme Administrative Court agreed that the right of access extends to data on a bank's client's own loan transactions and associated interest rates. The bank had argued that transaction statements and interest rate data are not part of the client data files because the microfilms containing this data are stored separately from the client's data file. However, according to the Court, this view is erroneous because the extent of the personal data file is determined by its use. According to the Personal Data Act, data processed in order to attend to the same task belongs to the same personal data file (logical data file), even though various parts of the data file (sub-registers) are stored separately. Because the purpose of using the interest rate data was the same as for the client's data, both data sets were part of the same data file. Whether it was technically stored together or apart was deemed irrelevant.¹⁴⁶

The demand for instant (quick) loans requested via mobile phone or over the Internet has lately dramatically increased in Finland. In several of the quick loan companies, authentication of the loan applicant is based solely on the social security number given by the applicant and subscription data from the telecommunications company. Inadequate authentication has in some cases led to identity theft. In March 2007 the Data Protection Board (DPB), on request of the Data Protection Ombudsman (DPO), ordered a quick loan company to change their authentication process pertaining to loan applicants. The DPB required that creditors identify their clients in order to ensure the accuracy of any personal data processed. The case proceeded to the Supreme Administrative Court, which

¹⁴⁴ Act on the Status and Rights of Patients (785/1992) Section 12 (30.6.2000/653), 17 August 1992, unofficial translation available at <http://www.finlex.fi/fi/laki/kaannokset/1992/en19920785.pdf>.

¹⁴⁵ Medical Research Act (488/1999), issued 9 April 1999, unofficial translation available at <http://www.finlex.fi/en/laki/kaannokset/1999/en19990488.pdf>.

¹⁴⁶ Supreme Administrative Court ruling (1771/2/05 and 1861/2/05), 27 February 2007, summary, available in Finnish at <http://www.tietosuoja.fi/38751.htm>.

gave its ruling in January 2010 in accordance with the decision of the Data Protection Board.¹⁴⁷

A 2008 amendment to the Act on the Protection of Privacy in Working Life concerns the employer's right to receive and process credit status information on the job applicant for evaluating his reliability if the job applied for includes tasks requiring a particular reliability, e.g. tasks relating to making decisions about financial commitments on the employer's behalf.¹⁴⁸

In 2009, the Supreme Administration Court made a ruling according to which the company Satakunnan Markkinapörssi Oy had violated the Personal Data Act by publishing data concerning the taxation of Finnish citizens in a publication named *Veropörssi*. The company intended to create a service where personal data was processed by ordering taxation information on individual persons by SMS. The Court deemed this particular type of publishing taxation information on private individuals a violation of the Personal Data Act. The ruling does not apply to the publicity of taxation information in general.¹⁴⁹

E-GOVERNMENT & PRIVACY

The Population Register Centre is also working with mobile operators to design a smart card suitable for remote electronic voting. The Ministry of Justice introduced e-voting at polling stations in three municipalities for the 2008 municipal election.¹⁵⁰ It was expected that electronic voting would be available throughout Finland by 2009.¹⁵¹ An electronic ID card or other certification was used with the goal of protecting voter identity.¹⁵² Several organisations are critical of electronic voting, citing increased potential for error and loss of voter confidence in the democratic process.¹⁵³ In June 2008, Electronic Frontier Finland (EFFi) released a shadow report on e-voting that argued that ensuring reliable

¹⁴⁷ Supreme Administrative Court ruling (1568/1/09), 8 January 2010, summary, available in Finnish at <http://www.tietosuoja.fi/49514.htm>.

¹⁴⁸ Amendment (511/2008) of 18 June 2008 to the Act on the Protection of Privacy in Working Life, available in Finnish at <http://www.finlex.fi/fi/laki/alkup/2008/20080511>.

¹⁴⁹ Supreme Administrative Court, ruling of 23 September 2009, press release, available in Finnish at <http://www.kho.fi/47999.htm>. Supreme Administrative Court, decision (2009:82), available in Finnish at <http://www.kho.fi/paatokset/47977.htm>.

¹⁵⁰ Ministry of Justice, "Electronic Voting," available at <http://www.vaalit.fi/42735.htm>.

¹⁵¹ "Finland: Electronic Voting to be Tested in 2007," eFinland, 13 January 2006, available at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=46243>.

¹⁵² "Finland: Electronic Voting To Be Tested in 2007," eFinland, 15 April 2005, at <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=35478>.

¹⁵³ See Press Release, "New Campaign Calls for Safe E-voting," Electronic Frontier Finland, 4 November 2003, available at <http://www.ffi.org/julkaisut/tiedotteet/pressrelease-2003-11-04.html>; "Policy on E-voting and Counting," Electoral Reform Society, available at <http://www.electoral-reform.org.uk/downloads/Electronic%20voting%20POLICY.pdf>.

results would be "extremely difficult."¹⁵⁴ The English translation of the report was released in September of the same year.¹⁵⁵ Effi had asked the Ministry of Justice for information about the e-voting system in February 2008, but was denied access to it the same month due to government concerns over trade secrets.¹⁵⁶

The pilot of the full e-voting system took place in October 2008 in the Finnish elections of three municipalities (namely Karkkila, Kauniainen, and Vihti).¹⁵⁷ In November 2008, the Ministry of Justice announced that 232 votes were prematurely aborted during the launch on account of usability errors in conjunction with unclear instructions.¹⁵⁸ Additionally, many complained of the risk of a breach of voter anonymity due to the electronic ballot box's archival rules.¹⁵⁹ The Helsinki Administrative Court ruled in January 2009 that the election met the requirements of Finnish election law, requesting that municipal authorities confirm the results.¹⁶⁰ The decision went up to the Finnish Supreme Administrative Court, which overturned the lower court's decision, holding that the voter instructions and user interface of the terminals were both flawed.¹⁶¹ The Supreme Administrative Court held that the elections had to be renewed in each of the participating municipalities.¹⁶² New elections were held on 6 September 2009 using the traditional paper voting system.

As a result, the Ministry of Justice prepared a memorandum on the e-voting experiment, compiled with 30 statements from various organisations, political parties, and authorities,¹⁶³ and held a public consultation on the *otakantaa.fi* platform. The cabinet eventually decided not to pursue the development of electronic voting for the time

¹⁵⁴ "Effi's E-voting 'Shadow Report,'" EDRI-gram newsletter, EDRI-gram newsletter, number 6.17, 10 September 2008, available at <http://www.edri.org/edri-gram/number6.17/effi-evoting-report>.

¹⁵⁵ *Id.*

¹⁵⁶ "Finnish E-voting System Must Not Stay A Trade Secret," number 6.3, 13 February 2008, available at <http://www.edri.org/edri-gram/number6.3/finland-e-voting>.

¹⁵⁷ "Finnish E-voting Fiasco: Votes Lost," number 6.21, 5 November 2008, available at <http://www.edri.org/edri-gram/number6.21/finnish-evoting-fiasco>.

¹⁵⁸ *Id.* Some voters did not press the "OK" button before removing their voting card. Consequently, their vote was not registered. The possibility for "losing a vote" was known to the technology services firm, Tieto, but for some reason it did not seem to be relevant at the time of testing the system.

¹⁵⁹ "An Error Margin of 2 Percent In Municipal Elections Ruled Acceptable In Finland," number 7.3, 11 February 2009, available at <http://www.edri.org/edri-gram/number7.3/evoting-finland-2percent>.

¹⁶⁰ *Id.*

¹⁶¹ "Finnish E-voting Results Annulled By the Supreme Administrative Court," number 7.8, 22 April 2009, available at <http://www.edri.org/edri-gram/number7.8/evoting-fannulled-finland>.

¹⁶² The Supreme Administrative Court's decision 2009:39 (only in Finnish), available at <http://www.kho.fi/paatokset/46372.htm>.

¹⁶³ "Memorandum on the E-Voting Experiment," 30 September 2009, in Finnish, available at <http://www.vaalit.fi/uploads/bwwbit.pdf>.

being.¹⁶⁴ It was also agreed that close attention would be paid to the development of electronic voting in other countries.

OPEN GOVERNMENT

The Act on the Openness of Government Activities replaced the Publicity of Official Documents Act of 1951.¹⁶⁵ It provides for a general right to access any document created, sent, or received by a government agency, including electronic records. Finland is a country that has traditionally adhered to the Nordic tradition of open access to government files. In fact, the world's first Freedom of Information act dates back as far as the Riksdag's (Swedish Parliament) 1766 Access to Public Records Act. This Act also applied to Finland, then a Swedish-governed territory.¹⁶⁶

The Act, most of which came into force in December 1999, also contains provisions on privacy.¹⁶⁷ Chapter 6 of the Act exempts from public disclosure government documents containing data on the annual income or net worth of a person, documents containing information on a secret telephone number or information on the location of a mobile communications device, and documents revealing a person's place of residence, telephone number, or other contact information if the person has asked that the information be kept secret and is justified in believing that disclosure would endanger himself or his family.¹⁶⁸ The latest amendments to the Act tighten the confidentiality of governmental documents, including the criminal and penalty records and the documents relating to election funding of Parliament candidates.¹⁶⁹

OTHER RECENT FACTUAL DEVELOPMENTS (WITH AN IMPACT ON PRIVACY)

In December 2008, the Finnish Science and Technology Policy Council, which became the Research and Innovation Council at the beginning of 2009, adopted the "Review 2008," which outlines policy on education, science, technology, and innovation.¹⁷⁰

¹⁶⁴ "Electronic Voting Will not Be Developed Further on the Current Basis," Finnish Government Press release 13/2010, 20 January 2010. Available at <http://www.valtionuuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=285753>.

¹⁶⁵ Act 83/9/2/1951.

¹⁶⁶ Wayne Madsen, *Handbook of Personal Data Protection* (Stockton Press 1992).

¹⁶⁷ Act on the Openness of Government Activities (621/1999), available at <http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf>.

¹⁶⁸ *Id.*

¹⁶⁹ Amendments dated 24 April 2009 and 14 May 2010 to the Act on the Openness of Government Activities (621/1999), available at <http://www.finlex.fi/fi/laki/alkup/2009/20090274> and <http://www.finlex.fi/fi/laki/alkup/2010/20100374>.

¹⁷⁰ Press Release, Government Communications Unit, "Science and Technology Policy Council Outlined Education, Science, Technology, and Innovation Policies for the Near Future," 12 September 2008, available at http://www.research.fi/en/what_s_new/stpc2008.

On 28 January 2009, Finland celebrated Data Protection Day with a theme of "Raising Awareness," focused on finding ways to improve citizen awareness of data protection issues.¹⁷¹

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Nothing to report.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Finland is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹⁷² Finland has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁷³ Finland signed the CoE Convention on Cybercrime in November 2001.¹⁷⁴ Finland ratified the convention on 24 May 2007, and went into force on 1 September 2007.¹⁷⁵ Finland is also a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

¹⁷¹ Electronic Frontier Finland, "Data Protection Day Seminar on 28 January 2009," 14 January 2009, available at http://www EFFI.org/tapahtumat/tietosuojaivaan_seminaari_20090128_english.html.

¹⁷² Signed April 10, 1991; ratified December 2, 1991; entered into force April 1, 1992.

¹⁷³ Signed 5 May 1989; ratified 10 May 1990; entered into force 10 May 1990; See also Finland Ministry of Foreign Affairs, Government Report to Parliament on the Human Rights Policy of Finland 2004, May, 2004, available at <http://formin.finland.fi/Public/download.aspx?ID=14259&GUID={D110454F-6D31-45EA-8610-84C1A292CD42}>.

¹⁷⁴ Convention on Cybercrime CETS No. 185

¹⁷⁵ *Id.*

FRENCH REPUBLIC¹

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The right of privacy is not explicitly included in the French Constitution of 1958. The Constitutional Council ruled in 1995 that the right of privacy was implicit in the Constitution,² and confirmed this in 1999, by stating that the freedom proclaimed in Article 2 of the 1789 Declaration of the Rights of Man and the Citizen ("*Déclaration des droits de l'homme et du citoyen de 1789*") implies the respect of privacy.³

The Legislative Committee of the Senate issued on 3 June 2009 a report on the right to privacy in the digital age ("*La vie privée à l'heure des mémoires numériques*").⁴ Among the 15 recommendations made in the report to better guarantee privacy against digital threats, one is to include the right to privacy in the French Constitution."⁵ Neither the President of the French Republic nor the Members of Parliament, who have the initiative of a revision of the Constitution under its Article 89, have followed up on this

¹ The EPHR 2010 "France" report has been updated by Pascale Gelly and Caroline Doulcet, Cabinet Gelly (Paris, France).

² Décision 94-352DC du Conseil constitutionnel du 18 Janvier 1995, available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html> (in French).

³ Décision 99-416DC du Conseil constitutionnel du 23 juillet 1999, available at <http://www.conseil-constitutionnel.fr/decision/1999/99416/index.htm> (in French).

⁴ The report is available at <http://www.senat.fr/rap/r08-441/r08-441.html> (in French).

⁵ "French Senate Issues report on Right to Privacy in the Digital Age," Privacy and Information Security Law Blog, Hunton & Williams, LLP, 11 June 2009, available at <http://www.huntonprivacyblog.com/2009/06/articles/european-union-1/french-senate-issues-report-on-right-to-privacy-in-the-digital-age/>.

recommendation.⁶ The CNIL's President confirmed on 10 June 2009⁷ that it is unlikely that the constitution will be modified in the coming years for this purpose.⁸

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The tort of privacy was first recognised in France as far back as 1858⁹ and was added to the Civil Code in 1970.¹⁰

The Data Protection Act, enacted in 1978 and amended in 2004, covers personal information held by government agencies and private entities.¹¹ It is supplemented by a Decree adopted in 2005 and amended on 25 March 2007.¹² These rules provide that any individual must be informed of the reasons for the collection of information and may object to its processing either before or after it is collected. Individuals have the right to access information being kept about them and to demand the correction and, in some cases, the deletion of this data. Fines and imprisonment can be imposed for violations.

⁶ Indeed, a Commission, created in April 2008 at the request of the French President, taking into consideration the fact that the right to privacy is already recognised under French law, failed to consider that the inclusion of the right to privacy in the Constitution would significantly enhance individuals' rights, in spite of the new technical challenges faced by society.

⁷ Speech of Alex Türk at the 5th Assembly of the Correspondents of the AFCDP (French Association of Privacy Correspondents) on 10 June 2009 in Paris.

⁸ In 2008, during the annual report press conference of the Commission nationale de l'informatique et des libertés, Alex Türk, CNIL's President, had indicated his strong wish to introduce data protection rights in the preamble of the French Constitution, as it is the case in 13 of the 27 European Union Member States. Mr. Türk had justified this proposal by the "worrying generalisation of mechanisms tracking individuals" every move from wake-up until bedtime. ("La CNIL veut inscrire dans la Constitution la protection des données personnelles," *Le Monde*, 16 May 2008, available at http://www.lemonde.fr/societe/article/2008/05/16/la-cnil-veut-inscrire-dans-la-constitution-la-protection-des-donnees-personnelles_1046127_3224.html). It has been his credo since then, and he was partly supported by the Legislative Committee of the Senate in its 3 June 2009 report.

⁹ The Rachel affaire. Judgment of 16 June 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

¹⁰ Civil Code, Article 9, Statute No. 70-643 of 17 July 1970.

¹¹ Loi n° 78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés, available at <http://www.cnil.fr/index.php?id=301> in French; available in English at <http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>.

¹² Décret n° 2007-451 du 25 mars 2007 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris en application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000824352&dateTexte=>.

It is worth noting that the Data Protection Act does not apply to data controllers outside the European Community who do not use data processing means in France.¹³

Sector-based laws

There are additional specific laws which relate to the protection of data such as laws on administrative documents,¹⁴ archives,¹⁵ video surveillance,¹⁶ employment,¹⁷ and consumer protection.¹⁸ There are also protections incorporated in the Penal Code.¹⁹

DATA PROTECTION AUTHORITY

The data protection authority is the *Commission nationale de l'informatique et des libertés* (CNIL), an independent agency that interprets and enforces the Data Protection Act.²⁰ The Commission takes complaints, issues rulings, sets rules, conducts audits, makes reports, and ensures public access to information by being a registrar of data controllers' processing activities. In addition, the 2004 amendments to the Data Protection

¹³ A user of Google Groups services such as Usenet discussion, who sued Google Inc. USA, learnt this to her detriment: she did not obtain the removal of her contributions dating back to 1998 that were still available through searches using Google tools. The Court of first instance, in an emergency proceeding, concluded that the applicable law was the law of the State of California, where the messages were archived. It took into consideration the fact that California's Constitution provides protection of privacy in its Section 1.1. Tribunal de Grande Instance de Paris, Ordonnance de refere, 14 April 2008, available in French at <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20080414.pdf>.

¹⁴ Loi No. 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (Journal officiel, 18 July 1978, at 2851), available at <http://www.cnil.fr/textes/text05.htm> (in French).

¹⁵ Loi No. 79-18 du 3 janvier 1979 sur les archives (Journal officiel, 5 January 1979, at 43, erratum at Journal officiel, 6 January 1979, at 55) (in French).

¹⁶ Loi d'orientation et de programmation n° 95-73 du 21 janvier 1995 relative à la sécurité (Journal officiel, 24 January 1995, at 1249), available at <http://www.cnil.fr/textes/text054.htm>; see also Décret n° 96-926 du 17 octobre 1996 relatif à la vidéo-surveillance pris pour l'application de l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (Journal officiel, 20 October 1996, at 15432), available at <http://www.cnil.fr/textes/text055.htm>, and Circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (décret sur la vidéosurveillance) (Journal officiel, 7 December 1996, at 17835), available at <http://www.cnil.fr/textes/text056.htm> (in French).

¹⁷ Articles L.2323-13, L.2323-14 and L4612-9 of the Labor Code. <http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006901943&idSectionTA=LEGISCTA000006198568&cidTexte=LEGITEXT000006072050&dateTexte=20101215> and <http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006903309&idSectionTA=LEGISCTA000006189745&cidTexte=LEGITEXT000006072050&dateTexte=20101215>.

¹⁸ Article L 34-5 of the Post and Electronic Communications Code. At <http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006465787&cidTexte=LEGITEXT000006070987&dateTexte=20101215&oldAction=rechCodeArticle>

¹⁹ Articles L 226-16 and following of the Penal Code.

²⁰ Commission nationale de l'informatique et des libertés Homepage, available at <http://www.cnil.fr>.

Act allow the CNIL to investigate data processes, issue warnings, order data processing to stop, and impose sanctions (fines of up to €150,000). In 2006 the CNIL issued its first financial sanction against the bank Crédit Lyonnais (€45,000) for violating its customers' right of access to their personal data.²¹ The highest published sanction ordered so far is €75,000.

The CNIL has more limited powers over large government information systems known as "sovereignty files".²² Sovereignty file systems, defined to include files relating to the safety of the State, defence, public security, or penal repression, or those that use the NIR (social security number), do not require CNIL approval but mere prior advice.

In 2009, the CNIL received 68,185 new notifications of data processing, leading to a total amount of 1,356,579 files notified since 1978.²³ The Authority received 4,265 complaints and issued 719 decisions including 91 cease-and-desist orders, five financial sanctions, and four warnings. The CNIL also carried out 270 onsite investigations.

Key issues addressed by the CNIL in 2009 were the investigation of a police database called "STIC", targeted online advertising, social networks and the right to be forgotten, online voting, and immigration records.

The CNIL declared that onsite investigations (that are *a posteriori* controls) will remain a priority. It suffered a setback in its strategy with two decisions of the *Conseil d'Etat* (of 6 November 2009)²⁴ that cancelled sanctions the CNIL had ordered against two companies following onsite investigations. The Conseil considered that the CNIL ought to remind the data controller, prior to the investigation, of its right to object to the investigation. In case of an objection, the investigation occurs under the control of the President of the court, as that is part of due process. As a result of this decision, the CNIL modified its practices. It is also seeking a change of the Data Protection Act to create the possibility of obtaining prior authorisation from the judge in certain circumstances. From a procedural standpoint, it is worth stressing that the CNIL, as it has the power to issue sanctions, has been characterised by the Conseil d'Etat²⁵ as being like a tribunal in the meaning of the

²¹ See "Première sanction pécuniaire prononcée par la CNIL," 9 September 2006, available at <http://www.cnil.fr/index.php?id=2104>.

²² Stéphane Foucart, "Les pouvoirs de la CNIL devraient être considérablement amoindris," *Le Monde*, 14 July 2004, available at http://www.lemonde.fr/cgibin/ACHATS/acheter.cgi?offre=ARCHIVES&type_item=ART_ARCH_30J&objet_id=861279, and "La nouvelle loi Informatique et libertés autorise le fichage des internautes," *Le Monde*, 17 July 2004, available at http://www.lemonde.fr/cgibin/ACHATS/acheter.cgi?offre=ARCHIVES&type_item=ART_ARCH_30J&objet_id=861631.

²³ CNIL, 30e Rapport d'Activité 2009 (2010), available in French at http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf.

²⁴ Conseil d'Etat (<http://www.conseil-etat.fr>), decision n° 304301, 6 November 2009, available in French at <http://arianeinternet.conseil-etat.fr/arianeinternet/getdoc.asp?id=91269&fonds=DCE&item=1>.

²⁵ Conseil d'Etat, Ordonnance de référé, 19 February 2008, req. n° 311974, available in French at <http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000018573269&fastReqId=286707310&fastPos=1>.

Article 6-1 of the Convention for the Protection of Human Rights and Fundamental Freedoms. As a consequence, the sanction procedure must comply with the rights of fair trial and due process.

In June 2010, the CNIL opened a new service on its Web site to provide Internet users with the possibility of filing claims online for non-compliance with their rights of access and objection to direct marketing.²⁶

The Authority is also preparing to issue data protection seals in the first half of 2011 to data protection training and audits and to expand this scope at a later stage. Under the Data Protection Act, a company sponsored by a professional association or an institution can submit to the Authority a product or process that it believes is compliant with the data protection principles to obtain a data protection seal (*label*).²⁷

At the 31st International Conference of Data Protection Commissioners, the CNIL voted along with almost 80 other data protection authorities a resolution ("The Madrid Resolution")²⁸ in order to adopt international standards for the protection of personal data and privacy.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In April 2008, a Paris Tribunal condemned different French Web sites for linking to another Web site containing gossip information on the French actor Olivier Martinez. Although the site allowed users to enter links and rate news, the court decided that the Web site owner had an editorial responsibility and awarded damages for infringing the actor's privacy. Another site posted a link to Yahoo!-based news on the same topic and faced a similar outcome.²⁹

On 13 April 2010 Facebook was ordered by the Court of first instance of Paris to remove the photograph of an individual that had been posted on the social network without his

²⁶ CNIL, "Plainte en ligne?" <http://www.cnil.fr/vos-libertes/plainte-en-ligne/>.

²⁷ CNIL, "2011 : Objectif labellisation !", 17 May 2010 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/2011-objectif-labellisation/>.

²⁸ International Standards on the Protection of Personal Data and Privacy – "The Madrid Resolution", 5 November 2009, available at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

²⁹ EDRI-gram, Number 6.7, April 2008, "Linking Can Be Damaging to Your Pockets," available at <http://www.edri.org/edriagram/number6.7/linking-decision-france>. See also 01Net, "A Wave of Condemnations Shakes the French Web 2.0" 27 March 2008, available at <http://www.01net.com/editorial/375750/une-vague-de-condamnations-eban> (in French). See also *Presse Citron*, "Case Olivier Martinez vs. Fuzz : Fuzz condemned," 27 March 2008, available at <http://www.presse-citron.net/?2008/03/27/3217-affaire-olivier-martinez>. See also *Presse Citron*, Parts of the Court decision, available at <http://www.presse-citron.net/?2008/03/28/3221-extraits-de-l-ordonnance> (in French). See also *Vivre en Normandie*, "The French web passes through black hours," March 2008, <http://www.vivre-en-normandie.com/blog/2008/03/le-web-franais.html> (in French).

consent.³⁰ Facebook users had created a group called "Running naked in the church after the bishop" on which several insulting and hateful comments had been posted. The bishop had asked Facebook several times without success to remove his photograph. Facebook submitted that it was not the publisher of the photograph but a mere host and therefore had no responsibility. The Court decided otherwise.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Electronic surveillance is regulated by a 1991 law that requires the permission of an investigating judge before a wiretap is installed. The duration of the tap is limited to four months and can be renewed.³¹ The law created a national commission controlling security wiretaps (*Commission nationale de contrôle des interceptions de sécurité*, or CNCIS), which sets rules and reviews wiretaps each year. In 2006, law enforcement conducted 5,985 interceptions (4,176 new interceptions and 1,809 renewals). This represents a 3.5 percent increase over 2005. There was a 15 percent decrease in 2006 in emergency interception requests (714 requests compared to 854 in 2005).³²

On 27 May 2009, Michèle Alliot-Marie presented the draft law on orientation and programming for the performance of security (LOPPSI 2) to the Council of Ministers.³³ The law allows the Criminal Investigation Police to physically or remotely install spying software on a suspect's computer to listen to electronic communications, gain access to all the data in a computer in real time, and introduces Internet filtering by administrative decision.³⁴ "The law also obliges ISPs to block access, 'without delay', to sites included on a list drafted under the authority of the Ministry of Internal Affairs."³⁵ The law will initially focus on curtailing child pornography.³⁶ ISPs that do not adhere to the law will

³⁰ "Tribunal de grande instance de Paris Ordonnance de référé 13 avril 2010 Hervé G. / Facebook France," available at http://legalis.net/breves-article.php?id_article=2898 (in French).

³¹ Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006077780&dateTexte=20090623> (in French).

³² Commission nationale de contrôle des interceptions de sécurité - 15ème rapport d'activité 2006, 21 mars 2007, available at <http://www.ladocumentationfrancaise.fr/rapports-publics/074000237/index.shtml> (in French).

³³ EDRI-gram, Number 7.11, 3 June 2009, "The French Government Wants to Spy on Electronic Communications," available at <http://www.edri.org/edri-gram/number7.11/france-law-on-spying>.

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

be fined up to €75,000 and a year in jail.³⁷ LOPPSI 2 was adopted by the National Assembly in February 2010 and its last version was submitted to the Senate in June 2010.³⁸ It provides the possibility for the police, in preliminary investigations relating to organised criminality, to remotely access, record, collect, and transfer any information or personal data stored in IT systems without the awareness of the individuals concerned. The sole exceptions are law firms, the media, and court officers, physicians, bailiffs, and notaries.

The CNIL, in its opinion of 6 May 2010, pointed out that the possibility, provided by the draft law, to implement such systems also in public areas, such as cybercafés, is dangerous for privacy. The CNIL insisted that the use of such systems should remain an exception and be supervised.

National security legislation

A new Anti-Terror Act was enacted on 23 January 2006.³⁹ It grants increased powers to the police and intelligence services, allowing them to get telecom data directly from ISPs.⁴⁰ It also extends telecom data retention possibilities, by assimilating cybercafé owners and WiFi providers (whether for free or with payment) such as bars, restaurants, and hotels to telecom operators. Any logged data may be seized directly by the police without any judicial order, "in order to prevent acts of terrorism." It extends the use of video surveillance, authorising private parties to install CCTV cameras in public places "likely to be exposed to terrorist acts" and in places open to the public when they are "particularly exposed to risks of aggression or theft." In case of emergency, CCTV cameras may be installed prior to any authorisation. Furthermore, the Act allows the police to automatically monitor cars on French roads and highways, taking pictures of licence plates and people in the cars, with various purposes ranging from the fight against terrorism to the identification of stolen cars.⁴¹ The same article provides for the monitoring of street gatherings during "big events." Finally, the Act provides that the Ministry of the Interior may process PNR (passenger name record) data collected on any travel by air, sea, or rail to or from non-EU countries.⁴² This article's objective is "to improve border controls and to fight against illegal immigration".⁴³

³⁷ *Id.*

³⁸ Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

³⁹ Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, available at <http://www.senat.fr/apleg/pjl05-109.html>.

⁴⁰ *Id.* at art.6.

⁴¹ *Id.* at art. 8.

⁴² *Id.* at art. 7.

⁴³ See generally EDRI-gram No. 4.2, February 2006, "French Anti-Terrorism Law Not Anti-Constitutional," available at <http://www.edri.org/edrigram/number4.2/frenchlaw>.

Data retention

The Daily Safety Law (LSQ) requires Internet Service Providers (ISPs) to store log files on all their customers' activities for up to one year. Electronic communication operators are subject to the legal obligation to retain traffic data of clients for one year for the purposes of research and prosecution of criminal offenses or breaches of authors' intellectual property rights, and allowing access to such data by judicial authorities.⁴⁴

In addition to the LSQ, the Law on Trust in the Digital Economy (LEN, or "*Loi pour la confiance dans l'économie numérique*") also provides for data retention. The concerned data are personally identifying information (including name, address, and log data). ISPs (host and access providers) are required to collect and keep identification and log data of their subscribers. These data are covered as a "professional secret", so that they may only be disclosed upon judicial request. The law also requires people wishing to post content on the Internet to identify themselves, either to the public by publishing their name and address on their Web site (in the case of a business), or to their host provider (in the case of a private individual). The duration of retention by ISPs and telecommunication providers of identification and log data of subscribers for purposes of investigation, prosecution, and determination of criminal offences has been specified in a Decree of 24 March 2006.⁴⁵ This duration was set at one year from the recording of the identification and log data.

Soon after the adoption of the Anti-Terror Act,⁴⁶ in March 2006, the long-awaited application decree regarding the data retention provisions of the LSQ, adopted in November 2001, was published – almost five years after their so-called emergency introduction.⁴⁷ This decree also provides for application measures of some articles of the Anti-Terror Act. It determines the duration of data retention by telecom operators, setting it to the maximum time allowed (one year) and the type of data to be retained (all kinds of data involved in a telephone or Internet communication, except its content) by the LSQ.

These provisions may be extended in the future with a new decree, the draft version of which was published in April 2007 by the French digital rights NGO IRIS. The draft would require webmasters, hosting companies, fixed and mobile telephony operators, and

⁴⁴ Articles L 34-1 and L34-1-1 of the Post and Electronic Communications Code. Decree n° 2006-358 of 24 March 2006.

⁴⁵ At http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=6A2770A08970ED1638D37F4F77195FF8.tpdjo02v_1?cidTexte=JORFTEXT000000637071&categorieLien=id.

⁴⁶ Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, *supra*.

⁴⁷ Décret n°2006-358 du 24 mars 2006, relatif à la conservation des données des communications électroniques, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSD0630025D>; see also EDRI-gram No. 4.6, March 2006, "Telecom Data To Be Retained For One Year In France," available at <http://www.edri.org/edriagram/number4.6/franceretention>.

Internet service providers to retain all information on Internet users and telephone subscribers and to deliver it to the police or the State at a simple request. It would even require retaining the passwords supplied when subscribing to a telephone service or an Internet account or payment details such as amount, date, or type. The draft text establishes that the data retained by ISPs and hosting companies and obtained by the police can be kept by the latter for a period of three years in the automatic processing systems provided by the Ministry of Interior and the Ministry of Defense. Civil liberties organisations, ISP associations, and major content provider organisations strongly opposed the provisions of this draft decree.⁴⁸

A major French daily newspaper revealed in June 2006 that the police and intelligence services had set up their own technical platform allowing them to easily collect traffic data related to text messages, mobiles, or the Internet. Security services are now in the position of knowing who has contacted whom, when, and where and, by a simple click, they can obtain from the telephone operators the list of all calls from and to a subscriber. They can obtain the subscription documents of the respective person with address and bank information and can also require all the Internet sites or forum addresses the respective person has accessed. The March 2006 Anti-Terror Act makes this platform lawful.⁴⁹

It results from the draft law dated from 27 May 2009 (*Projet de loi d'orientation et de programmation pour la performance* (LOPPSI 2)), submitted to the Senate in June 2010,⁵⁰ that personal data collected by the police for the analysis of the operating methods of authors of serial offences, could be kept for an indefinite period of time. The law indeed provides that the data shall be deleted at the end of the investigation, or no later than three years from the last operation of updating the data, which means that each time the file is updated, the data can be kept three more years. The CNIL felt the need to remind, in its opinion on LOPPSI 2 of 6 May 2010,⁵¹ that personal data should be kept for a limited period of time, to be determined in light of the purpose of the processing.

⁴⁸ Projet de décret portant application de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (document de travail version de janvier 2007), available at <http://www.iris.sgdg.org/actions/len/ProjetDecretLCEN0107.pdf>; see also EDRI-gram No. 5.8, April 2007, "French Government Decree On Data Retention - Another Big Brother Act," available at <http://www.edri.org/edriagram/number5.8/france-data-retention>.

⁴⁹ *Le Figaro*, 28/05/07, available at http://www.lefigaro.fr/france/20070528.WWW000000165_lantiterrorisme_espionne_aussi_mails_et_textos.html; see also EDRI-gram No. 5.11, June 2007, "The French Ministry of Interior has a new interception platform," available at <http://www.edri.org/edriagram/number5.11/french-interior-interception>.

⁵⁰ Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

⁵¹ CNIL, "L'enregistrement des conversations téléphoniques sur le lieu de travail", <http://www.cnil.fr/la-cnil/actu-cnil/article/article/12/les-observations-de-la-cnil-sur-les-nouvelles-dispositions-de-la-loppsi/>.

In its report dated 6 May 2010,⁵² the CNIL voiced its concerns about the extension of the scope of data matching by police of distinct databases of computerised files of individuals' judicial proceedings. This data matching is the result of the LOPPSI 2 draft, submitted to the Senate in June 2010.⁵³ Initially limited to serious serial criminals, such data processing may now be extended to authors of offences punished by a minimum sanction of five years of imprisonment.

National databases for law enforcement and security purposes

Between 1987 and 2010 the number of national computerised files created for law enforcement and security purposes increased continuously.

One of the first databases was the National computerised file of digital fingerprints (*Fichier automatisé des empreintes digitales*,⁵⁴ or FAED), created in 1987. It is used by the judicial police for the identification of authors of criminal offences. In January 2010, the CNIL noted that this file recorded more than 3 millions of identified people (the entire population of France is over 64 million).⁵⁵

Then the National computerised file of genetic data (*Fichier national automatisé des empreintes génétiques*, or FNAEG), was created in 1998. At its creation, the FNAEG was restricted to genetic data of individuals who were condemned for serious sexual crimes, like rape and child abuse. After successive extensions of its use, it can now contain genetic data of individuals simply suspected (but not yet condemned) of infractions related to prejudice against property or people. The Internal Safety Law⁵⁶ (*Loi pour la sécurité intérieure*) promulgated on 18 March 2003, has extended the list of infractions leading to the creation of a record in the FNAEG, as well as the list of individuals whose genetic data may be kept in the FNAEG or compared to its content. While the CNIL has obtained a few minor improvements to this regime after its opinion of 16 April 2009 (e.g., the maximum duration of data retention limited to 25 years instead of 40), the FNAEG remains a significant concern in France.

During 2006 the use of FNAEG reached an unprecedented level. Following the 2005 and 2006 protests that took place in various urban neighborhoods throughout France, many individuals were compelled to register their information in the FNAEG, effectively

⁵² CNIL, *supra* at 51.

⁵³ Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

⁵⁴ CNIL, "Les collectivités locales et la protection des données personnelles", <http://www.cnil.fr/dossiers/police-justice/les-grands-fichiers/article/34/fichier-automatise-des-empreintes-digitales/>.

⁵⁵ CNIL, *supra* at 54.@@

⁵⁶ Loi No. 2003-239 du 18 mars 2003, Loi pour la sécurité intérieure, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0200145L> (in French).

expanding the database to include a register of "civil disobedience."⁵⁷ Police decided who would be registered, and there was no judicial process authorising the selection. Failure to oblige with the request carries a penalty of up to €15,000 and up to one year in prison.⁵⁸

Another national file has been added to the many files already in place, with the adoption in March 2004 of the "Perben II Law"⁵⁹ (*loi portant adaptation de la justice aux évolutions de la criminalité*).⁶⁰ It creates the National judicial computerised record system of sexual offenders (*Fichier judiciaire national automatisé des auteurs d'infractions sexuelles*, or FNAIS). This file records, for up to 30 years, the identity and addresses of individuals (including minors) who have committed all kinds of sexual offences, except exhibitionism and sexual harassment. The records system can only be consulted by judicial authorities and specific government agencies.

The Ministry of Education set up as an experiment in 2004 the "*Base-élèves*," a database containing personal data on children, their families, including psychosocial data and information on competence, skills, and problems. Although initially accessed by educators and social actors, the new French law of March 2007 for the prevention of delinquency granted access to such information to Mayors for the purpose of preventing delinquency. However, after important protests, data related to citizenship, language, and culture of origin were removed in October 2007. Protests to suppress this file have increased and national petitions have been launched.⁶¹ The Conseil d'Etat, the highest administrative jurisdiction, held in two decisions of 19 July 2010⁶² that the "*Base-élèves*" and the computerised file of student identifiers ("*Base nationale des identifiants des élèves*," or BNIE) were not functioning in compliance with the Data Protection Act. Indeed, the Conseil d'Etat considered that the collection of health data in the "*Base-élèves*" relating to children was not relevant. The Conseil d'Etat reminded in its decisions that parents have a right to object to the collection and processing of their children's data.

⁵⁷ "Les insoumis du fichier génétique," dossier de candidature au Prix Voltaire des Big Brother Awards France, available at <http://bigbrotherawards.eu.org/Les-insoumis-du-fichier-genetique-FNAEG.html>; see also L'association "Refus ADN," <http://refusadn.free.fr>.

⁵⁸ "Prélèvements de salive : le front du refus s'organise", Le Figaro, 16 May 2007, available at http://www.lefigaro.fr/france/20070516.FIG000000039_prelevements_de_salive_le_front_du_refus_s_organise.html.

⁵⁹ Called "Perben II" after the name of the French Minister of Justice, Dominique Perben.

⁶⁰ Loi No. 2004-204 du 9 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995&dateTexte=> (in French).

⁶¹ EDRI-gram, No. 6.2, January 2008, "Key Privacy Concerns in France," available at <http://www.edri.org/edriagram/number6.2/privacy-france-2007> ; see also Web site detailing all the protests against this database <http://www.ldh-toulon.net/spip.php?rubrique141> (in French).

⁶² Conseil d'Etat, "Education nationale : fichiers 'Base élèves 1er degré' et 'BNIE'", <http://www.conseil-etat.fr/cde/node.php?articleid=2099>.

It also held that the retention period of 35 years for the children identifiers contained in the BNIE was excessive.

The ELOI file, a database aimed at facilitating the expulsion of illegal migrants, created initially by a ministerial order of 30 July 2006, has been invalidated twice by the Conseil d'Etat, the highest administrative court. On 13 March 2007, the Conseil d'Etat cancelled the ministerial order ("*Arrêté*") allowing the Interior Ministry to create the ELOI file. While the database creation itself was allowed by the French code on immigration and asylum, NGOs argued that the ELOI file would contain excessive and inadequate personal data on foreigners, their children, the citizens with whom they were staying, and, for those in retention centers, their visitors. Moreover, this data would be kept for an excessive duration. The law further introduced DNA testing to prove family links for foreign candidates applying for a visa for longer than three months on family regrouping grounds. Beneficiaries of financial support were to have their photograph and digital fingerprints taken and stored in yet another biometric database.⁶³ The Conseil d'Etat's order was based on a procedural issue and did not address privacy concerns. As a result, the French Ministry of Interior announced the next day that it planned to submit a new draft text.⁶⁴ A decree of 26 December 2007 was then submitted by the Prime Minister to the Conseil d'Etat after the CNIL published its opinion. Still, the Conseil d'Etat decided to partly invalidate the decree because of two provisions violating the French Data Protection Act.⁶⁵ Indeed, the Conseil d'Etat considered that the collection of the "AGDREF" number (the national identification number of foreigners on French Territory), was neither relevant nor proportionate to the aim of the processing. Moreover, it stated that it was excessive to retain during three years data relating to the identification of foreigners, their children, the application and characteristics of the measures of eviction, the exercise of recourse, and the request for a residence permit before consular authorities.

A new database, "EDVIGE," (*Exploitation Documentaire et Valorisation de l'Information Générale*) created in 2008⁶⁶ has given rise to mass protest. It was initially established for use by the French intelligence agencies and the administrative police. EDVIGE was

⁶³ EDRI-gram, No. 6.2, January 2008, "Key Privacy Concerns in France," available at <http://www.edri.org/edrigram/number6.2/privacy-france-2007>.

⁶⁴ Text of the Conseil d'Etat decision of 13 March 2007, available at http://www.conseil-etat.fr/ce/jurispd/index_ac_id0712.shtml; see also EDRI-gram No. 5.7, March 2007, "French High Court Cancels The Creation of Illegal Migrants Database," available at <http://www.edri.org/edrigram/number5.5/france-cancels-database>.

⁶⁵ Conseil d'Etat, "Section du contentieux, 10ème et 9ème sous-sections réunies, Séance du 4 décembre 2009, Lecture du 30 décembre 2009, Nos 312051, 313760. Association SOS Racisme – Groupe d'Information et de Soutien des Immigrés et autres", available at <http://www.conseil-etat.fr/cde/node.php?articleid=1906>.

⁶⁶ Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé "EDVIGE", JORF n° 0152, 1st July 2008, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019103207>.

supposed to record individuals, groups, and organisations, who, due to their individual or collective activity, are likely to attempt disrupting public order, or to have "direct and non-fortuitous relations" with such entities.⁶⁷ The database was intended to centralise various categories of data, including data relating to health and sexual orientation. This led in 2008 to a mass protest, including more than 40 parliamentarians, opposing its creation.⁶⁸ As a consequence, the decree that created the EDVIGE database was cancelled in November 2008.⁶⁹ However, EDVIGE has been replaced by new databases created by two decrees of October 2009.⁷⁰ One of these databases is intended to record individuals who, due to their individual or collective activity, are likely to attempt to disrupt public order. The other database will be used for administrative investigations to ensure that an applicant for a security job with a public authority did not act in contradiction with such a mission in the past. These databases will not contain personal data relating to sexual orientation or health, but other sensitive data relating to geographical origins, political, religious, and philosophical opinions, or trade union affiliations. The data of the first database may be kept for ten years for adults and three years for minors (aged 13 to 18). Their creation has led to new mass protests.⁷¹

Another database, "CRISTINA," was also created at the same time as EDVIGE and provides for "[c]entralising inland intelligence for homeland security and national interests".

On 20 January 2009, the CNIL published a report on the police database "STIC" (*Système de traitement des infractions constatées*, or recorded offences treatment system).⁷² The report "reveals that STIC is accessed by each one of the 100,000 authorised policemen

⁶⁷ Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé "EDVIGE", supra at 66; see also EDRI-gram, Number 6.14, July 2008, "Edvige French Database," available at <http://www.edri.org/edrigram/number6.14/edvige-french-database>.

⁶⁸ EDRI-gram, Number 6.15, August 2008, "More than 50,000 Signatures against EDVIGE," available at <http://www.edri.org/edrigram/number6.15/50000-signatures-edvige>.

⁶⁹ Décret n° 2008-1199 du 19 novembre 2008 portant retrait du décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé "EDVIGE", available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019774085&dateTexte=>.

⁷⁰ Décret n° 2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique, JORF n° 0242, 18 October 2009, at 17245, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021163904&fastPos=10&fastReqId=353873481&categorieLien=id&oldAction=rechTexte>; Décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique, JORF n° 0242, 18 October 2009, at 17244, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021163879&fastPos=11&fastReqId=353873481&categorieLien=id&oldAction=rechTexte>.

⁷¹ Pour obtenir l'abandon du fichier "EDVIGE" <http://www.nonaedvige.sgdg.org/>.

⁷² CNIL, "Conclusions du contrôle du système de traitement des infractions constatées (STIC)," available at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Controles_Sanctions/CNIL-Conclusions_des_controles_STIC.pdf (in French).

200 times a year on average."⁷³ A major problem with the database is the amount of errors – 83 percent – in the system.⁷⁴ The database records the name and other information of both the victim and the assailant in any case where an offence has been committed. The CNIL found that sometimes individuals are mistakenly placed in the wrong category. The database is supposed to be updated after a court decision but frequently is not. Furthermore, there are no restrictions on who is included in the database. Employers in a large range of job sectors are allowed by law to search the database when considering whether to hire an individual.⁷⁵

In February 2009, the Ministry of Justice sent a reminder to prosecutors confirming the shortcomings of the STIC updates, and asked them to be vigilant in view of the important human and social issues involved. The CNIL announced that it would carry out new audits of the database before the end of 2011.⁷⁶

A draft law of 27 May 2009 (*Projet de loi d'orientation et de programmation pour la performance*, or LOPPSI 2), submitted to the Senate in June 2010,⁷⁷ contemplated that genetic data could be used for criminal investigations purposes, medical and scientific research, and research about and identification of deceased individuals. Biological data could also be collected for the identification of deceased people. Agents of the technical and scientific police would be entitled to register genetic data in the FNAEG. As the CNIL noted in its opinion of 6 May 2010,⁷⁸ the data collected in a judiciary context cannot be used for civil or administrative identification purposes; genetic data relating to members of the family of people whose identification is searched for are recorded separately in the FNAEG, subject to their consent.

A law promulgated on 10 March 2010 in order to fight against serial crimes (*loi tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale*)⁷⁹ specifies the cases in which genetic data can be recorded in the FNAEG. This law permits the recording of not only genetic data of perpetrators of serious criminal

⁷³ Meryem Marzouki, "France: Who have They Forgotten to Control Today?" EDRI-gram, 7.2, 28 January 2009, available at <http://www.edri.org/edri-gram/number7.2/france-+forgotten-to-control-today>.

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ CNIL, 30e Rapport d'Activité 2009 (2010) at 14, available in French at http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf.

⁷⁷ *Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure*, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

⁷⁸ CNIL, "Les observations de la CNIL sur les nouvelles dispositions de la LOPPSI", 21 June 2010 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/les-observations-de-la-cnil-sur-les-nouvelles-dispositions-de-la-loppsi/>.

⁷⁹ Loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale, JORF n° 0059, 11 March 2010 at 4808, available at: <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021954436&dateTexte=&categorieLien=id>.

offences (e.g., sexual abuse, attempted murder, crimes against humanity, etc.), but also of authors of infractions related to prejudice against property (e.g., robbery and vandalism), individuals suspected of such crimes, individuals concerned by a decision of criminal irresponsibility, and deceased people who may correspond to a missing person or presumed deceased.

A French database called "OSCAR" ("*Outil de Statistiques et de Contrôle de l'Aide au Retour*" in French, or Tool for Repatriation Aid Statistics and Control) was created by decree in October 2009.⁸⁰ The database collects biometric data – digital photograph and ten fingerprints – of foreigners expelled from France or leaving it voluntarily, with the benefit of a small grant. In the case of EU citizens, the grant takes the form of a "humanitarian repatriation help" of €300 per person, with an additional €100 for each accompanying child. If the child is more than 12 years old, his biometric data are also collected and stored in OSCAR for five years.⁸¹

National and international data disclosure agreements

Nothing to report under this section.

Cybercrime

The Daily Safety Law (LSQ) also provides the government access to private encryption keys; import and export of encryption software are restricted, and strict sanctions are imposed for using cryptographic techniques to commit a crime.

The LEN includes the LSQ provisions on cryptography, with the following two additions: first, a lower penalty is applicable (jail and fine) in cases where cryptography has been used to commit or prepare an infraction, where the suspect herself provided decryption keys to the police, thus allowing for self-incrimination; second, some uses of cryptography for research or professional purposes are not specifically mentioned anymore, therefore assimilating these categories of people to cybercriminals, when they conduct such activities.⁸²

On 14 February 2008, the French Internal Affairs Minister announced new measures to combat cybercrime. Among other efforts, it will increase the blacklist of Web sites that make available child pornography information and racial hate speech, terrorist

⁸⁰ Décret n°2009-1310 du 26 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour géré par l'Office français de l'immigration et de l'intégration (J.O. of 28 October 2009), available in French at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=IMIK0922946D>.

⁸¹ See generally CNIL, "OSCAR : Outil de Statistique et de Contrôle de l'Aide au Retour", 26 August 2010, available in French at <http://www.cnil.fr/en-savoir-plus/fichiers-en-fiche/fichier/article/oscar-outil-de-statistique-et-de-contrôle-de-laide-au-retour/>, IRIS, "Fichiers et étrangers" <http://www.iris.sgdg.org/actions/fichiers/>.

⁸² The LEN has also added a definition of electronic mail, as part of the transposition of the EU Directive on Privacy and Electronic Communications (2002/58/EC). This definition does not provide that email is a correspondence, notwithstanding the fact that all the legislation on privacy (including the already cited 1991 law) refers to correspondence.

propaganda, and information about making explosives and chemical weapons. The Minister will also move forward with computer online investigations without the authorisation of the country of the hosting company.⁸³

A new criminal offence, the fraudulent use of someone else's identity on an electronic communications network in order to infringe on that person's peace, honour or dignity, was created by a bill of 27 May 2009 (*Projet de loi d'orientation et de programmation pour la performance* (LOPPSI 2)), then adopted by the National Assembly in February 2010, and submitted to the Senate in June.⁸⁴

Critical infrastructure

Nothing to report under this section.

INTERNET & CONSUMER PRIVACY

In late 2009 the Secretary of State in charge of the Development of the Digital Economy launched a debate on the topic of the right to be forgotten on the Internet ("*le droit à l'oubli*"). In May 2010, the Secretary of State in charge of the Development of the Digital Economy launched a public consultation on the "right to be forgotten", but considered from a wider angle.⁸⁵

E-commerce

Consent (opt-in) must be obtained before sending an electronic message (email, SMS, MMS,...) of a promotional nature to a consumer.⁸⁶ There are exceptions to the opt in rule applicable to electronic messages sent to consumers: (i) if the electronic contact details have been obtained directly from the targeted recipient in the framework of a sale of goods or services, (ii) if the solicitation relates to similar goods or services, (iii) if the solicitation is made by the same person, and (iv) if the target has been offered the possibility of opting out and will be given this possibility in any subsequent message sent, easily and free of charge.

The Union Française de Marketing Direct (UFMD) and the Syndicat National de la Communication Directe (SNCD), two direct marketing associations, have issued codes of

⁸³ EDRI-gram, No. 6.4, 27 February 2008, "French Police Extends the Internet Blacklist," available at <http://www.edri.org/edriagram/number6.4/french-internet-blacklist> ; see also "Guerre contre la criminalité sur Internet," Le Figaro, 12 December 2008, available at <http://www.lefigaro.fr/actualites/2008/02/13/01001-20080213ARTFIG00013-guerre-contre-lacriminalite-surinternet.php> (in French).

⁸⁴ *Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure*, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

⁸⁵ Secrétariat d'État à la Prospective et au Développement de l'économie numérique, "Droit à l'oubli numérique", 13 October 2010, available at <http://www.prospective-numerique.gouv.fr/numerique/usages-et-services/protection-de-l-internaute/droit-l-oubli-numerique.html>.

⁸⁶ Article L34-5 of the Post and Electronic communications Code. and article L 121-20-5 of the Consumer Code, available at http://www.legifrance.gouv.fr/affichCode.do?jsessionid=467705B2F34E4F50039D4ED9D675E640.tpdjo06v_2?idSectionTA=LEGISCTA000006165910&cidTexte=LEGITEXT000006070987&dateTexte=20101215.

conduct on email marketing⁸⁷ to provide guidance to their members (remote selling companies and companies operating email campaigns). These codes were approved by the CNIL in 2005.

To assist individuals in fighting unsolicited communications, private and public sector organisations, including the CNIL, created a non-profit organisation called "Signal-Spam"⁸⁸ that develops a tool enabling email recipients to easily report spam.

In addition to the *signal-spam.fr* website to report spam and the *mediateurdunet.fr* website for private or commercial dispute on the Internet, the French government has launched a new official website called *internet-signalement.gouv.fr* that offers Internet users the opportunity to report any illegal content or behavior that they might come across on the Internet.⁸⁹

ISPs and telecom operators' terms and conditions are under the scrutiny of consumer groups or associations whose mission is to prevent the violation of consumers' privacy. The consumer group *UFC Que Choisir* challenged Amazon.fr's online terms and conditions in court. On 28 October 2008, the Court of First Instance of Paris⁹⁰ found that the Amazon.fr site included several "improper or unlawful" clauses that were held unenforceable, some of which related to the processing of personal data, including the provision by which Amazon.fr can share personal data with Amazon.com, Inc. and the affiliates controlled by Amazon.com, Inc. The Court considered that this situation created an imbalance between the rights and obligations of the contracting parties as the sharing of personal data with undetermined affiliates was imposed upon the consumer without specification of the contemplated purpose and usefulness of the sharing. Clauses relating to solicitation, data disclosure, and co-branding were also criticised. The Court required Amazon to pay to UFC €30,000 in damages and ordered the removal of the illegal clauses from Amazon.fr's terms and conditions within a month.

The Data Protection Act allows intellectual property rights societies to create private records of rights infringers through the collection of their IP addresses in P2P networks; however, the use of automatic software for such collection is subject to CNIL approval. The CNIL decided in October 2005 to reject the introduction of surveillance devices,

⁸⁷ Union Française de Marketing Direct, Charte de l'emailing - Code relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe, available at http://www.ufmd.org/telechar/code_ufmd_prospection_emailing.pdf; Syndicat National de la Communication Directe, Livre collectif sur la délivrabilité des campagnes d'e-mail marketing", March 2005, available at http://www.sncd.org/_uses/lib/3853/deontologie_e_mailing_2005_03.pdf.

⁸⁸ At <http://www.signal-spam.fr>.

⁸⁹ Julie de Meslon, "Le gouvernement ouvre son portail de signalement des contenus illicites", 01Net, 6 January 2009 <http://www.01net.com/editorial/399983/le-gouvernement-ouvre-son-portail-de-signalement-des-contenus-illicites/>.

⁹⁰ Tribunal de Grande Instance de Paris, 1re chambre section sociale, 28 October 2008, Association Union Fédérale des Consommateurs Que Choisir vs. Amazon, available in French at <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20081028.pdf>.

proposed by Sacem and three other author and producer associations, for the automatic tracing of infringements of the Intellectual Property Code. This decision was cancelled by the Conseil d'Etat on 23 May 2007. The court found that the proposed devices are not disproportionate, and are acceptable considering the extent of piracy occurring in France. The author and producer associations resubmitted their request to the CNIL, and obtained the required authorisations in November 2007 and January 2008.⁹¹

Copyright holders envisaged a new role for ISPs for addressing online copyright infringement.⁹² In November 2007, some French ISPs and music and movie representatives signed the Olivenness Cooperation Agreement. French ISPs would monitor Internet customer's communications to identify peer-to-peer users who may infringe French copyright law. The agreement includes the "gradual response system" which involves a newly created independent authority, entitled HADOPI (*Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet*), to combat online piracy.⁹³

On 10 June 2009, the French Constitutional Council rejected key parts of the enforcement provisions of HADOPI.⁹⁴ The Council determined that a "three strikes" rule, in which HADOPI could cut off users' access to the Internet for a period of three months to a year after three warnings (the first two would be sent first by email then by registered mail) to stop their illegal downloads, violated a fundamental human right to freely communicate under the 1789 Declaration of Human Rights (*Déclaration des droits de l'homme*). The Council ruled that this was contrary to the presumption of innocence and did not provide adequate due process.⁹⁵ The Council found that HADOPI could issue the first two warnings but the third warning would have to be issued by a judge.⁹⁶ The Council explained that freedom of speech "implies today, considering the development of the Internet, and its importance for the participation in democratic life and the expression of

⁹¹ CNIL press release of 25 May 2005, available at <http://web.archive.org/web/20070824015532/http://www.cnil.fr/index.php?id=2221&news%5buid%5d=464&cHash=57a0f43bbe>; see also EDRI-gram No. 5.11, 6 June 2007, "French State Council Allows Tracing P2P Users," available at <http://web.archive.org/web/20080201013701/http://www.edri.org/edrigram/number5.11/france-tracing-p2p>.

⁹² IFPI, ISPs – Technical Options for Addressing Online Copyright Infringement (2006), available at http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf.

⁹³ EDRI-gram, Number 6.13, July 2008, "France Promotes The Three-Strike Scheme in Europe," available at <http://www.edri.org/edrigram/number6.13/france-europe-3-strikes>.

⁹⁴ Rick Mitchell and Christine Mumford, "French Constitutional Council Defangs Controversial 'Three-Strikes' Piracy Law," *Electronic Commerce & Law Report*, BNA, Inc., 17 June 2009, 851.

⁹⁵ *Id.*; see also Andrew Moshirnia, "Liberté, Egalité, Technologie: The French Resistance and the Anti-Piracy Campaign," *Citizen Media Law Project*, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

⁹⁶ *Id. supra* at 42.

ideas and opinions, the online public's freedom to access these communication services."⁹⁷

A second version of the law has been presented to the Parliament and brought again by some MEPs before the Constitutional Council who this time approved most of the text that was enacted on 28 October 2009.⁹⁸

The principle of "graduated riposte" is maintained but the suspension of Internet access can only be ordered by a judge. Some of the implementation decrees have been submitted to the CNIL for its opinion but have not yet been finalised, while others are still expected.

Cybersecurity

On 23 March 2010, the Senate voted on a bill⁹⁹ intended to enhance the protection of personal data, in particular by the creation of a security breach notification obligation upon data controllers. Senators wished to create a two-level notification obligation. At a first level, in case of violation of the processing of personal data, the data controller must inform the data protection correspondent or, in his absence, the CNIL. At a second level, if the violation has impacted the personal data of one or more individuals, the data controller must also inform those individuals, except for some "sovereignty files". This notification obligation would apply regardless of industry sector; hence would not be limited to the e-communications sector. The French government objected to the introduction of this measure. The bill is still to be reviewed by the National Assembly. As of September 2010, it has not been put on the agenda of the competent committee.

Additionally, the Ministry of the Economy, Industry, and Labour is preparing the implementation of the so-called EU "telecoms package",¹⁰⁰ including the 2009/136/EC Privacy and E-communications Directive that must be implemented into member states' laws before 25 May 2011. This Directive provides for a security breach notification obligation to a national authority by providers of electronic communications services. The Ministry conducted a public consultation in May 2010. The bill drafted by the Ministry provides for a notification by providers of electronic communications services on open networks, to both the CNIL and the individuals impacted by a "violation of

⁹⁷ Eric Pfanner, "French Council Defangs Plant to Crackdown on Internet Piracy," *The New York Times*, 10 June 2009, available at http://www.nytimes.com/2009/06/11/technology/internet/11net.html?_r=1&ref=technology.

⁹⁸ Loi n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, JORF n° 0251, 29 October 2009, at 18290, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021208046&categorieLien=id>.

⁹⁹ Proposition de loi adoptée par le Sénat visant à mieux garantir le droit à la vie privée à l'heure du numérique, 23 March 2010, available at <http://www.senat.fr/leg/tas09-081.html>.

¹⁰⁰ Projet de dispositions législatives de transposition. Textes en version consolidée, available at http://www.telecom.gouv.fr/fonds_documentaire/consultations/10/100505paquet-telecom-dispolegisaltive.pdf.

personal data" (i.e., a violation of security leading accidentally or unlawfully to the destruction, damage, loss, or disclosure of personal data).¹⁰¹

Online targeted advertising and search engine privacy

The phenomenon of targeted advertising on the Internet is recent in France; however it has been identified as a potential threat to Internet users' right to data protection, and is closely followed by the CNIL. In this respect, the Authority issued a report at the beginning of 2009 stressing that technological and economical changes in the business model of companies doing business on the Internet are worrisome.¹⁰² More and more companies, either by diversification or acquisition (e.g., Yahoo! and Google), become content providers, service providers (Internet access, email, search engines, etc) and advertising agencies for third parties, and, as a result, have the opportunity to aggregate the data they collect from users through various means.

The concentration of actors and data sources is therefore seen as a potential risk to privacy, in particular as individuals do not realise the impact these dynamics may have on the processing of personal data, especially since the CNIL finds that opt-out mechanisms (e.g., opt-out cookies) do not work adequately in practice. If advertising agencies were to share data they collect with businesses such as banks, insurance companies, or recruiters, selections and assessments of consumers, applicants, or job candidates could be made based on assumptions about their health, finances, or other sensitive information without individuals being fully aware of it. This is viewed as a real threat by the Authority.

The CNIL's report underlines the various challenges that online targeted advertising presents to data protection authorities. It indeed opens the debate as to whether a technical identifier (IP address or identifier placed in a tracking cookie) is "personal data", and how to ensure that individuals can exercise their opt-out and opt-in rights efficiently.

¹⁰¹ For more details, see Marie-Andrée Weiss & Cédric Laurant, "Will France Adopt a Law Requiring The Notification of Security Breaches?," Information Security Breaches & The Law Blog, 6 August 2010 http://blog.security-breaches.com/2010/08/06/will_france_adopt_a_law_requiring_the_notification_of_security_breaches/. [French version: Marie-Andrée Weiss & Cédric Laurant, "La France va-t-elle se doter d'une loi rendant obligatoire les notifications des violations de sécurité ?," Information Security Breaches & The Law Blog, 3 August 2010 http://blog.security-breaches.com/2010/08/03/la_france_va_t_elle_se_doter_d_une_loi_rendant_obligatoire_les_notifications_des_violations_de_securite/.]

¹⁰² CNIL, La publicité ciblée en ligne (Communication), 5 February 2009, available at http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf. For an English translation of the key sections of this report go to the "Publications" page of the website <http://pascalegelly.com>.

On 30 September 2010, the Secretary of State in charge of the development of the Digital Economy, gathered industry associations to sign a Code of Conduct on "targeted advertising and protection of internet users".¹⁰³

Online social networks and virtual communities

See updates under sections "Major Privacy & Data Protection Case Law", "Online Youth Safety", and "Workplace Privacy"

Online youth safety

The protection of minors (people under the age of 18) surfing on the Internet is a topical subject in France, in particular because of the success of social networks and the development of direct marketing techniques that target them specifically.

Several direct marketing associations have issued recommendations and guidelines¹⁰⁴ in order to encourage providers of Internet services and marketing professionals to carry out protective measures before processing minors' data and offering them services and products.

A well-known association of IT professionals, that deals with Internet and issues related to new technologies, provides advice to parents¹⁰⁵ and minors¹⁰⁶ in order to help the former protect their children when they surf the Internet, and help the latter more cautiously use the Internet.

TERRITORIAL PRIVACY

Video surveillance

A new Anti-Terror Act of 23 January 2006¹⁰⁷ extends the use of video surveillance for police and intelligence services, authorising private parties to install CCTV cameras in

¹⁰³ Union Française de Marketing Direct, Charte sur la publicité ciblée et la protection des internautes, available at http://www.ufmd.org/telechar/20100929UFMD_v26_final.pdf.

¹⁰⁴ Union Française de Marketing Direct, Charte de l'emailing - Code relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe, available at http://www.fevad.com/images/DocArticle/code_ufmd_prospection_emailing.pdf; Syndicat National de la Communication Directe, Code de Déontologie de la communication directe électronique, March 2005, available at http://www.sncd.org/_uses/lib/3853/deontologie_e_mailing_2005_03.pdf.

¹⁰⁵ Fiches pratiques "Parents" <http://www.foruminternet.org/particuliers/fiches-pratiques/parents/> (not available at this URL anymore since 1 Dec. 2010); but available at <http://web.archive.org/web/20080716074140/www.foruminternet.org/particuliers/fiches-pratiques/parents/>.

¹⁰⁶ Fiches pratiques "Juniors" <http://www.foruminternet.org/particuliers/fiches-pratiques/juniors/> (not available at this URL since 1 December 2010 but available at <http://web.archive.org/web/20080822083249/http://www.foruminternet.org/particuliers/fiches-pratiques/juniors/>).

¹⁰⁷ Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, available at <http://www.senat.fr/apleg/pjl05-109.html>.

public places "likely to be exposed to terrorist acts" and in places open to the public when they are "particularly exposed to risks of aggression or theft". In case of emergency, CCTV cameras may be installed prior to any authorisation. Furthermore, the Act allows the police to automatically monitor cars on French roads and highways, taking pictures of licence plates and people in the cars, with various purposes ranging from the fight against terrorism to the identification of stolen cars.¹⁰⁸ The same article provides for the monitoring of street gatherings during "big events."

Video surveillance (CCTV) is increasingly used in the French society. In October 2008, the Paris City Council announced its project to install 1,226 video cameras in the streets of Paris.¹⁰⁹ Their presence will be made clear and an ethics committee will supervise their use.

Two distinct set of rules co-exist and intermingle with regard to CCTV. On the one hand, the Law of 21 January 1995, which subjects video surveillance cameras located in public places to prior authorisation by a local administrative authority, and, on the other, the Data Protection Act, which applies to video cameras implemented either in "private" areas such as business premises or in association with biometrics. Moreover, the CNIL considers that all systems, if digital, are subject to the Data Protection Act. The superposition of texts creates great confusion.

The CNIL has recommended that the government subject all CCTV devices to the control of the CNIL, pointing to a public survey whereby 79 percent of individuals would like CCTV to be under the control of an independent body to prevent risks of misuse and guarantee civil liberties. That recommendation is supported by the Legislative Committee of the Senate.

The LOPPSI 2¹¹⁰ extends the possibilities of use of video surveillance (called video protection in the draft law) in public areas. According to a law of 1995 relating to security on the French territory,¹¹¹ authorised uses of video cameras in public areas were initially limited to the surveillance of public and military buildings, road traffic and infringements on public roads, areas that are particularly exposed to aggression, robbery, or terrorist attacks. According to the draft LOPPSI 2, the use of video surveillance in public areas would also be extended in order to monitor areas particularly exposed to drug traffic, to prevent natural or technological disasters and to fight against fire.

LOPPSI 2 also provides the possibility for public authorities, after mere notification to the mayor, to delegate to public or private operators the operation of their video

¹⁰⁸ *Id.* at art. 8.

¹⁰⁹ "Paris : la carte des 1200 caméras de surveillance", *Le Parisien*, 20 October 2008, available at <http://www.leparisien.fr/une/paris-la-carte-des-1200-cameras-de-surveillance-20-10-2008-283302.php>.

¹¹⁰ Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

¹¹¹ Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, available at <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005617582&dateTexte=20100812>.

surveillance systems. The CNIL pointed out in its opinion of 6 May 2010¹¹² the danger of such outsourcing, especially if made to other countries, as it would make their control by public authorities impossible. As a result, it may give rise to serious issues in terms of security of data processing, national security and sovereignty.

The CNIL has been lobbying for several years to be the Authority in charge of regulation and control of video surveillance.¹¹³ However, LOPPSI 2 creates a new Authority, the "Commission nationale de la vidéoprotection" in charge of controlling video surveillance systems on the French territory. The CNIL will still have the power, on its own initiative or at the request of the "Commission nationale de la vidéoprotection," to analyse and control compliance of video surveillance systems with the Data Protection Act and order sanctions in case of violation.

The video surveillance system installed in city buses in the city of Lille in the north of France recorded images and sound in a continuous way to ensure drivers' and passengers' safety. The CNIL considered that continuous sound recording was disproportionate to the purpose of the system and invasive of drivers' privacy in their workplace. Instead, the recording could simply be triggered by the bus driver in case of an assault.

Location privacy (GPS, mobile phones, location-based services, etc.)

Insurance companies and car manufacturers are now interested in implementing geo-location technologies into their customers' cars. The objective is to propose "pay-as-you-drive" services to customers in order to adapt the amount of their insurance premiums in light of new criteria such as mileage, driving duration without break, speed, and style of driving. One of the risks is that such technologies would enable insurance companies to access and process data relating to driving offences, such as driving over the speed limit, whereas the Data Protection Law prohibits such collection. The CNIL has authorised their use by insurance companies and car manufacturers, and recommended in a decision of 8 April 2010 to limit the collection to average speed, to the exclusion of any data that may help characterise offences.¹¹⁴

¹¹² CNIL, "Les observations de la CNIL sur les nouvelles dispositions de la LOPPSI", 21 June 2010 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/les-observations-de-la-cnil-sur-les-nouvelles-dispositions-de-la-loppsi/>.

¹¹³ *Supra* at 112.

¹¹⁴ CNIL, Délibération 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules, 8 April 2010, JORF n° 0114, 19 May 2010, available at <http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/224/>.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The use of biometric identifiers is increasing for immigration and border control.¹¹⁵ Since November 2003, the Immigration Law has set out the use of biometric techniques for visa delivery and border controls, and the storing of all visa requesters' fingerprints and biometric pictures in databases for further processing. As part of the implementation of this law, and at the request of the European Commission, an experimental file was created from November 2004 to November 2006 as a complement to the French worldwide visa requests management system, RMV2 (Réseau Mondial Visas 2). RMV2 links central administration to French Consulates abroad and communicates with the Schengen Information System (SIS). This experimental file contains the digitised photograph and all fingerprints of persons who requested visas at select French consulates during that time period. This data is retained for two years for a short-stay visa request, five years for a long-stay visa request or in case of visa denial. Access to this file is allowed to some border police officers at some French airports, harbours, or land frontiers. Biometric identifiers may be included in an electronic chip on the visa. In 2006, a new decree further extended the use of the file so as to allow identity controls by the police everywhere in France, not only upon entry at the borders. The same decree also extended the collection of biometric identifiers of other EU member state consulates, and the access to these data to police officers other than those working in border control.¹¹⁶

France has issued biometric passports since 30 March 2006, following ICAO requirements. Because the chip included in the passport only contains a digitised photograph, as provided by a 30 December 2005 Decree, and does not include fingerprints, it is officially called an "electronic" passport. In February 2007, the government created the "National Agency for secured identity documents." The agency's missions include the definition, control, and assessment of technical standards and tools used for the creation of electronic and biometric identity and travel documents.¹¹⁷

¹¹⁵ Loi n° 2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0300040L> (in French); Décret n° 2004-1266 du 25 novembre 2004 portant création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTD0400325D> (in French).

¹¹⁶ Décret n° 2006-470 du 25 avril 2006 modifiant le décret n° 2004-1266 du 25 novembre 2004, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTD0600085D> (in French).

¹¹⁷ Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTD0500343D>; Décret n° 2007-240 du 22 février 2007 portant création de l'Agence nationale des titres sécurisés, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTA0700020D> (in French).

A new Anti-Terror Act enacted on 23 January 2006¹¹⁸ provides that the Ministry of the Interior may process PNR (passenger name records) data collected on any travel by air, sea, or rail to or from non-EU countries.¹¹⁹ The objective of the law is "to improve border controls and to fight against illegal immigration."¹²⁰

A French database called "OSCAR" (*Outil de Statistiques et de Contrôle de l'Aide au Retour*, or Tool for Repatriation Aid Statistics and Control) was created by decree in October 2009.¹²¹ The database collects biometric data – digital photograph and ten fingerprints – of foreigners expelled from France or leaving it voluntarily.¹²²

(See more details under the "National databases for law enforcement and security purposes" section.)

NATIONAL ID & SMART CARDS

The French biometric ID card project (INES) is still in a frozen state after it received strong criticisms from civil rights NGOs and the French Data Protection Authority, and through a report synthesising a public debate commissioned by the Ministry of Interior. The only public presentation document of the project is dated March 2005. According to this document, the project aimed to provide the whole population with a new ID card by 2007, with an RFID chip containing the civil status of the citizen as well as two biometric identifiers: photograph and fingerprints. This data would be recorded in centralised databases. The card would be mandatory and would also include the address of the holder. It would also be programmable, to become an electronic portfolio that could be used for e-administration as well as commercial electronic transactions.¹²³

¹¹⁸ Loi No. 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, available at <http://www.senat.fr/apleg/pjl05-109.html>.

¹¹⁹ *Id.* at Art. 7.

¹²⁰ See generally EDRI-gram No. 4.2, February 2006, "French Anti-Terrorism Law Not Anti-Constitutional," available at <http://www.edri.org/edriagram/number4.2/frenchlaw>.

¹²¹ Décret n°2009-1310 du 26 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour géré par l'Office français de l'immigration et de l'intégration (J.O. of 28 October 2009), available in French at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=IMIK0922946D>.

¹²² See generally CNIL, "OSCAR : Outil de Statistique et de Contrôle de l'Aide au Retour", 26 August 2010, available in French at <http://www.cnil.fr/en-savoir-plus/fichiers-en-fiche/fichier/article/oscar-outil-de-statistique-et-de-contrôle-de-laide-au-retour/>, IRIS, "Fichiers et étrangers" <http://www.iris.sgdg.org/actions/fichiers/>.

¹²³ See the Web site of the NGO campaign with relevant documents, available at <http://www.ines.sgdg.org/>.

RFID tags

From 2008 several maternity hospitals started using electronic bracelets on newborn babies to deter kidnapping.¹²⁴ Reviewing their legality in light of data protection principles, the CNIL raised the issue of their proportionality with regard to the risks at stake. It feared that legitimising these systems by compromising the children's vulnerability could lead society to extend their use for other reasons later in children's lives, when they are at kindergarten or school, and subject any child from his earliest age to constant tracking. Because of the difficult issues these new devices raise - elderly people included - the CNIL wants to start a discussion about the implications of electronic tracking devices for vulnerable persons.

BODILY PRIVACY

The draft law of 27 May 2009 (*Projet de loi d'orientation et de programmation pour la performance*, or LOPPSI 2), adopted by the National Assembly in February 2010 and submitted to the Senate in June 2010¹²⁵ provides the possibility of experimenting with the use of body scanners in areas of airports not freely accessible to the public for a duration of three years. This system enables the agent to see a schematic image of the person as opposed to a real image of the naked person. The images would not be stored and would be watched by agents located in a dedicated room who do not know the identification of the person on the screen. The travelers can choose between the use of the body scanner or other security measures such as a body frisk.

From February 2010 body scanners have been trialed at Paris Roissy Airport. The CNIL has audited the airport and stated that the body scanners¹²⁶ were used in compliance with its recommendations, which were taken into consideration in the LOPPSI 2 draft law.

Biometrics devices are subject to the prior authorisation of the CNIL, which favours devices using biometrics without tracks (vein, face, hand shape, and so on) over those leaving tracks such as fingerprints. It is easier for the CNIL to authorise devices where fingerprint data (transformed into an algorithm) is stored on an individual media (e.g., a card) that the individual holds himself, than devices involving the storage of fingerprint data in a central database. In the latter case, the requester has a higher burden of proof to meet since the stakes go well beyond the interest of the data controller, and there are rigorous conditions to comply with in order to obtain the CNIL's authorisation.

¹²⁴ CNIL, "Antivols pour nouveau-nés : pour ou contre les bracelets électroniques dans les maternités?", 19 May 2008, <http://www.cnil.fr/la-cnil/actu-cnil/article/article/antivols-pour-nouveau-nés-pour-ou-contre-les-bracelets-electroniques-dans-les-maternites/>.

¹²⁵ Projet de loi adopté par l'Assemblée Nationale, d'orientation et de programmation pour la performance de la sécurité intérieure, 2 June 2010, available in French at <http://www.senat.fr/leg/pjl09-518.html>.

¹²⁶ CNIL, "Body scanner : quel encadrement en France et en Europe ?", 8 June 2010 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/body-scanner-quel-encadrement-en-france-et-en-europe/>.

On 18 June 2009, the CNIL granted an authorisation¹²⁷ to the testing company GMAC (Graduate Management Admission Council) to use biometric technology in France to control access to examination centers for the GMAT test used for student selection by business schools around the world. The authorised system uses palm vein identification technology and stores students' biometrics in a central database for five years for the purpose of fighting exam fraud.

Biometrics systems are now used in hospitals to identify radiotherapy patients in order to avoid the risks of excessive irradiation. On 11 February 2010, the CNIL authorised for the first time such use of biometrics by a hospital.¹²⁸

WORKPLACE PRIVACY

Employees have a right to privacy in the workplace.

In 2001, the French high labour court (Chambre sociale de la Cour de Cassation) held in *Nikon v. Onof* that employees have a right to privacy at the workplace and that an employer cannot access an employee's personal emails stored on a work computer without violating the employee's privacy.

Since 2006, case law has determined that emails and files stored on company systems at the workplace are presumed to be work-related unless they are clearly flagged as "personal" or "private". As a result, the principle is established that the employer can access the employee's emails and files stored in his work computer or his office, except for those flagged as "private" or "personal".¹²⁹ But there are exceptions: the employer can access even the private files of an employee if the employee is present or if the company is facing particular risks.¹³⁰

The violation of company rules relating to the use of the Internet by an employee are not necessarily sufficient justification to terminate an employee. The Supreme Court (*Cour de cassation*) decided such a case where an employee accessed porn Web sites during

¹²⁷ CNIL, Délibération n° 2009-360 du 18 juin 2009, autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT (demande d'autorisation n° 1323460), available at <http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000020972764&fastReqId=1603510912&fastPos=1>.

¹²⁸ CNIL, "40.000 euros d'amende pour DirectAnnonces", 28 July 2009 <http://www.cnil.fr/dossiers/sante/actualites/article/552/la-biometrie-entre-a-lhopital-pour-identifier-des-patients-traites-par-radiotherapie-1/>.

¹²⁹ Cour de cassation (chambre sociale), audience publique du Wednesday 18 October 2006, n° de pourvoi: 04-48025, available at <http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007054915&fastReqId=2027183576&fastPos=1>.

¹³⁰ Cour de cassation (chambre sociale), audience publique du Tuesday 17 May 2005 n° de pourvoi: 03-40017, available at <http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007048803&fastReqId=1280562535&fastPos=1>.

working hours. It was considered that this behavior did not negatively affect the employee's work.¹³¹

In November 2009, the recruitment association "A Compétence Egale" presented a code of conduct¹³² aimed at ensuring the proper use of Internet resources in job selection and recruitment procedures, and in particular of information available on social networks.

HEALTH & GENETIC PRIVACY

Health privacy

Computerised patient records (*dossier médical personnel*, or "DMP") were created by law in 2004 for the entire population of France. In its April 2007 study, the CNIL found a serious lack of data protection and many security breaches in the DMP process, and called for reinforced security measures. Furthermore, the Ministry of Health proposed a modification to the law in 2006 that would use individuals' social security numbers (NIR) to identify and link medical records. Civil rights NGOs strongly protested against this project, as it would breach privacy rights by facilitating the interconnection between medical data and other personal data contained in various national files.¹³³ The CNIL proposed in its conclusions the use of a different identifying number, derived through a non-reversible anonymisation process.¹³⁴

In 2008, the Ministry of Health, asked the National Consultative Ethics Committee (*Comité Consultatif National d'Ethique*, or CCNCE) for an opinion regarding the blocking factors of the DMP implementation and the possible ways to address them. The Committee's report¹³⁵ stated that these factors were, among others, the opposition between the right of the patients not to reveal certain elements of their health records to the DMP and the necessity for the health care system to trust the information contained in the DMP, also the inability of hospitals' and health professionals' current information systems to guarantee the effective operation of the DMP, the important risks of failure in the security and confidentiality of health data, which could result from the

¹³¹ Cour de cassation (chambre sociale), audience publique du Tuesday 8 December 2009, n° de pourvoi: 08-42097, available at <http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000021476363&fastReqId=354890225&fastPos=1>.

¹³² A Compétence Egale, "L'association A Compétence Egale lance la charte réseaux sociaux, Internet, vie privée et recrutement" (SocialNetworks, Internet, Privacy, and Recruitment), press release, 12 November 2009, available at http://www.acompetenceegale.com/upload/12%20novembre%202009%20CP%20Charte_1.pdf.

¹³³ As of May 2007, the NGOs' petition had reached 12,000 signatures.

¹³⁴ CNIL, "La CNIL contrôle le dossier médical personnel", 14 April 2007, <http://web.archive.org/web/20080530002013/http://www.cnil.fr/index.php?id=2212>; see also EDRigram No. 4.23, December 2006, "France - Using Social Security Number to Identify Medical Records," available at <http://www.edri.org/edrigram/number4.23/nir>.

¹³⁵ Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé, Avis n° 104: Le "dossier médical personnel" et l'informatisation des données de santé", 29 May 2008, available at http://www.ccne-ethique.fr/docs/Avis_104.pdf.

interconnection of several computerised files, and the important cost of implementation of the DMP. The Committee proposed in particular to limit the use of the DMP, on a voluntary basis, to patients who are suffering from serious illness involving long treatments with several health care professionals.

In July 2010,¹³⁶ the Ministry of Health confirmed its plan to relaunch¹³⁷ the DMP. The objective announced consists of implementing the DMP before the end of 2010. In order to do so, the Minister announced the strengthening of the steering committee, the implementation of technical measures to ensure system interoperability and data security, and the definition of a national identifying number. In the relaunch plan of April 2009, the government indicated that this number had to be determined in accordance with the CNIL's recommendations.¹³⁸ Recently, the official Web site of the government mentioned that such a number would be calculated on the basis of an algorithm based on several elements of patient identification, among others the NIR (the Social Security Number).¹³⁹

The law of 2002 concerning the rights of patients and the quality of healthcare (*Loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de soins*), provides that suppliers of storage services of health data on behalf of healthcare professionals must obtain a licence issued by the Ministry of Health. A Decree of January 2006 sets forth the procedure to request that licence. Their delivery had been interrupted for two years because of organisational difficulties. Reference documents were created to ease the application process and the procedure was relaunched in 2009. In June 2010, 12 suppliers had obtained a licence from ASIP Santé (Agency of the Health Ministry) as a result of the procedure, which also involves a review by the CNIL.¹⁴⁰

In parallel, a computerised file of pharmaceutical data ("*données pharmaceutiques*", or DP) has been created by the Law of 30 January 2007. The aim of the DP is to improve the level of information of pharmacists in order to prevent the risks of dangerous interactions between medicines. The DP contains the history of the pharmaceutical products provided to a person during the last four months. People are not obliged to use it. Access to this file

¹³⁶ Agence des systèmes d'information partagés de santé (Ministère de la Santé et des Sports), "Discours de la Ministre de la Santé et des Sports sur le DMP - Bordeaux, le 22 juillet 2010", 26 July 2010, available at <http://esante.gouv.fr/contenu/discours-de-la-ministre-de-la-sante-et-des-sports-sur-le-dmp-bordeaux-le-22-juillet-2010>.

¹³⁷ Ministère de la Santé et des Sports, Programme de relance du DMP et des systèmes d'information partagés de santé, Dossier de presse, 9 April 2009, available at <http://www.sante-sports.gouv.fr/IMG/pdf/DP-DMP.pdf>.

¹³⁸ Ministère de la Santé et des Sports, Programme de relance du DMP et des systèmes d'information partagés de santé, Dossier de presse, 9 April 2009, at 7, available at <http://www.sante-sports.gouv.fr/IMG/pdf/DP-DMP.pdf>.

¹³⁹ Agence des systèmes d'information partagés de santé (Ministère de la Santé et des Sports), "L'identifiant national de santé : une mise en œuvre progressive", 24 April 2010, available at <http://esante.gouv.fr/contenu/l-identifiant-national-de-sante-une-mise-en-oeuvre-progressive>.

¹⁴⁰ Agence des systèmes d'information partagés de santé (Ministère de la Santé et des Sports), "Hébergeurs agréés", 16 November 2010, available at <http://esante.gouv.fr/contenu/hebergeurs-agrees>.

is limited to pharmacists. After a period of experimentation, which started in May 2007, the CNIL has authorised the generalisation of its implementation on 2 December 2008. The CNIL published its first authorisation decisions (for pharmacists in hospitals) to carry out the DP processing in May 2010. As for the DMP, the storage of health data contained in the DP is subject to a licence of the Minister of Health and the patients' national identifying number cannot be used. The CNIL has temporarily authorised the National Council of Pharmacists (*Conseil National de l'Ordre des Pharmaciens*, or CNOP) to use an identifying number based on the personal data available on the each patient's individual health card ("*carte vitale*").

In 2009, a law called "Hospitals, Patients, Health and Territories" (*Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires*) harmonised all the rules relating to the DMP and the DP into the same code, the Code of Public Health (*Code de la santé publique*) and stated that access by healthcare professionals to the DMP is subject to patient consent. This law also provides the possibility for HIV screening centres to remove the anonymity of seropositive patients, in the conditions fixed in Minister Order (*arrêté ministériel*) of 8 July 2010,¹⁴¹ in the cases where there is a therapeutic interest for the patient to do so and provided that the patient has given his express prior consent.

Genetic privacy

Nothing to report under this section.

FINANCIAL PRIVACY

In September 2008, the European Court of Human Rights ruled for the second time that French searches and seizures of documents by tax authorities on a suspicion of fraud violated the European Convention on Human Rights.¹⁴² The court further observed that such searches were already established as violating the Convention, thus it was unnecessary to consider if it was a violation of the right to privacy.¹⁴³

E-GOVERNMENT & PRIVACY

Voting is open to those 18 years or older, but is not mandatory. Although the right to privacy is not enumerated in the French Constitution, the French Constitutional Court ruled in 1994 that it is implied.¹⁴⁴ The French Electoral Code requires voters to cast their

¹⁴¹ Arrêté du 8 juillet 2010 fixant les conditions de la levée de l'anonymat dans les consultations de dépistage anonyme et gratuit et dans les centres d'information, de dépistage et de diagnostic des infections sexuellement transmissibles, available at http://www.legifrance.com/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20100721&numTexte=46&pageDebut=13459&pageFin=13461.

¹⁴² *Kandler v. France* (No. 18659/05), Privacy Law and Business, 8 October 2008.

¹⁴³ *Id.*

¹⁴⁴ Décision 94-352 du Conseil Constitutionnel du 18 Janvier 1995, available at <http://www.conseil-constitutionnel.fr/decision/1994/94352dc.htm>.

vote in total confidentiality.¹⁴⁵ Reform of the French electoral legislation leaves the regulation of electronic elections to the High Council for French Expatriates (CSFE). In 1993, the CNIL adopted recommendations on electronic voting systems.¹⁴⁶ The recommendations warn about the need to maintain rigorous measures for the separation of the voter's identity and his vote.¹⁴⁷ During the last presidential elections, 1.44 million voters used electronic voting machines.¹⁴⁸ The "association Ordinateurs de vote," an NGO dedicated to voter privacy, circulated a petition opposing electronic voting machines. As of June 2007, the petition had over 86,000 signatures.¹⁴⁹

In September 2000, France allowed for the first time Internet voting on a five-year term referendum in the City of Brest.¹⁵⁰ There are concerns regarding Internet voting and about voters being intimidated or denied privacy in casting their ballots.¹⁵¹ On 11 December 2002, 860 volunteers participated in an Internet voting project conducted by the EU in the city of Issy-les-Moulineaux.

In 2008, the CNIL conducted 20 audits of electronic voting systems carried out by public entities,¹⁵² and in 2009, the CNIL audited the use of such systems by public and private entities. In its annual activity report for 2009,¹⁵³ the CNIL noted that these audits reveal a certain number of violations of the Data Protection Act.

¹⁴⁵ European Commission, CyberVote Report Chapter 3: "The Election regulations today," 1 July 2001, available at <http://www.eucybervote.org/Reports/KUL-WP2-D4V2-v1.0-02.htm>.

¹⁴⁶ Commission nationale de l'informatique et des libertés (CNIL), Vote électronique, 1 July 2003, available at <http://www.cnil.fr/index.php?id=1009>.

¹⁴⁷ *Id.*

¹⁴⁸ "Machines à voter ou machines à truquer?" *Politis*, 8 mars 2007, available at <http://www.politis.fr/Machines-a-voter-ou-machines-a,527.html>.

¹⁴⁹ See <http://www.ordinateurs-de-vote.org/petition/>. Pierre Muller, founder of the organization, received le Prix Voltair, a positive Big Brother Award, for his work in this area. See <http://bigbrotherawards.eu.org/Pierre-Muller-le-webmaster-de-Ordinateurs-de.html>.

¹⁵⁰ European Commission, Cybervote Report, An Innovative Cyber Voting System, *supra*.

¹⁵¹ "What is the Future of Electronic Voting in France, Recommendations," 26 September 2003, available at <http://www.foruminternet.org/telechargement/documents/reco-evote-en-20030926.htm>.

¹⁵² CNIL, Annual Activity Report 2008, available at: <http://www.ladocumentationfrancaise.fr/rapports-publics/094000211/index.shtml>.

¹⁵³ CNIL, Annual Activity Report 2009, available at: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf.

OPEN GOVERNMENT

As far as access to information is concerned, two laws in France provide for a right to access administrative documents held by public bodies.¹⁵⁴ The Commission of Access to Administrative Documents (*Commission d'accès aux documents administratifs*, or CADA)¹⁵⁵ is charged with enforcing the Acts.¹⁵⁶ It can mediate and issue recommendations but its decisions are not binding. According to the CADA, it received 4,900 inquiries in 2000 and 5,400 in 2004.¹⁵⁷ The law was amended in April 2000 to clarify access to legal documents and also the identity of the civil servant processing the request.¹⁵⁸

An ordinance was adopted in June 2005 to amend the 1978 law to implement the EU Directive on the re-use and commercial exploitation of public sector information (2003/98/EC).¹⁵⁹ It also made a number of other changes to the law including setting out the structure and composition of the Commission, requiring bodies to appoint a responsible person, and allowing access in electronic form.¹⁶⁰

OTHER RECENT FACTUAL DEVELOPMENTS (WITH AN IMPACT ON PRIVACY)

There has been an increase of public awareness of privacy in the last few years in France. Privacy is now increasingly addressed in the media. The newspaper *Le Canard enchaîné* issued a special "dossier" on surveillance,¹⁶¹ while UFC Que Choisir?, an influential consumer group association, published a special release, "Do not touch my privacy", in September 2009,¹⁶² The consumer group has also been active before the courts to obtain the cancellation of unconscionable privacy clauses in online stores and telecom providers'

¹⁵⁴ Loi n° 78-753 du 17 juillet 1978 sur la liberté d'accès aux documents administratifs; Loi n° 79-587 du juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public. Amended by Loi N° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations (Journal officiel, 13 April 2000).

¹⁵⁵ At <http://www.cada.fr>.

¹⁵⁶ Commission d'accès aux documents administratifs, 12e rapport d'activité 2002, July 2003, available at <http://www.ladocumentationfrancaise.fr/brp/notices/034000645.shtml>.

¹⁵⁷ For more details, see David Banisar, Freedom of Information and Access to Government Records around the World, available at http://obcan.ecn.cz/docs/FOI_survey.pdf.

¹⁵⁸ Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations (J.O. April 13, 2000).

¹⁵⁹ Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, available at <http://admi.net/jo/20050607/JUSX0500084R.html>.

¹⁶⁰ See freedomofinfo.org Country Survey – France, available at <http://www.freedominfo.org/countries/france.htm#4>.

¹⁶¹ "Je te vois. Filés ! Fichés ! Fliqués ! Comment nous sommes tous sous surveillance," Les dossiers du *Canard Enchaîné*, n° 113, October 2009.

¹⁶² UFC Que Choisir, Que Choisir spécial: "Touche pas à ma vie privée", n° 81, September 2009.

terms and conditions (See the "E-commerce" section). In July 2009, civil society groups opposed the implementation of intelligent advertising LCD screens in a Parisian subway station.¹⁶³ These screens not only broadcast messages but can also count the number of people passing by and measure the time spent looking at the screen, thanks to a face-scanning sensor. Since these actions, the French data protection Authority, the CNIL, has issued a report arguing that this technology must take into consideration the data protection rights of individuals as provided under the Data Protection Law: individuals must receive proper notice and the devices must be notified to the CNIL.¹⁶⁴

"Correspondents for the protection of personal data", was created by the law of 6 August 2004 to ensure the protection of personal data within data controllers and become an intermediary with the CNIL, is growing: 6,869 data controllers have so far appointed a "*Correspondant*".¹⁶⁵ The profession is also getting organised: in June 2009 a professional association of Correspondents, the French Association of Personal Data Correspondents (*Association Française des Correspondants aux Données Personnelles*, or AFCDP) set up a conference on "the role and future of the data protection officials".

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Every year Privacy International and a growing number of affiliate human rights groups present the Big Brother Awards to government agencies, private companies, and individuals who have excelled in the violation of an individual's privacy.¹⁶⁶

The 2010 Big Brother Awards, held in May, declared the winners to be: Nicolas Sarkozy, President of the French Republic, winning for his entire career; the Ministers of Culture along with all French school headmasters for implementing the national database "*base élèves*" and for their use of biometrics at school; the Director of the Institute of National Statistics (INSEE); the music industry lobby; and the Thales Group for all of its work.¹⁶⁷

At the 4 April 2009 Big Brother Awards ceremony, the French Minister of the Interior, Michèle Alliot-Marie, received the lifetime menace award for her "immoderate taste for police files," for redefining the term video surveillance as "video-protection," her "incitements to denouncement", and "her talent to construct the 'internal enemy'." Other winners included Paris Mayor, Bertrand Delanoë; Humabio, an EC-funded research

¹⁶³ RAP (Résistance à l'agression publicitaire), "Ecrans de pub espions du métro : les associations contre-attaquent !" <http://www.antipub.org/spip.php?article48>. The civil society groups were: Résistance à l'agression publicitaire, Souriez vous êtes filmés, Big Brother Awards, Robin des Toits, and Le Publiphobe.

¹⁶⁴ CNIL, "Panneaux publicitaires de mesure d'audience : la CNIL est compétente et contrôle !", 22 April 2009 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/panneaux-publicitaires-de-mesure-daudience-la-cnil-est-competente-et-contrrole/>; CNIL, "Dispositifs d'analyse du comportement des consommateurs : souriez, vous êtes comptés !", 19 April 2010 <http://www.cnil.fr/la-cnil/actu-cnil/article/article/dispositifs-danalyse-du-comportement-des-consommateurs-souriez-vous-etes-comptes-2/>.

¹⁶⁵ CNIL, "Correspondants" <http://www.cnil.fr/la-cnil/nos-relais/correspondants/>.

¹⁶⁶ Big Brother Award International, available at <http://www.bigbrotherawards.org/>.

¹⁶⁷ Big Brother Awards France <http://bigbrotherawards.eu.org/>.

project; the family benefits sector of the social security system; MEP and spokesman for Nicolas Sarkozy's party, Frédéric Lefebvre; the French minister of the Budget, Eric Woerth; and the French mutual insurance system. The Voltaire awards were given to the coalition against the EDVIGE police file; the coalition of elementary and primary school directors against the central database of children ("*base élèves*"); the coalition against the use of biometrics in schools; and to two humanitarians who helped irregular migrants based in Calais to reach the UK.¹⁶⁸ Other Big Brother Award ceremonies took place in 2007¹⁶⁹ and 2008.¹⁷⁰

The Novlang Award was invented by the French organisers to honour the creative use of language to hide the real meaning, accurately described in George Orwell's novel *1984* as "newspeak". The Director of the Criminal Investigation Department received the 2006 Novlang prize for encouraging the expansion of the collection of genetic data on the entire population.

Three French NGOs, IRIS, GISTI (an association defending the rights of migrants), and LDH (*Ligue des Droits de l'Homme*, or the French Human Rights League) have filed a complaint in December 2009 before the Conseil d'Etat to obtain the annulment of the "OSCAR" database. The three NGOs claim that the biometric nature of the data and the duration of its storage are arbitrary and disproportionate, given the purpose of the

¹⁶⁸ EDRI-gram, Number 7.7, 8 April 2009, "Big Brother Awards France 2009," available at <http://www.edri.org/edri-gram/number7.7/bba-france-2009>; see Big Brother Awards 2009, available at <http://bigbrotherawards.eu.org/-Big-Brother-Awards-2008-.html>.

¹⁶⁹ The 2007 Big Brother Awards, held in January, declared the winners to be the sub-prefect in charge of security in the Seine St. Denis neighborhood, where the Charles de Gaulle de Roissy airport is located since he, without cause or process, denied thousands of individuals the chance of employment because he suspected that they had terrorist associations. Sony-BMG received its award for having embedded "rootkit" spyware into its audio CDs. The Mayor of Ploërmel was given his award for his enthusiastic use of video surveillance (50 cameras in a village of 9,000 people). The Minister of Justice earned the Life Menace Award for his work on the sexual offender GPS tracking bracelet. See BBA France press release, 20 January 2007, available at <http://bigbrotherawards.eu.org/Palmares-2006-des-Big-Brother-Awards-France.html>.

¹⁷⁰ On 21 March 2008, Paris was host to the French Big Brother Awards for the year 2007. President Nicolas Sarkozy was excluded from the competition this year, because of his "genetic predisposition" for violating privacy and civil liberties. The 2007 jury had granted the State Award to the Constitutional Council for validating a safety imprisonment law that allows for the imprisonment of people considered dangerous by experts and not judges. The Corporate Award was granted to Taser France for its drone prototype "Quadri-France", surveillance equipment used mainly in rural areas. The Local Menace Award was granted to Claude Journès, president of Lyon II University for using students as a surveillance technology test subjects. The Orwell Newspeak Award was granted to the TV show *Envoyé Spécial* of France 2 for an unbalanced report about foreigners' expulsion procedures, and finally, Google Inc. received the Lifetime Menace Award – "who has no genetic excuses for their Big Brother-like behaviours." EDRI-gram, Number 6.6, March 26. 2008, "Big Brother Awards – France 2007," available at <http://www.edri.org/edri-gram/number6.15/50000-signatures-edvige>.

database, which is simply to manage the grant distribution to ensure that no one can claim it twice. It is disproportionate given the amount of the grant, which is minimal (€300).¹⁷¹

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

France ratified the Universal Declaration of Human Rights, which was proclaimed by the General Assembly on 10 December 10, 1948.¹⁷² On 4 November 1980, France ratified the International Covenant on Civil and Political Rights.¹⁷³

France is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)¹⁷⁴ and the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁷⁵ On 10 January 2006 France ratified the Council of Europe Convention on Cybercrime and its additional protocol against racism and xenophobia. Both texts entered into force in the country on 23 May 2006.¹⁷⁶ France is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

¹⁷¹ GISTI, IRIS & LDH, press release: Fichage biométrique des Roms. L'annulation du fichier Oscar par le Conseil d'État devient urgente" (Biometric Filing of Roma: the Conseil d'Etat Annulment of OSCAR File Becomes Urgent), 31 August 2010, available in French at <http://www.iris.sgdg.org/info-debat/comm-oscar0810.html>. See also Meryem Marzouki, "France: Imminent 'Humanitarian Fingerprinting' of Roma with OSCAR", EDRi-gram, no. 8.17, 8 September 2010, <http://www.edri.org/edriagram/number8.17/fingerprinting-roma-france-oscar>.

¹⁷² The Declaration was ratified through a proclamation by the General Assembly on 10 December 1948 with a count of 48 votes to none with only 8 abstentions. See Universal Declaration of Human Rights, 10 December 1948, available at <http://www.un.org/Overview/rights.html>.

¹⁷³ International Covenant on Civil and Political Rights, 16 December 1966, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

¹⁷⁴ Signed 28 January 1981; ratified 24 March 1983; entered into effect 1 October 1985.

¹⁷⁵ Signed 11 November 1950; ratified 3 May 1974; entered into effect 3 May 1974.

¹⁷⁶ Council of Europe. Convention on Cybercrime, CETS n° 185 available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=1&CL=ENG&NT=185>. Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, available at <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MAEJ0630050D>.

FEDERAL REPUBLIC OF GERMANY¹

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 10 of the Basic Law (or *Grundgesetz*, the German Constitution) states: "(1) Privacy of letters, posts, and telecommunications shall be inviolable. (2) Restrictions may only be ordered pursuant to a statute.² Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament."

In a 1983 case against a government census law, the Federal Constitutional Court formally acknowledged an individual's "right of informational self-determination," which is only limited by the "predominant public interest." The central part of the verdict stated, "Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situations knows about them."³ This landmark court decision derived the "right of informational self-determination" directly from Articles 1(1) and 2(1) of the Basic Law, which declare personal rights (*Persönlichkeitsrecht*) to freedom are inviolable. Attempts to amend the Basic Law to include a right to data protection were discussed after reunification, when the Constitution was revised, and were successfully opposed by the then-conservative political majority.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

Germany has one of the strictest data protection laws in the European Union. The world's first data protection law was passed in the German Land of Hessen in 1970. In 1977, a Federal Data Protection Act (*Bundesdatenschutzgesetz* or BDSG) followed, which was reviewed in 1990, amended in 1994 and 1997. The major revision in 2001 was used to adjust the BDSG to the EC

¹ The EPHR 2010 "Germany" report has been updated in October 2010 by Werner Hülsmann, Datenschutzconsulting (Konstanz, Germany), and completed by Kristina Irion and Cédric Laurant.

² Available at <http://www.gesetze-im-internet.de/englisch_gg/index.html>.

³ Federal Constitutional Court (Bundesverfassungsgericht) decision of 15 December 1983, reference number: 1 BvR 209, 269, 362, 420, 440, 484/83, available in German at <http://zensus2011.de/uploads/media/volkszaehlungsurteil_1983.pdf>.

Data Protection Directive.⁴ Some more revisions took place in 2006 and 2009. The general purpose of this Act is to protect the individual against his right to privacy being impaired through the handling of his personal data. The Act covers collection, processing and use of personal data by public federal authorities and state administrations (as long as there is no state regulation and insofar as they apply federal laws), and by private bodies, if they rely on data-processing systems or non-automated filing systems for commercial or professional use. The majority of federal statutes that have an impact on personal information and privacy contain references to the BDSG if they do not carry special sections on the handling of personal data themselves.

The 2001 revisions to the BDSG include regulations on personal data transfers abroad, video surveillance, anonymisation and pseudonymisation, smart cards, and sensitive data collection (relating to race or ethnic origin, political opinions, religious or philosophical convictions, union membership, health, and sexual orientation). It grants data subjects greater rights of objection. It also states that, apart from public bodies, private companies are now also required to appoint a data protection officer if they collect, process, or use personal information. Without this responsible person, each introduction of automated data processing must be registered with the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The BDSG also provides that consent from the individual whose data is collected is required after full disclosure of data collection and its consequences.

A general revision of the BDSG had been considered for 2005.⁵ Albeit an expert report on the modernization of the data protection law was published in 2001, there has been for a long time no visible legislative progress.⁶ This reputable report recommends reducing the number of laws governing specific details of privacy protections and creating one general statute, which would only refer to more detailed regulations where necessary.⁷ An ideal statute would provide general rules about the use of privacy-friendly techniques, data security, privacy standards, control of data processing, and self-regulation tools.⁸ On 17 February 2005, the German Parliament called upon the government to swiftly submit a draft for a Federal Data Protection Act incorporating these recommendations.⁹ The German Parliament (*Bundestag*) renewed its request for secondary legislation on auditing requirements.¹⁰

⁴ Federal Act on Data Protection ("BDSG"), 14 January 2003, last amended on 15 November 2006 (Bundesgesetzblatt, Part I, No 3, 16 January 2003, last amended on 15 November 2006), available at <http://www.bfdi.bund.de/cIn_030/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct.templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf>.

⁵ See Modernisierung des Datenschutzes: Öffentliche Anhörung des Innenausschusses (Modernisation of the data security: Public hearing of the interior committee), 6 March 2007, available at <http://www.bundestag.de/aktuell/archiv/2007/innen_kw10/index.html> (in German).

⁶ English summary available at <<http://www.datenschutz-berlin.de/recht/de/bdsg/summary-gutachten.pdf>>; Full version available at <http://www.bfdi.bund.de/cIn_134/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.html;jsessionid=E3DE6514718754590E66A6C4AC20BE70?nn=1091786> (in German).

⁷ *Id.*

⁸ *Id.*

⁹ German Parliament (Bundestag) decision of 17 February 2005, available at <<http://dip.bundestag.de/btd/15/045/1504597.pdf>>.

¹⁰ German Parliament (Bundestag) decision of 17 February 2005, available at <<http://dip.bundestag.de/btd/15/045/1504597.pdf>>; Response of the Federal Government from 26 January 2005 to the questionnaire of the Parliament, available at <<http://dip.bundestag.de/btd/15/047/1504725.pdf>> (in German).

Only minor modifications regarding the requirements for in-house data protection officers had been implemented in 2006. The threshold number of employees that would trigger a company data protection officer was raised from four to nine. This change has significant impact, because many small companies who were previously encouraged to have a privacy officer are no longer enticed by statute to have one. Further reforms, mainly regarding the use of credit scoring systems, data processing on behalf of a data controller by a data processor, the data subject's right of access to credit databases and the duty of companies to notify them or the public in case of a massive data loss, have been adopted in 2009 by the Cabinet of Ministers and the Parliament.¹¹

Due to several data breaches committed by discount retailers,¹² a call to reform the Employee Data Protection Rules has been discussed since 2008. A first article (§ 32, *Beschäftigtendatenschutz*, Employee Data Protection Rules) has been added in 2009 to the BDSG. This article, however, only incorporated applicable case law so that there are only minor changes about how to deal with employees' personal data. A more detailed draft of the Employee Data Protection Rules has been adopted in August 2010 by the Cabinet of Ministers, but that the Parliament has not adopted yet.¹³

Sector-based laws

All of the 16 states (*Bundesländer*) have their own specific data protection regulations that cover the public sector of the state administrations as well as the communal administration of each state. All states have adopted new data protection laws pursuant to the EC Data Protection Directive.¹⁴ Each state also has a data protection commissioner to enforce the state data protection acts.¹⁵ It falls within the competence of the state supervisory authorities for the non public sector¹⁶ to supervise the compliance of the non public sector with the Federal Data Protection Act. The federal and *state* data protection officers as well as the supervisory authorities for the non public

¹¹ Press release of the Federal Ministry of Interiors, 30 July 2008, available at <http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2008/07/Aenderung_BDSG.html>; See summary of the Federal Ministry of Interior, available at <<http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/ohneMarginalspalte/aktuelleaktivitaeten.html>> (in German).

¹² See Data Protection Authority of the Federal State of Baden-Württemberg, press release: "Datenschutzauufsichtsbehörden verhängen gegen Lidl-Vertriebsgesellschaften hohe Bußgelder wegen schwerwiegender Datenschutzverstöße," 11 September 2008, available at <<https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf>> (in German).

¹³ <<http://www.bundesrat.de/SharedDocs/Drucksachen/2010/0501-600/535-10.html>>.

¹⁴ For example <<http://bremen.beck.de/default.aspx?bcid=Y-100-G-brdsg-name-inh>> or <<http://beck-online.beck.de/?vpath=bibdata%2Fges%2FSaDSG%2Fcont%2FSaDSG.inh.htm>>.

¹⁵ Landesbeauftragte für den Datenschutz (the Representatives of the Länder's data protection authorities), available at <http://www.bfdi.bund.de/cln_136/EN/AdressesAndLinks/Landesdatenschutzbeauftragte/AnschriftenLandesdatenschutzbeauftragte.html?nn=408884>.

¹⁶ See <http://www.bfdi.bund.de/cln_136/EN/AdressesAndLinks/AufsichtsbehoerdenNichtOeffentlich/AnschriftenAufsichtsbehoerdenFuerDenNichtoeffentlichenBereich.html?nn=408884>.

sector hold conferences on a regular basis to exchange information and issue common statements.¹⁷

DATA PROTECTION AUTHORITY

The Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, or BfDI) is an independent federal agency that supervises the Federal Data Protection Act (BDSG) as well as the Federal Freedom of Information Act.¹⁸ Its chief duties include monitoring the compliance with the provisions of the BDSG by public bodies of the Federation as well as providers of telecommunications and postal services, receiving and investigating complaints, as well as submitting recommendations to parliament and other governmental bodies. The BfDI publishes a biannual activity report.¹⁹ However, the number of controllers is steadily decreasing as federal agencies, in compliance with the 2001 changes to the Act, appoint in-house data protection officers, as an alternative to registration under the Act.²⁰ The BfDI, which has 70 people on staff,²¹ handles about 5.516 written and oral complaints (an increase of 28 percent) and carries out approximately 75 investigations each year.²²

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In March 2004, the Federal Constitutional Court ruled²³ that significant portions of the Eavesdropping Law infringed the Constitution, or Basic Law, especially Article 1 on human dignity and Article 13 on the inviolability of private homes.²⁴ The court held that certain

¹⁷ See for a complete list of documents <http://www.bfdi.bund.de/cln_134/DE/Entschliessungen/DSBundLaender/DSBundLaender_node.html> (in German).

¹⁸ See Homepage <http://www.bfdi.bund.de/Vorschaltseite__EN__node.html>; English description of the duties of the Federal Data Protection Commissioner available at <http://www.bfdi.bund.de/cln_029/nn_670410/EN/Home/homepage__node.html__nnn=true>.

¹⁹ A list with all activity reports is available at <http://www.bfdi.bund.de/cln_134/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/Functions/TB_BfDI_table.html?nn=408924> (in German).

²⁰ E-mail from Ulrich Dammann, Bundesbeauftragter für den Datenschutz, to Christian Schröder, Law Clerk, Electronic Privacy Information Center, 4 April 2003 (on file with EPIC).

²¹ <http://www.bfdi.bund.de/cln_030/nn_531068/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2007/PM-15-07-Uebergabe21TB.html__nnn=true>.

²² Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI), Tätigkeitsbericht (Bi-Annual Report) 2005-2006, 24 April 2007 at 160, available at <http://www.bfdi.bund.de/cln_030/nn_531940/SharedDocs/Publikationen/Taetigkeitsberichte/21-Taetigkeitsbericht-2005-2006,templateId=raw,property=publicationFile.pdf/21-Taetigkeitsbericht-2005-2006.pdf>.

²³ Federal Constitutional Court (Bundesverfassungsgericht) decision of 3 March 2004, reference number: 1 BvR 2378/98, available at <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html> (in German).

²⁴ Basic Law for the Federal Republic of Germany, I. Basic Rights, Articles 1, 13, available at <<http://www.bundesregierung.de/en/Federal-Government/Function-and-constitutional-ba-,10222/I.-Basic-rights.htm>>.

communications are protected by an absolute area of intimacy wherein citizens can communicate privately without fear of government surveillance.²⁵ The German legislature was granted a transitional period until June 2005 to comply with the court's decision, and in May 2005 the German *Bundestag* passed new legislation to comply with the court decision.²⁶

(See more details under the "Wiretapping, access to, and interception of communications" section.)

In February 2008, in a landmark decision, the Federal Constitutional Court declared unconstitutional provisions of the North-Rhine Westphalia Law on the domestic intelligence service that allowed for secret online searches of private computers.²⁷ The Court interpreted the Basic Law (Articles 1 (1) and 2 (1)) as containing a fundamental right for every citizen to have the integrity and confidentiality of systems of information technology guaranteed by the state. The decision is considered to be the most important on privacy issues since the census decision of 1983.

(See more details under the "Wiretapping, access to, and interception of communications" section.)

After 34.000 people filed a case before the Federal Constitutional Court against the implementation of the EU Data Retention Directive (2006/24) into German law,²⁸ the Court issued a preliminary ruling on 11 March 2008 suspending the provisions of a new law that go beyond the Data Retention Directive.²⁹ A decision on the merits of the case, in particular on the constitutionality of data retention, did not occur until 2nd March 2010, when the Federal Constitutional Court declared unconstitutional the data retention and void the relevant section of the Telecommunications Act.³⁰

(See more details under the "Data retention" section.)

²⁵ C. Schröder, "Wiretap in Germany," German American Law Journal: American Edition (11 March 2004), available at <<http://www.recht.us/amlaw/2004/03/11>>.

²⁶ "Änderungen beim großen Lauschangriff", Das Parlament, Nr. 20 of 17 May 2005, available at <http://www.bundestag.de/dasparlament/2005/20/plenumundausschuesse/021.html> (in German).

²⁷ Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, available at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html> (in German); see also press release of the Federal Data Protection Commissioner available at <http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/07-08-OnlineSearches.html>.

²⁸ See German Working Group on Data Retention (*AK Vorrat*) website <<https://www.vorratsdatenspeicherung.de/content/view/51/70/lang,en/>>.

²⁹ Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 11 March 2008, reference number: 1 BvR 256/07, available (in German) at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html>. See also Federal Data Protection Commissioner, "The Federal Constitutional Court Reduces Constitutional Risk Posed by Data Retention for Later Use", press release, 19 March 2008, available at <http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/11-08-FederalConstitutionalCourtReducesSonstitutionalRisk.html>.

³⁰ Federal Constitutional Court (*Bundesverfassungsgericht*) - Press office, press release no. 11/2010 of 2 March 2010, available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html>>; decision: BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), available at <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> (in German).

The Federal Constitutional Court has ruled that the police may use GPS technology to track suspects driving motor vehicles in cases of serious crimes even without a judicial warrant.³¹ However, the Court stressed that Parliament had to monitor the fast technological developments in this field and may have to correct laws if the risks for fundamental rights caused by technical surveillance increase.

(See more details under the "Location privacy" section.)

The Federal Constitutional Court ruled that laws allowing police to indiscriminately scan automobile license plates using electronic surveillance devices, and match them against databases kept by law enforcement and state officials were unconstitutional.³² This does not foreclose completely the automatic number plate data recognition which would still be possible under narrowly described circumstances.

(See more details under the "Video surveillance" section.)

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Another important federal law in Germany is the G-10 Law, which imposes limitations on the secrecy of certain communications as provided in Article 10 of the Basic Law (*Grundgesetz*).³³ Under the G-10 Law, parliamentary control commissions, established on federal and *Länder*'s level, supervise the surveillance powers of intelligence agencies. As amended in 1994 by the Crime Fighting Law (*Verbrechensbekämpfungsgesetz*), the G-10 Law allows warrantless automated wiretaps of domestic and international communications by the national and states' Intelligence Services for purposes of protecting the freedom and the democratic order, preventing terrorism and illegal trade in drugs and weapons. In July 1999, the Federal Constitutional Court upheld the screening method authorized under the G-10 Law.³⁴ The Law was amended in 2001 to require that electronic communications service providers give intelligence agencies the means to

³¹ Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 12 April 2005, reference number 2 BvR 581/01, available at <http://www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html> (in German).

³² Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 11 March 2008, reference number 1 BvR 2074/05, press release available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-027.html>>. "The Hallmarks of a Totalitarian State," Spiegel Online, 3 December 2008, available at <<http://www.spiegel.de/international/germany/0,1518,541025,00.html>>.

³³ Available at <http://bundesrecht.juris.de/bundesrecht/g10_2001/gesamt.pdf> (in German).

³⁴ Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 14 July 1999, reference numbers: 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95.

monitor data as well as voice lines. DPAs complain that after a G-10 measure any notification of the person concerned is dispensable if the data is ready for deletion.³⁵

Service providers are legally compelled to request the name and address of new customers to which they allocate a telephone number, even though they only use prepaid services.³⁶ Telecommunications operators providing publicly available services are also mandated to provide – at their own expense – the technical facilities required to implement telecommunications interception for law enforcement purposes. The Telecommunications Interception Ordinance (*Telekommunikations-Überwachungsverordnung, TKÜV*) of November 3, 2005 issued by the German government under the Telecommunications Act of 2004 (TKG) lays out specific technical requirements for the implementation of lawful interception by providers of public electronic communications services.³⁷ Telephone monitoring has been on the increase since 1995, when there were 4,674 instances of monitoring, up to 35,329 in 2006.³⁸ Four out of five wiretappings monitor cell phones. This renewed rise of interventions in secret communications gives the Federal Commissioner for Data Protection and Freedom of Information (BfDI) great concern for data security. For years, the Commissioner has appealed to prosecution authorities to use this means sparingly.³⁹

According to a 2003 survey, 75 percent of conducted telephone wiretapping actions violated the law. In most instances of wiretapping, law enforcement agencies did not inform the subjects after the eavesdropping took place, contrary to what is stipulated by the law.⁴⁰

The so-called "*Grosser Lauschangriff*" ("Big Eavesdropping Attack") formed part of the Law for the Enhancement of the Fight against Organized Crime, which became effective in 1999, and was intended to provide the legal basis for law enforcement agencies to survey potential criminals. In April 1998, Article 13 of the Constitution (*Grundgesetz*) that provides for the inviolability of private homes was amended in order to allow police authorities to place bugging devices in private homes (provided there is a court order).

³⁵ 61. Conference of Data Protection Commissioners (*Konferenz der Datenschutzbeauftragten des Bundes und der Länder*), Düsseldorf, 8/9 May 2001. available at <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/61DSK-NovellierungDesG_10-Gesetzes.pdf?__blob=publicationFile> (in German).

³⁶ See Paragraph 111 Telecommunications Law (*Telekommunikationsgesetz, TKG*), available at <http://www.gesetze-im-internet.de/tkg_2004/_111.html> (in German).

³⁷ Telecommunications Interception Ordinance (*Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation, TKÜV*). Available at <<http://www.bmwi.de/BMWi/Navigation/Service/gesetze,did=24138.html>> (in German).

³⁸ Bundesnetzagentur, press release of 26 April 2007, "Telefonüberwachung: Keine Steigerung in 2006", available at <http://www.bundesnetzagentur.de/cln_1911/SharedDocs/Pressemitteilungen/DE/2007/070426StatistikUeberwachung.html?nn=107064> (in German).

³⁹ Press information 12/05 of the Federal Data Protection Commissioner (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) of March 31, 2005, "Telefonüberwachungen auch 2004 wieder stark gestiegen".

⁴⁰ See Backes, O. und Gusy, Ch. (2003). Wer Kontrolliert Die Telefonüberwachung? Eine Empirische Untersuchung Zum Richtervorbehalt Bei Der Telefonüberwachung, Verlag Peter Lang. "Dreiviertel aller Lauschangriffe rechtswidrig." Der Spiegel Online, 9 January 2003, available at <<http://www.spiegel.de/politik/deutschland/0,1518,229958,00.html>> (in German).

In March 2004, the German Federal Constitutional Court ruled⁴¹ that significant portions of the eavesdropping law infringed the Constitution, or Basic Law, especially Article 1 on human dignity and Article 13 on the inviolability of private homes.⁴² The court held that certain communications are protected by an absolute area of intimacy wherein citizens can communicate privately without fear of government surveillance.⁴³ This includes conversations with close family members, priests, doctors and defense attorneys, but excludes conversations about crimes that have already been committed or the planning of future crimes. However, to justify surveillance between the target and such persons of trust, competent law enforcement agency must show that "there is strong reason to believe that the content of conversation does not fall in the area of intimacy,"⁴⁴ and that the crime is "particularly serious."⁴⁵ Once a specially protected conversation begins, the eavesdropping must stop immediately and any recordings of that portion of the conversation must be erased. The German legislature was granted a transitional period until June 2005 to comply with the court's decision, and in May 2005 the German *Bundestag* passed legislation to comply with the court.⁴⁶

In 2001, the *Bundestag* (the German Parliament) passed a law that added to the Criminal Procedural Code (StPO) further means of investigation into electronic communications. It serves as the legal basis for police and law enforcement to access "telecommunications connection data" for the investigation of serious crimes.⁴⁷ The law took effect in January 2002 and requires telecommunications service providers to disclose data, such as time and duration of use, place of use and identifying numbers.

In February 2008, in a landmark decision, the Federal Constitutional Court declared unconstitutional provisions of the North-Rhine Westphalia Law on the domestic intelligence service (*Nordrhein-westfälisches Verfassungsschutzgesetz*) that allowed for secret online searches of private computers (*Online-Durchsuchung*).⁴⁸ The Court interpreted the German Constitution (Articles 1 (1) and 2 (1)) as containing a fundamental right for every citizen to have the integrity and confidentiality of systems of information technology guaranteed by the state ("*Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*") The

⁴¹ Federal Constitutional Court (Bundesverfassungsgericht) decision of 3 March 2004, reference number: 1 BvR 2378/98, available at <http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html> (in German).

⁴² Basic Law for the Federal Republic of Germany, I. Basic Rights, Articles 1, 13, available at <<http://www.bundesregierung.de/en/Federal-Government/Function-and-constitutional-ba-,10222/1.-Basic-rights.htm>>.

⁴³ C. Schröder, "Wiretap in Germany," German American Law Journal: American Edition (11 March 2004), available at <<http://www.recht.us/amlaw/2004/03/11>>.

⁴⁴ *Id.*

⁴⁵ University College of London, Faculty of Laws, Institute of Global Law, "German Legal News - Constitutional Law," available at <http://www.ucl.ac.uk/laws/global_law/legal-news/german/index.shtml?constitution>.

⁴⁶ "Änderungen beim großen Lauschangriff", Das Parlament, Nr. 20 of 17 May 2005, available at <<http://www.bundestag.de/dasparlament/2005/20/plenumundausschuesse/021.html>>.

⁴⁷ Paragraphs 100g and 100h of the Criminal Procedures Act (*Strafprozessordnung*), available at <<http://www.gesetze-im-internet.de/stpo/>> (in German).

⁴⁸ Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, available at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html> (in German); see also press release of the Federal Data Protection Commissioner available at <http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/07-08-OnlineSearches.html>.

decision is considered to be the most important on privacy issues since the census decision of 1983. However, the Court did not categorically rule out the possibility of secret online searches of computers by law enforcement agencies. However, such measures can only be justified under strict preconditions (such as a judicial warrant) and only where concrete facts indicate that there is an imminent threat to the life, physical integrity or liberty of persons, or to the foundations of the state or the existence of mankind. Furthermore, the exercise of such a secret information technology system search is subject to judicial oversight. Without those conditions, any regulation on online searches – at the federal and at the federal state (*Länder*) level - would be unconstitutional.⁴⁹

Meanwhile, the Federal Government was pushing through Parliament a bill to extend the powers of the Federal Office of Crime Prevention (*Bundeskriminalamt, BKA*) that has the power to secretly search private computers (so called "*Bundestrojaner*"). The preemptive online-search has been legally implemented in Article 20k of the Federal Office of Crime Prevention Act (*BKA-Gesetz*).⁵⁰ The Bill vests to the *Bundeskriminalamt* investigatory powers that used to be restricted to intelligence agencies. It will lead to the biggest restructuring of police authorities in Germany since 1949. It was then that the Allied Powers ordered a strict separation of police and intelligence agencies, learning from the experience with the Gestapo in World War 2 Nazi Germany. Police matters were also mandated to be under the jurisdiction of the federal states (*Länder*) rather than the Federation. These principles have already gradually been eroded before September 11, 2001 ("9/11"). In 2006 the Federal Constitution was amended to give the *Bundeskriminalamt* powers to fight international terrorism.

National security legislation

The G-10 Law imposes limitations on the secrecy of certain communications as provided in Article 10 of the Basic Law (*Grundgesetz*).⁵¹ As amended in 1994 by the Crime Fighting Law (*Verbrechensbekämpfungsgesetz*), the G-10 Law allows warrantless automated wiretaps of domestic and international communications by the national and states' Intelligence Services for purposes of protecting the freedom and the democratic order, preventing terrorism and illegal trade in drugs and weapons. (*See more information under the section "Wiretapping, access to, and interception of communications"*).

A new bill extended the powers of the Federal Office of Crime Prevention (*Bundeskriminalamt, BKA*) to secretly search private computers (so called "*Bundestrojaner*"). The preemptive online-search has been legally implemented in Article 20k of the Federal Office of Crime Prevention Act (*BKA-Gesetz*).⁵² (*See more information under the section "Wiretapping, access to, and interception of communications"*).

⁴⁹ Press release of the Federal Data Protection Commissioner (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) at <http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/07-08-OnlineSearches.html>; The Herald Tribune Europe Edition, 27 February 2008, <<http://www.iht.com/articles/2008/02/27/europe/german.php>>.

⁵⁰ Federal Office of Crime Prevention Act (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BKA-Gesetz*), Available at <http://www.gesetze-im-internet.de/bkag_1997/> (in German).

⁵¹ Available at <http://bundesrecht.juris.de/bundesrecht/g10_2001/gesamt.pdf> (in German).

⁵² Federal Office of Crime Prevention Act (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, BKA-Gesetz*), Available at <http://www.gesetze-im-internet.de/bkag_1997/> (in German).

On 2nd March 2010, Germany's data retention legislation has been declared unconstitutional by the Federal Constitutional Court.⁵³ (*See more information under the section "Data retention"*).

Data retention

In March 2006, the EU adopted the Data Retention Directive that mandates the retention of telecommunications data for a period of 6 months to 24 months.⁵⁴ The Directive has been implemented in Germany by amendments to the Telecommunications Act of 2007, which came into force on 1st January 2008.⁵⁵ It requires data retention for six months.⁵⁶ Access to retained data is given only with a warrant issued by a judge, and only if the authorities investigate a crime in the list enumerated in the proposal. However the list also covers offences not covered by the directive, such as those committed via telecommunication. This effectively would include the possibility to access the retained data also in cases of online copyright violations. At the same time a direct access of the data by the copyright holders had been discussed under the implementation of the EC law enforcement directive but was finally abandoned.⁵⁷

A significant public movement against data retention has been formed, with some thousand people attending demonstrations, and about 34.000 people have filed a case before the Federal Constitutional Court (*Bundesverfassungsgericht*), which is quite extraordinary, since the procedures do not allow for class action suits.⁵⁸ The *Arbeitskreis Vorratsdatenspeicherung* (German Working Group on Data Retention) is an association of civil rights campaigners, data protection activists and Internet users. The *Arbeitskreis* is coordinating the campaign against the introduction of data retention in Germany.

The Constitutional Court issued a preliminary ruling on 11 March 2008 suspending those provisions of the law that go beyond the Data Retention Directive.⁵⁹ On 2nd March 2010, the

⁵³ Federal Constitutional Court - Press office, press release no. 11/2010 of 2 March 2010, available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html>>; decision of 2 March 2010, available at <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> (in German).

⁵⁴ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006 P. 0054 – 0063, available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>>.

⁵⁵ Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 21.12.2007, Bundesgesetzblatt I, p. 3198; see also "Stellungnahme zum Regierungsentwurf für eine Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" of 20 June 2007, available at <http://wiki.vorratsdatenspeicherung.de/images/StN-E_19-06-2007.pdf> (in German).

⁵⁶ EDRI-Gram, Number 5.8, April 2007, available at <<http://www.edri.org/edriagram/number5.8/germany-data-retention>>.

⁵⁷ See netzpolitik.org, „Vorratsdatenspeicherung und Urheberrechts-Auskünfte“, of 24 November 2007, available at <<http://www.netzpolitik.org/2007/vorratsdatenspeicherung-und-urheberrechts-auskuenfte/>> (in German).

⁵⁸ See AK Vorrat, „Sammel-Verfassungsbeschwerde gegen die Vorratsdatenspeicherung“, <<http://www.vorratsdatenspeicherung.de/content/view/51/1/lang,de/>> (in German).

⁵⁹ Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 11 March 2008, reference number: 1 BvR 256/07, available (in German) at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html>. See also Press release of the Federal Data Protection Commissioner at <http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/11-08-FederalConstitutionalCourtReducesConstitutionalRisk.html>.

Federal Constitutional Court declared unconstitutional the data retention and void the relevant section of the Telecommunications Act.⁶⁰ The Federal Constitutional Court's decision does not rule out the possibility to introduce data retention schemes in principle though. Significant would be that the data "is not directly retained by the state, but that it is realized through a commitment of private service operators".⁶¹ Moreover, such storage would require "sufficiently sophisticated legislation with well-defined provisions on data security, data use, transparency and legal protection".⁶² As a consequence of this decision all retained telecommunications traffic data has to be deleted without undue delay and can not anymore be transferred to law enforcement agencies.⁶³ For the time being there is in Germany no legal basis for data retention.

National databases for law enforcement and security purposes

In April 1998, a law was passed that allows the *Bundeskriminalamt* (Federal Police) to run a nationwide database of genetic profiles related to criminal investigations and convicted offenders.⁶⁴

No more has been reported.

National and international data disclosure agreements

Nothing has been reported.

Cybercrime

Nothing has been reported.

Critical infrastructure

Nothing has been reported.

⁶⁰ Federal Constitutional Court (*Bundesverfassungsgericht*), press release no. 11/2010 of 2 March 2010, available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html>>; decision: BVerfG, 1 BvR 256/08 of 2 March 2010, , available at <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> (in German).

⁶¹ Federal Constitutional Court, press release of 2 March 2010.

⁶² *Id.*

⁶³ *Id.*

⁶⁴ "New Powers for the Border Police: Checks Anywhere at Any Time," *Fortress Europe*, FECL 56 (December 1998), available at <<http://www.fecl.org/circular/5605.htm>>.

INTERNET & CONSUMER PRIVACY

On 29 April 2010, the Düsseldorf Kreis, an informal group of German federal state data protection authorities, published a decision⁶⁵ clarifying some due diligence responsibilities for German companies that export personal data to US companies that have self-certified themselves under the EU-US "Safe Harbour" Agreement.⁶⁶ One of the due diligence requirements is for German companies exporting personal data to the United States to check if the US data importer does indeed comply with the Safe Harbor Framework.⁶⁷

On December 1, 2010, the Minister of Interior Thomas de Maizière presented a draft law intended to improve data protection and the protection of individual rights from serious infringements in the Internet.⁶⁸ The draft law proposes to introduce regulation of individual profiling for which personal data from online services has been collected and combined for commercial purposes and define a "red line" which would require expressive and informed consent of the person concerned.

E-commerce

Direct marketing issues are addressed by Section 7 of the German Unfair Competition Act.⁶⁹ According to its general clause, it is unfair to annoy market players, *e.g.*, consumers, inappropriately. By default this applies to clearly unwanted advertisements, unsolicited commercial phone calls, marketing methods making use of automated calling machines, fax machines or e-mail (spam) without prior consent, and any direct marketing that cannot be linked back to the senders' identity. Direct marketing via e-mail is not prohibited as spam under the conditions that (1) an organization has received the e-mail address in the context of selling goods or services to the customer; (2) the organization uses the e-mail contact for marketing of very similar products and services; (3) the customer has not opposed the use of his e-mail for further direct marketing; and (4) at the time of the collection and each usage of the e-mail address clearly sets out the right to opt-out from direct marketing via e-mail. Cold calling of consumers is a

⁶⁵ Düsseldorf Kreis, "Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 28./29. April 2010 in Hannover", 28-29 April 2010, available at <http://securitybreaches.files.wordpress.com/2010/12/100428_29-dusseldorfer_kreis_decision.pdf> (in German). English version: "Supreme Supervisory Authorities for Data Protection in the Nonpublic Sector (Germany), Examination of the Data Importer's Self-Certification According to the Safe-Harbor Agreement by the Company Exporting Data (revised version of Aug. 23, 2010), available at <http://www.datenschutzberlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129>.

⁶⁶ US Department of Commerce, "Safe Harbor" website <<https://www.export.gov/safeharbor/>>.

⁶⁷ For more details, see Marie-Andrée Weiss & Cédric Laurant, "The Safe Harbor Framework: not a 'Safe Harbor' anymore for US Companies? German Expert Body Insists on Stronger Compliance Stance". Information Security Breaches & The Law Blog, 9 July 2010 <http://blog.security-breaches.com/2010/07/09/safe_harbor_framework_not_a_safe_harbor_anymore_for_us_companies/> and Willkie Farr & Gallagher, "German Authorities Issue Privacy Decision Clarifying Due Diligence That Must Be Conducted on Companies Using the Safe Harbor Framework to Transfer Personal Data to the U.S.", 17 June 2010, available at <http://www.willkie.com/files/tbl_s29Publications%5CFileUpload5686%5C3392%5CGerman%20Authorities%20Issue%20Privacy%20Decision.pdf>.

⁶⁸ See "Datenschutz im Internet – Gesetzentwurf des BMI zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht". Available at <http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile> (in German).

⁶⁹ The German Act Against Unfair Competition, available at <http://www.gesetze-im-internet.de/englisch_uwg/index.html>.

violation of Unfair Competition Law⁷⁰ and, since 2009, a misdemeanor that is punishable by a fine up to 50.000 EUR.

The Telemedia Act (TMG) was passed in March 2007, and applies to all electronic information and communications services which are not merely concerned with the conveyance of signals.⁷¹ Telemedia service providers must inform users about the "character, extent and reason" of the collection and processing of user-related data. Service providers are required under the TMG to produce user data, such as user names or addresses, upon request of the German secret services. Further, user data may be demanded if necessary for the enforcement of intellectual property rights.⁷²

Cybersecurity

Nothing has been reported.

Online behavioural marketing and search engine privacy

Nothing has been reported.

Online social networks and virtual communities

Mid 2010, Hamburg's Data Protection Commissioner has launched an investigation against Facebook and its Friend Finder application which provides for the synchronization of email and mobile phone address books.⁷³ In a nutshell, the practice to process entries with personal data of people who don't use the respective social networking site was scrutinized in the light of the applicable German data protection legislation. On January 22, 2011, Facebook made concessions which address the privacy concerns by giving every Facebook member transparent control over the addresses he or she imports into the network and to whom invitations to join the social network will be sent.⁷⁴ It is unclear whether the changes will be introduced only for the German Facebook services or across the platform.

⁷⁰ *Id.*

⁷¹ For example "webshops, mobile commerce, newsgroups, music download platforms, video on demand (VOD), internet search engines, emails and even simple company websites, but not to live-streaming of video, web-casting, IPTV (Internet Protocol TV) or VoIP (Voice Over Internet Protocol - internet telephony)." See Henning Kreig, "German Telemedia Act introduces new rules for New Media," Bird & Bird Articles, 5 March 2007, available at <http://www.twobirds.com/english/publications/articles/German_Tele_Media_Act_new_rules.cfm>.

⁷² *Id.*

⁷³ EDRIgram of July 14, 2010: "Facebook Faces Serious Fines In Germany". Available at <<http://edri.org/edriagram/number8.14/facebook-germany-investigation-dpa>>.

⁷⁴ See press release of Hamburg's Data Protection Commissioner of 24 January 2011: „Facebook ändert Verfahren des Friend-Finding Verbesserungen für den Datenschutz vereinbart“, available at <http://87.106.89.173/2011-01-24_Facebook.pdf> (in German); Spiegel Online International of January 22, 2011: "Facebook Agrees to Change 'Friend Finder' Feature". Available at <<http://www.spiegel.de/international/business/0,1518,741027,00.html>>.

Online youth safety

Children and youth data protection is not separately regulated but the general data protection framework applies. Many initiatives concentrate on awareness raising and empowerment of young Internet users.⁷⁵ Certain social network sites operating in Germany such as Facebook and VZNet have signed the EU Safer Social Networking Principles which aim at enhancing the protection of child users on this platforms.⁷⁶

TERRITORIAL PRIVACY

Photographic and video surveillance

In 2004, a new regulation of the German Criminal Code (§201a StGB) took effect. This regulation protects private life against the invasion of privacy by the taking of pictures of persons in their apartments or other protected areas, *e.g.*, changing cabins. Furthermore, publishing and distribution of such photographs on the Internet is punishable as a criminal offense.

On 12 April 2002 the motorway toll law (*Autobahnmautgesetz, ABMG*) came into effect, which contains significant data protection requirements pertaining to the collection and control of the toll levied on lorries in Germany.⁷⁷ For this purpose two types of movement data are used, on the one hand traffic data (route, amount of the toll, license plate number of the lorry, place and time of the payment) and on the other hand control data (image and license plate number of the lorry, size and type of the lorry, place and time of tolled motorway use).⁷⁸ These data can be used and processed exclusively for the purpose of the toll. Any access by law enforcement authorities for criminal investigations is inadmissible, which is frequently challenged from politicians.⁷⁹ In principle, the infrastructure for automated toll collection and control would be capable to monitor traffic and search vehicles. The Federal Government (*Bundesregierung*) recently stated that it is not aware of any access by law enforcement to information of the toll system.⁸⁰

Independently from the toll system, in the State of Hessen and Schleswig Holstein the new Police Laws permitted the electronic scanning of vehicles' number plates that are then automatically

⁷⁵ See for example <<https://www.klicksafe.de>>.

⁷⁶ See for further information <http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm>.

⁷⁷ Motorway Toll Act for Heavy Commercial Trucks (*Autobahnmautgesetz, ABMG*), available at <<http://www.gesetze-im-internet.de/abmg/>> (in German). Operator is the Toll Collect GmbH, see <http://en.wikipedia.org/wiki/Toll_Collect>.

⁷⁸ The Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI*): „Die LKW-Maut“. Available at <http://www.bfdi.bund.de/cln_136/DE/Themen/WirtschaftUndFinanzen/Verkehr/Artikel/LkwMaut.html?nn=409802> (in German).

⁷⁹ *Id.*

⁸⁰ Response of the Federal Government from 26 January 2005 to the questionnaire of the Parliament, available at <<http://dip.bundestag.de/btd/15/047/1504725.pdf>> (in German), at 30 (in German).

matched with a database of searched vehicles.⁸¹ Nevertheless, on 11 March 2008, the Federal Constitutional Court ruled that laws allowing police to indiscriminately scan automobile license plates using electronic surveillance devices, and match them against databases kept by law enforcement and state officials were unconstitutional.⁸² In both cases there is a lack of designation of the purpose of automatic number plate data recognition, which coincides with an unconstitutional lack of determinedness regarding collectable information and does not comply with the proportionality principle.⁸³ This does not foreclose completely the automatic number plate data recognition which would still be possible under narrowly described circumstances.

There are several other video surveillance projects in Germany that have generated not only a response from privacy and data protection advocacy groups. For example, in Weimar, Germany, a local newspaper protested the installation of video surveillance cameras that watched the entrance of a newspaper building (along with medical and political offices), and the local government eventually uninstalled the cameras.⁸⁴ Public debate on camera observation was heightened by the revelation that a museum's security camera could see into chancellor Angela Merkel's private flat in Berlin. Upon discovery, the mechanism of the camera was changed to reduce the angle of observation.⁸⁵

In February 2007, the Federal Constitutional Court declared illegal a video surveillance scheme in the city of Regensburg where the site of a former synagogue (destroyed by the Nazis) was to be put under video surveillance to prevent vandalism.⁸⁶ The Court stressed the freedom of individuals to freely walk the streets and places and not to be put under surveillance without good reason. In Regensburg the city had based the video surveillance on the general provisions of the State Data Protection Act, which however did not determine with sufficient clarity the purpose and limits of such measures in order to rely on this legal basis for the video surveillance. The Bavarian Police Act (unlike Police Acts in most other German Länder) did not contain provisions on preventive video surveillance when the case came before the Constitutional Court.

Location privacy (GPS, mobile phones, location based services, etc.)

As prescribed by EC Directive on Privacy and Electronic Communications, the TKG 2004 sets out the requirements of the processing of location data, either anonymously or with the

⁸¹ Heise News of 15 December 2004, "Hessen dehnt Polizeibefugnisse deutlich aus," available at <<http://www.heise.de/newsticker/meldung/54298>> (in German).

⁸² Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 11 March 2008, reference number 1 BvR 2074/05, press release available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-027.html>>. Der Spiegel online, "The Hallmarks of a Totalitarian State," Spiegel Online, 3 December 2008, available at <<http://www.spiegel.de/international/germany/0,1518,541025,00.html>>.

⁸³ *Id.*

⁸⁴ Peter Nowak, "Weimarer Provinzposse mit Kamera," Telepolis, 27 October 2003, available at <<http://www.heise.de/tp/deutsch/inhalt/te/15950/1.html>> (in German).

⁸⁵ "Wachleute filmten heimlich Merkels Wohnzimmer", Spiegel online of 26 March 2006, available at <<http://www.spiegel.de/politik/deutschland/0,1518,408015,00.html>> (in German).

⁸⁶ Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 23 February 2007, reference number 1 BvR 2368/06, press release available at <<http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg07-031.html>> (in German).

subscriber's consent, for the provision of location based services.⁸⁷ It is upon the subscriber to inform any co-users of all such consent given. In the case of "Track your Kid" services parents consent to give up their child's data protection because they are the subscribers, whereas the child is the user of the mobile phone.⁸⁸ Apart from content, all positive and negative (e.g. the unsuccessful attempt to call) circumstances of telecommunications are protected as telecommunications privacy. Service providers are required to protect their users' personal data and telecommunications privacy. The collection and use of traffic data is strictly limited to: (1) the purposes of charging and billing, (2) remedy malfunctions in telecommunications systems, and (3) detect telecommunications service fraud and, (4) to market and customize services to service providers' subscribers, as well as to provide value-added services *with the consent of the data subject*.

Germany also implemented in the Criminal Procedures Law (*Strafprozessordnung, StPO*) the possibility of using a so-called IMSI-Catcher system to track individuals through the location of their cell phones. The law, which entered into force on August 14, 2002, provides law enforcement with the ability to obtain, upon court request and from the time it is granted, the data of individuals' movements and their cell phone device number (IMEI number - International Mobile Equipment Identity) for a period of up to six months.⁸⁹ The location of a mobile phone can further be conducted with silent SMS that is covered by general investigation powers in criminal cases.⁹⁰ Silent SMS means that an empty message is sent to a mobile phone, which allows for some approximation of its whereabouts, but it does not report itself to the respective user.

The Federal Constitutional Court (*Bundesverfassungsgericht*) has ruled that the police may use GPS technology to track suspects driving motor vehicles in cases of serious crimes even without a judicial warrant.⁹¹ The Court approved §100c StPO to be consistent with the Constitutional principle of clarity and definiteness and when allowing police to use "all technical observational means" to investigate suspicious behaviour that might be considered a crime of substantial significance. However, the Court stressed that Parliament had to monitor the fast technological developments in this field and may have to correct laws if the risks for fundamental rights caused by technical surveillance increase. Parliament also has to ensure by procedural rules that law enforcement agencies (e.g. from different Länder or the Federal level) do not subject citizens to uncoordinated surveillance measures. The "additive effect" on fundamental rights has to be kept in mind.

⁸⁷ Telecommunications Act 2004, available at <http://www.bfdi.bund.de/cln_030/nn_946430/EN/DataProtectionActs/Artikel/TelecommunicationsAct-TKG,templateId=raw,property=publicationFile.pdf/TelecommunicationsAct-TKG.pdf>.

⁸⁸ Response of the German government (Bundesregierung) of 26 January 2005, to parliamentary question, reference number (Drucksache) 15/4725, available at <<http://dip.bundestag.de/btd/15/047/1504725.pdf>> (in German).

⁸⁹ 19. Tätigkeitsbericht – 2001/2002 at 54-55, available at <<http://www.bfd.bund.de/information/19tb0102.pdf>> (in German).

⁹⁰ Response of the Federal Government from 26 January 2005 to the questionnaire of the Parliament, available at <<http://dip.bundestag.de/btd/15/047/1504725.pdf>> (in German).

⁹¹ Federal Constitutional Court (*Bundesverfassungsgericht*), decision of 12 April 2005, reference number 2 BvR 581/01, available at <http://www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html> (in German).

In 2005, a new system to electronically collect tolls for trucks using the national highways was launched.⁹² The system tracks vehicles through GPS (Global Positioning System) and cellular phone networks. According to a common standpoint of the DPAs in 2001⁹³, the Federal government implemented special data protection measures in the laws governing toll systems: data collection and processing is limited only for the purpose of billing; all data must be deleted after the payment; and all data collected from vehicles that are not subject to a toll must be immediately deleted.⁹⁴ After a series of murders allegedly committed by the same offender, there are now plans by the government to abolish these restrictions.⁹⁵ If law enforcement could have access to the data, the existing infrastructure would enable the monitoring of the movement of almost all cars and trucks on German highways.

The introduction of Google's Street View service has sparked public controversy⁹⁶ and the competent supervisory authority, *i.e.* Hamburg's Data Protection Commissioner (*Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*), has started investigations into the admissibility of the service under German data protection laws. Individuals have the possibility to object electronically or in writing against the publication of private premises, houses and flats. Until October 22, 2010, Google reported a total of 244.237 opt-outs which equals nearly 3 percent of households in Germany's 20 largest cities for which Google's Street View service was launched in 2010.⁹⁷ Where an opt-out has been declared Google has to pixel the concerned premise's image.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

In May 1998, the *Bundespolizei* (Border Protection Forces), originally a federal border police force but now responsible for securing and controlling borders, as well as working in foreign

⁹² Based on the Motorway Toll Act for Heavy Commercial Trucks (*Autobahnmautgesetz, ABMG*), available at <<http://www.gesetze-im-internet.de/abmg/>> (in German).

⁹³ 62. Conference of the Data Protection Commissioners of the Federation and the Länder (*Konferenz der Datenschutzbeauftragten des Bundes und der Länder*), Resolution „Lkw-Maut auf Autobahnen und allgemeine Maut auf privat errichteten Bundesfernstraßen“, Münster, 24.-26. October 2001, available at <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/62DSK-Lkw-MautAufAutobahnenUndAllgemeineMautAufPrivatErrichtetenBundesfernstrassen.pdf?__blob=publicationFile> (in German).

⁹⁴ Based on the Motorway Toll Act for Heavy Commercial Trucks (*Autobahnmautgesetz, ABMG*), available at <<http://www.gesetze-im-internet.de/abmg/>> (in German).; Response of the Federal Government from 26 January 2005 to the questionnaire of the Parliament, available at <<http://dip.bundestag.de/btd/15/047/1504725.pdf>> (in German).

⁹⁵ The Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI*): „Die LKW-Maut“. Available at <http://www.bfdi.bund.de/cln_136/DE/Themen/WirtschaftUndFinanzen/Verkehr/Artikel/LkwMaut.html?nn=409802> (in German).

⁹⁶ See EDRIgram Number 8.9, 5 May 2010: “UK And Germany Question The Data Collected By Google Street View”. Available at <<http://edri.org/edriagram/number8.9/google-street-view-wifi-germany-uk>>.

⁹⁷ See Google's blogpost; “How many German households have opted-out of Street View?”. Available at <<http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html>>.

embassies, received permission to check persons' identities and baggage without any concrete suspicion.⁹⁸

Germany was among the first states in the EU to introduce the new biometric passports, following the EU Council Regulation on standards for security features and biometrics in passports and travel documents issued by the Member States.⁹⁹ Since November 1, 2005, the German passports contain RFID (Radio Frequency Identification) chips with facial images, and beginning 1st November 2007, the chips also include fingerprints. After much debate between the ruling coalition parties (Social Democrats and Christian Democrats), it was decided to store the fingerprint data neither in a central nor in local databases. Subsequent to the production of the passport, the manufacturer and local authorities are obliged to delete the data. Furthermore, this also applies after every verification process. Apart from the short-term processing of the data in specific control situations, the fingerprints are thus only to be stored in the German passport itself and not in any databases of public authorities.

National ID & smart cards

More recently the Federal Government has adopted a bill, still under discussion, to introduce ID cards (*Personalausweise*) with the option to have digitized fingerprints included on a voluntary basis. The original plan of the Federal Home Secretary to include digitized fingerprints on a compulsory basis met with strong public opposition. The crucial question is whether people who reject fingerprints on their identity card will be at a disadvantage.¹⁰⁰ In Germany there is a general duty for each individual to have an ID card (as opposed to passports).

RFID tags

RFID chips, when queried by a radio device, would respond by transmitting a unique ID code. Under § 6(c) of the BDSG, notice must be provided to data subjects of communications with "intelligent" RFID (devices with integrated processors), thus prohibiting secret reading or writing of personal information. However, Germany does not yet have any regulations specifically addressing "non-intelligent" RFID, which still create a privacy risk, as they can be linked to personal information held elsewhere without violating § 6(c).

In May 2003, the German retail giant Metro started a trial project to introduce a new cashing and customer convenience program with small chips, called Radio Frequency Identification (RFID) chips, at their Metro Future Store. The chips were to be attached to all products. It therefore would have allowed customers to pay and check out automatically by pushing a loaded trolley past a sensor. Combined with an automatically readable customer client card, the system would

⁹⁸ "New Powers for the Border Police: Checks Anywhere at Any Time," *Fortress Europe*, FECL 56 (December 1998). Available at <<http://www.fecl.org/circular/5605.htm>>.

⁹⁹ Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *Official Journal* 2004 L 385, p.1.

¹⁰⁰ Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*), „Neuer Personalausweis: Sie haben die Wahl!“, Bonn/ Berlin, 29 October 2010. Available at <http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2010/45_NeuerPA.html> (in German).

have allowed the tracking of all purchases and linking to the customer's identity.¹⁰¹ Metro claimed that the RFID chips could easily be deactivated, thus erasing any privacy invasions, but their process for deactivation leaves intact the unique identifying number on the RFID chip, so even "deactivated" cards can be traced back to their origin.¹⁰² In March, 2004, Metro halted the trial program in response to protests from digital rights groups regarding possible privacy violations.¹⁰³ In a speech, the Federal Data Protection Commissioner pointed out the privacy implications of RFID, and called on the legislature to make provisions on RFID tags.¹⁰⁴

RFID-chipped tickets for the 2006 Football World Cup in Germany enabled authorities to track the movements of the individualized spectator during the event.¹⁰⁵ The application forms for tickets required a large number of personal information, *i.e.* passport number, nationality, and day of birth. This was subsequently upheld by the courts.¹⁰⁶

Bodily Privacy

In 2004, a new regulation of the German Criminal Code (§201a StGB) took effect. This regulation protects private life against the invasion of privacy by the taking of pictures of persons in their apartments or other protected areas, *e.g.*, changing cabins.

Since September 2010 the Hamburg airport operates two body scanners in a government initiated pilot to test the technology for six months.¹⁰⁷ Passengers can decide whether to pass the security control with the body scanners. The use of the technology is controversial due to interferences with the intimacy of an individual's body and the exposure to radiation on the one hand and on the other hand the ability to enhance the security is questionable.

Workplace Privacy

New employee data protection rules has been discussed since 2008. A first article (§ 32, *Beschäftigendatenschutz*, Employee Data Protection Rules) has been added in 2009 to the

¹⁰¹ "Retail Future: Painless Checkout, Knowing Scanners," Reuters, 14 May 2003 <http://www.forbes.com/home_europe/newswire/2003/05/14/rtr970418.html>.

¹⁰² E-mail from Bettina Winseman, Staff Member, STOP1984, to EPIC, 12 July 2004.

¹⁰³ "German Revolt Against RFID", The Register, 1st March 2004, available at <http://www.theregister.co.uk/2004/03/01/german_revolt_against_rfid/>.

¹⁰⁴ Peter Schaar, Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*), "Datenschutz als Verbraucherschutz: Neue Herausforderungen am Beispiel von Smart Chips und Kundenkarten," 5 April 2004, available at <http://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzUndVerbraucherschutzVorNeuenHerausforderungen.pdf?__blob=publicationFile> (in German).

¹⁰⁵ Monika Ermert, "World Cup 2006 'Abused for Mega-surveillance Project', The Register of 8 February 2005, available at <http://www.theregister.co.uk/2005/02/08/world_cup_2006_big_brother_charges/>.

¹⁰⁶ Decision of September 1, 2006, 2-01 S 111/06.

¹⁰⁷ Federal Ministry of the Interior (*Bundesministerium des Inneren*) press release of September 27, 2010 : "Start des Probebetriebs für den Körperscanner" Available at <http://www.bmi.bund.de/cln_165/SharedDocs/Pressemitteilungen/DE/2010/mitMarginalspalte/09/koerperscanner.html?nn=109632> (in German).

BDSG. A more detailed draft of the Employee Data Protection Rules has been adopted in August 2010 by the Cabinet of Ministers, but that the Parliament has not adopted yet.¹⁰⁸

Article 19 of the Genetic Diagnostic Law (*Gendiagnostikgesetz*) bans the request of genetic examinations or the use of results from genetic examinations before or during employment relationships.¹⁰⁹

The Federal Labour Court (*Bundesarbeitsgericht*) ruled that the use of biometrics at entrance controls of workplaces is subject to compulsory employee participation (*Mitbestimmung*) and thus only legal after approval of the respective workers' council or arbitration board.¹¹⁰ Importantly, this also applies if the biometric system is placed at the premises of a third party (e.g. the customer of a service company), when the employer instructs his/her employees to use the system.

HEALTH & GENETIC PRIVACY

Health privacy

Since 2005, *gematik*, a joint venture of doctors', hospitals, pharmacies' and health insurances' associations, is responsible for the development and introduction of the electronic health card (*elektronischen Gesundheitskarte, eGK*) and supporting infrastructure in Germany.¹¹¹ In November 2009, the Federal Ministry of Health put the roll-out of the electronic health card temporarily on hold out of data security concerns mainly raised by doctors.¹¹² The new priorities are a secure patient data management system and a voluntary possibility to store emergency data; other applications have to prove its utility, practicability and security.

Genetic privacy

In April 1998, a law was passed that allows the *Bundeskriminalamt* (Federal Police) to run a nationwide database of genetic profiles related to criminal investigations and convicted offenders.¹¹³

¹⁰⁸ <<http://www.bundesrat.de/SharedDocs/Drucksachen/2010/0501-600/535-10.html>>.

¹⁰⁹ Law on Genetic Examinations of Humans (*Gesetz über genetische Untersuchungen bei Menschen*). Available at <<http://www.gesetze-im-internet.de/gendg/index.html>> (in German).

¹¹⁰ Federal Court for Employment (*Bundesarbeitsgericht*), 1 ABR 7/03, 24 January 2004, available at <http://www.judicialis.de/Bundesarbeitsgericht_1-ABR-7-03_Beschluss_27.01.2004.html> (in German).

¹¹¹ See at <<http://www.gematik.de/cms/de/startseite/index.jsp>>.

¹¹² See Heise online, November 19, 2009: "Elektronische Gesundheitskarte: Abgespeckt bis aufs Gerippe". Available at <<http://www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Abgespeckt-bis-aufs-Gerippe-863578.html>> (in German).

¹¹³ "New Powers for the Border Police: Checks Anywhere at Any Time," Fortress Europe, FECL 56 (December 1998), available at <<http://www.fecl.org/circular/5605.htm>>.

In 2009, the German Parliament passed the Genetic Diagnostic Law (*Gendiagnostikgesetz*) which covers genetic examinations for medical purposes, clarifications of parentage and descent as well as in the insurance and employment sector.¹¹⁴ The law is founded on the principle of informational self-determination which comprises also the right not to know. Article 18 concerns the genetic examinations and the use of its results in the insurance sector which is with a few exceptions unlawful. Article 19 of the law bans the request of genetic examinations or the use of results from genetic examinations before or during employment relationships.

Financial Privacy

In Germany, financial privacy (so called *Bankgeheimnis*) is not especially codified but acknowledged as customary law. Banks and other financial institutions have a duty of confidentiality about the financial affairs of their customers. In 2002, new legislation imposes an obligation on banks and financial institutions to set up a new database which allows for automated access to customer information by the competent financial supervisory authority *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)*.¹¹⁵ German authorities have acquired datasets revealing German citizens bank account information abroad, in particular of banks in Lichtenstein and Swizz (so called “*Steuerstünder-CDs*”). According to a decision of the Federal Constitutional Court (*Bundesverfassungsgericht*) the use of these personal data for law enforcement is permissible even if the acquisition has not been lawful.¹¹⁶

E-Government & Privacy

The Federal Data Protection Act (*Bundesdatenschutzgesetz*) and data protection laws of the Länder apply to e-government services. The delivery of public services online can in addition fall in the scope of application of specialized laws regulating the processing of personal data in telecommunications and telemedia services.¹¹⁷

¹¹⁴ Law on Genetic Examinations of Humans (*Gesetz über genetische Untersuchungen bei Menschen*). Available at <<http://www.gesetze-im-internet.de/gendg/index.html>> (in German).

¹¹⁵ Federal Commissioner for Data Protection and Freedom of Information (*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*), “Kontenabrufverfahren - Staatliche Überwachung von privaten Konten “. Available at <http://www.bfdi.bund.de/cln_134/DE/Themen/WirtschaftUndFinanzen/Kredit-undVersicherungswirtschaft/Artikel/KontenabrufverfahrenVonPrivatenKonten.html?nn=409796> (in German).

¹¹⁶ See press release of the Federal Constitutional Court (*Bundesverfassungsgericht*) of November 30, 2010. Available at <<http://www.bverfg.de/pressemitteilungen/bvg10-109.html>> (in German).

¹¹⁷ See Working Party eGovernment of the Conference of the Data Protection Commissioners of the Federation and the Länder (*Arbeitsgruppe "eGovernment" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*): “Datenschutzgerechtes eGovernment”. Available at <http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/eGovernment.pdf?__blob=publicationFile>(in German).

OPEN GOVERNMENT

On 1st January 2006, the Federal Freedom of Information (FOI) Act entered into force,¹¹⁸ thereby closing the gap in transparency between Germany and all other Member States of the European Union (except Cyprus, Luxembourg, and Malta). FOI legislation had been proposed for five years but the administration had been reluctant to agree on a draft statute. Eventually, Members of Parliament from the ruling coalition parties grew impatient for a draft and presented their own.¹¹⁹ The draft was followed by an intense debate in the German Parliament (*Bundestag*) and among legal scholars that particularly focused on the exceptions included in the Act. Much criticism focused on the fact that information can be rather easily excluded from disclosure on grounds of public security and fiscal interests of the government. Personal data will only be disclosed if the information interest outweighs the interest of the data subject. Importantly, information containing intellectual property or business secrets is completely excluded from the ambit of the Act. The Federal Commissioner for Data Protection and Freedom of Information enforces the FOIA Act.¹²⁰

10 of the *Länder* already have their own FOI laws in effect.¹²¹ The *Land* of Brandenburg has the right of access to governmental records in its constitution and adopted a FOI law in 1998.¹²² Later, Berlin, Schleswig-Holstein, Nordrhein-Westfalen, Hamburg, Bremen, Mecklenburg-Vorpommern, Saarland, Sachsen-Anhalt and Thüringen also adopted FOI laws.

Other Recent Factual Developments (with an impact on privacy)

There is nothing to report under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

A significant public movement against data retention has been formed, with some thousand people attending demonstrations, and about 34.000 people filed a case before the Federal Constitutional Court (*Bundesverfassungsgericht*), which is quite extraordinary, since the procedures do not allow for class action suits.¹²³ The *Arbeitskreis Vorratsdatenspeicherung* (German Working Group on Data Retention) is an association of civil rights campaigners, data

¹¹⁸ Available at <<http://www.gesetze-im-internet.de/ifg/BJNR272200005.html>> (in German).

¹¹⁹ See Draft Freedom of Information Act available at <<http://dip.bundestag.de/btd/15/044/1504493.pdf>> (in German) and <http://www.freedominfo.org/news/germany/FOI_Ger_1204.pdf>.

¹²⁰ See at <http://www.bfdi.bund.de/IFG/Home/homepage_node.html> (in German).

¹²¹ See for an overview <http://www.informationsfreiheit.de/info_deutschland/index.htm>.

¹²² FOI Brandenburg (Akteneinsichts- und Informationszugangsgesetz ("AIG"), 1998), available at <http://www.la.brandenburg.de/sixcms/detail.php?id=68313&template=allgemein_lda> (in German).

¹²³ See AK Vorrat: „Sammel-Verfassungsbeschwerde gegen die Vorratsdatenspeicherung“, available at <<http://www.vorratsdatenspeicherung.de/content/view/51/1/lang,de/>> (in German).

protection activists and Internet users. The *Arbeitskreis* is coordinating the campaign against the introduction of data retention in Germany.

(See more details under the "Data retention" section.)

Several video surveillance projects in Germany have generated a reaction from privacy and data protection advocacy groups. For example, a private group called *Der Grosse Bruder* (Big Brother)¹²⁴ has created a map of Munich, highlighting all the video surveillance cameras installed there. In 2003, the *Humanistische Union* (Humanistic Union)¹²⁵ sued a Berlin shopping center employing a video surveillance system with a range of vision that included a public street.¹²⁶ In Weimar, Germany, a local newspaper protested the installation of video surveillance cameras that watched the entrance of a newspaper building (along with medical and political offices), and the local government eventually uninstalled the cameras.¹²⁷ Public debate on camera observation was heightened by the revelation that a museum's security camera could see into chancellor Angela Merkel's private flat in Berlin. Upon discovery, the mechanism of the camera was changed to reduce the angle of observation.¹²⁸

In March 2004, following German retail giant Metro's RFID cards trial project in 2003, that would have allowed the tracking of all purchases and linking to the customer's identity,¹²⁹ the company halted the trial program in response to protests from digital rights groups regarding possible privacy violations.¹³⁰ Outcry was particularly forceful upon discovery that Metro had placed RFID devices in their "Extra Future Card" (personal customer shopping card) without notifying consumers.¹³¹ This use of RFID was uncovered by a German NGO called FoeBuD by taking X-ray photos of the card.¹³² FoeBuD also staged two protests, one in front of the Metro Future Store and one at a "pro-RFID" conference, and has recently been granted money by the *Bewegungsstiftung*¹³³ (a German group which supports and promotes social movements and

¹²⁴ Homepage at <<http://dergrossebruder.org>>.

¹²⁵ Homepage at <<http://www.humanistische-union.de>>.

¹²⁶ Stefan Kreml, "Urteil schränkt Videoüberwachung ein" ("Judgement Limits Video Monitoring"), Heise online, 12 December 2003, available at <<http://www.heise.de/newsticker/meldung/43130>> (in German).

¹²⁷ Peter Nowak, "Weimarer Provinzposse mit Kamera," Telepolis, 27 October 2003, available at <<http://www.heise.de/tp/deutsch/inhalt/te/15950/1.html>> (in German).

¹²⁸ "Wachleute filmten heimlich Merkels Wohnzimmer", Spiegel online of 26 March 2006, available at <<http://www.spiegel.de/politik/deutschland/0,1518,408015,00.html>> (in German).

¹²⁹ "Retail Future: Painless Checkout, Knowing Scanners," Reuters, 14 May 2003 <http://www.forbes.com/home_europe/newswire/2003/05/14/rtr970418.html>.

¹³⁰ "German Revolt Against RFID", The Register, 1st March 2004, available at <http://www.theregister.co.uk/2004/03/01/german_revolt_against_rfid/>.

¹³¹ See FoeBuD, RFID web page at <<http://www.foebud.org/rfid/>>;

¹³² FoeBuD, RFID web page available at <<http://www.foebud.org/rfid/>>.

¹³³ Bewegungsstiftung <<http://www.bewegungsstiftung.de/>>.

reform projects) to develop the "privatizer," a small device which consumers could use to find hidden and embedded RFID chips in consumer products.¹³⁴

(See more details under the "RFID tags" section.)

In 2009, the Federal Government has adopted a bill, still under discussion, to introduce ID cards (*Personalausweise*) with the option to have digitized fingerprints included on a voluntary basis. The original plan of the Federal Home Secretary to include digitized fingerprints on a compulsory basis met with strong public opposition.

The introduction of Google's Street View service in Germany has sparked public controversy¹³⁵ and individuals have the possibility to object electronically or in writing against the publication of images of their private premises, houses and flats. Until October 22, 2010, Google reported a total of 244,237 households which opted-out from the service which equals nearly 3 percent of households in Germany's 20 largest cities for which Google's Street View service was launched in 2010.¹³⁶ Where an opt-out has been declared Google has to pixel the concerned premise's image.

Some leading German news media, such as *Der Spiegel*, *Spiegel Online* and *Die Zeit* as well as *heise online* frequently and critically report about privacy relevant topics.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Germany ratified the Universal Declaration of Human Rights which was proclaimed by the General Assembly on 10 December 1948.¹³⁷ On 17 December 1973, Germany ratified the International Covenant on Civil and Political Rights.¹³⁸

Germany is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention

¹³⁴ E-mail from Bettina Winsemann, Staff Member, STOP1984, to EPIC, 12 July 2004 (on file with EPIC); See also FoeBuD-Newsletter, Edition 001, February 2004 <<http://www.foebud.org/newsletter/newsletterarchiv/newsletter-2004-02>> (in German)..

¹³⁵ See EDRIgram Number 8.9, 5 May 2010: "UK And Germany Question The Data Collected By Google Street View". Available at <<http://edri.org/edrigram/number8.9/google-street-view-wifi-germany-uk>>.

¹³⁶ See Google's blogpost; "How many German households have opted-out of Street View?". Available at <<http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html>>.

¹³⁷ On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights with a count of 48 votes to none with only 8 abstentions (which include South Africa). See Universal Declaration of Human Rights, 10 December 1948, available at <<http://www.un.org/Overview/rights.html>>.

¹³⁸ International Covenant on Civil and Political Rights, 16 December 1966, available at <<http://www2.ohchr.org/english/bodies/ratification/4.htm>>.

No. 108)¹³⁹ and later signed an Additional Protocol to this convention.¹⁴⁰ It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (Convention No. 005).¹⁴¹ In November 2002, Germany signed the Convention on Cybercrime which was finally ratified in 2009.¹⁴² It is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Germany has been instrumental in setting up platforms for international cooperation. International Working Group on Data Protection in Telecommunications (IWGDPT) was founded in 1983 in the framework of the International Conference of Data Protection and Privacy Commissioners at the initiative of the Berlin Commissioner for Data Protection, who has since then been chairing the Group.¹⁴³

¹³⁹ Council of Europe, Legal Affairs, Treaty Office at <<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>>.

¹⁴⁰ Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, available at <<http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=181&CM=8&DF=>>>.

¹⁴¹ Council of Europe, Legal Affairs, Treaty Office at <<http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>>.

¹⁴² Council of Europe, Convention on Cybercrime, available at <<http://conventions.coe.int/treaty/EN/searchsig.asp?NT=185&CM=7&DF=09/01/02>>.

¹⁴³ See at <<http://www.datenschutz-berlin.de/content/europa-international>>.

HELLENIC REPUBLIC (GREECE)

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Constitution of Greece recognises the rights of privacy and confidentiality of communications. Article 9 states: "(1) Every person's home is a sanctuary. The private and family life of the individual is inviolable. No home search shall be made, except when and as specified by law, and always in the presence of representatives of the judicial power. (2) Violators of the preceding provision shall be punished for violating the home's asylum and for abuse of power, and shall be liable for full damages to the sufferer, as specified by law."¹ A constitutional amendment in 2001 added a new provision to this article granting individuals a direct right to protection of their personal information.

Article 9A, states: "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law".² Article 9A provides that "the protection of personal data is ensured by an independent authority, which is established and operates as specified by law."³ Article 19 of the Constitution protects the privacy of communications. It states: "Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guarantees under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes shall be specified under law." The 2001 amendment, in addition to adding two new provisions to this article, establishes an independent authority to supervise matters relating to telecommunications.⁴ Article 19(2) now states: "The matters relating to the establishment, operation, and powers of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law." Article 19(3) states: "The use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited."⁵

¹ Constitution of Greece (1975) as amended in 2001, available at http://www.nis.gr/npimages/docs/Constitution_EN.pdf.

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ *Id.*

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Law on the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act) was approved by the Parliament in April 1997.⁶ Greece was the last member of the European Union (EU) to adopt a data protection law and its law was written to directly transpose the EU Data Protection Directive (1995/46/EC) into the Greek legal system. The Act's passage was also required for Greece to join the Schengen Agreement. Greece has incorporated into its national law all of the EU data protection directives in the telecommunications sector with the exception of the 2006 Data Retention Directive.⁷

The first major amendment to the Data Protection Act of 1997 came in 2006.⁸ The amendment refined the term "personal data" and adds provisions concerning the transfer of data to third countries.⁹

A second significant amendment came in 2007 as a consequence of a dispute that took place between the Data Protection Authority and the Police Authority that planned to use CCTV cameras (originally installed to monitor traffic during the Athens Olympics) to monitor public gatherings such as protests. In October 2007, the Supreme Court ruled in favour of the police authority's plan.¹⁰ Thus, later, Law No. 3625/2007 amending the Data Protection Act was passed with the aim of excluding CCTV cameras from the scope of the Act.¹¹ In practice, the 2007 amendment was far more substantial, as it practically excluded from the Data Protection Act's scope all crime-related personal data processing. The amendment, although inspired by the need to use already installed CCTV cameras for purposes other than traffic control (i.e., during public protests), eventually placed outside the data protection provisions all processing of personal data undertaken by (public) crime prosecution authorities when performed in the process of prosecuting a wide list of crimes (for instance, against human life or property, drug-related crimes, crimes against the public order, crimes against minors etc.).

⁶ Law No. 2472 on the Protection of Individuals with regard to the Processing of Personal Data, available at http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL.

⁷ Directive 1997/66/EC was transposed into national law through Law No. 2774/1999, that later was replaced by Law No. 3471/2006, whose first part transposed Directive 2002/58/EC into the national legal order. The transposition of Directive 2006/24/EC on data retention is still pending. See *infra* in this report.

⁸ Law No. 3471/2006 on the Protection of Personal Data and Privacy in Electronic Communications Sector and Amendment of Law 2472/1997, 28 June 2006, available at http://www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL.

⁹ *Id.*

¹⁰ Christine Pirovolakis, "Greek Privacy Chief Resigns in Protest Over Camera Monitoring of Demonstrators," BNA. Privacy Law & Security, Volume 6, Number 47, 3 December 2007, available at <http://www.bna.com>.

¹¹ Law No. 3625/2007.

Sector-based laws

Some specific provisions regarding processing of personal data are contained in sector-based legislation such as, for example, the Penal Law.¹²

DATA PROTECTION AUTHORITY

Implemented to ensure basic privacy protection, the Data Protection Act established the Hellenic Data Protection Authority (HDPa),¹³ The HDPa was established in November 1997 as an independent authority to monitor privacy violations in Greece. It was created to supervise the implementation of the Data Protection Act and all regulations referring to the protection of personal data.¹⁴ It also exercises other powers delegated to it from time to time.

The HDPa is composed of a president, assisted by a secretariat that operates at the directorate level. The president is a judge of a rank corresponding at least to that of a *Conseiller d'État*.¹⁵ The secretariat consists of three departments: a) auditors' department, b) communications department, c) department of administration and budgetary affairs. Each of these departments has a supervisor. All departments are supervised by the director.¹⁶

The HDPa enforces the Act. The Authority may impose both administrative and penal sanctions on controllers or their representatives. Administrative sanctions range from a warning with an order requiring the violation to cease within a specified time limit to requiring the destruction of the file or a ban on further processing and require the destruction of the relevant data.¹⁷ The penal sanctions include: punishment by imprisonment for up to three years and a fine of €1,000 to €150,000.¹⁸

The HDPa is responsible for archival audits, issuing regulatory acts arising from legislation on data protection, and providing information and recommendations to interested parties to ensure compliance with the data protection regulations. Its mandate includes issuing directives to enhance uniformity in implementation and to protect

¹² See *infra* the text and footnotes.

¹³ Data Protection Act, *supra*.

¹⁴ Homepage at http://www.dpa.gr/home_eng.htm.

¹⁵ Data Protection Act, Chapter D, Article 16 (Composition of the Authority),. See generally http://www.dpa.gr/portal/page?_pageid=33,43430&_dad=portal&_schema=PORTAL.

¹⁶ Email from Amalia Logiaki, Hellenic Data Protection Authority, to Ula Galster, International Policy Fellow, Electronic Privacy Information Center, 31 May 2005 (on file with EPIC). For detailed information on Departments staff, see http://www.dpa.gr/portal/page?_pageid=33,43456&_dad=portal&_schema=PORTAL.

¹⁷ Data Protection Act, Chapter E, Sanctions, Article 21. Other administrative sanctions include: a fine, a temporary or definitive revocation of the different permit that HDPa granted to data controllers (sensitive data processing permit and interconnection permit).

¹⁸ *Id.*, Article 22.

personal data *vis-à-vis* technological developments; assisting controllers in drafting codes of conduct; examining complaints; reporting violations; and issuing decisions related to the right to access information. The HDPa grants permits for the collection and processing of sensitive personal data and is accountable for the interconnection of files, including sensitive data, and the trans-border flow of personal data. The HDPa's communications office is in charge of all public relations and communication with private and public services and institutions, the media, foreign data protection authorities, European Union authorities, and international organisations and institutions.¹⁹

The HDPa has issued directives relating to direct marketing, CCTV, DNA testing, and workplace surveillance. The HDPa has also issued guidelines covering data protection in the workplace, in particular surveillance of phone calls and emails.²⁰

In 2004, the year of the Athens Olympic Games, privacy issues handled by the HDPa mostly related to the Games' security. All together,²¹ the Greek Data Protection Authority received 626 complaints, 682 questions regarding data protection matters, and 663 registrations for Robinson's List (the list of persons who do not wish data relating to them to be submitted for processing for the promotion of sales and long distance services), conducted 36 controls to files, and issued 66 decisions and three opinions.²² The majority of the complaints are examined by the Auditors Department. Some are also examined by the internal HDPa Board,²³ which issues a decision or answer and notifies the interested parties.²⁴

In 2005, the HDPa refused to give permission to the Minister of National Defence to publish the names of the persons who were illegally disqualified from military service. The Minister wanted to publish the names as a public example in order to avoid similar situations in the future. The HDPa concluded that the purpose could be more appropriately served by publishing statistics on the number of cases that were examined and sanctioned.²⁵ An appeal by the Minister of National Defence to the Supreme Administrative Court (*Simvoulío tes Epikrateas*) against the HDPa was rejected.

¹⁹ See http://www.dpa.gr/portal/page?_pageid=33,43482&_dad=portal&_schema=PORTAL.

²⁰ Article 29 Data Protection Working Party, Fifth Annual Report for the year 2000, Part II, 6 March 2002, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

²¹ Compared to 2001 and 2002, the total number of complaints submitted to the HDPa for the year 2003 decreased to reach 228. 23 were against banks, 129 for access to files, 16 against creditworthiness ascertainment companies, 22 against telecommunications companies, 15 against hospitals, ten against CCTV, 11 against marketing companies and two against Schengen Information System.

²² Email from Amalia Logiaki, *supra*.

²³ See http://www.dpa.gr/portal/page?_pageid=33,43430&_dad=portal&_schema=PORTAL.

²⁴ Email from Amalia Logiaki, *supra*.

²⁵ Article 29 Data Protection Working Party, 9th Annual Report for the year 2005, 14 June 2006 at 48, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

In 2006, the Hellenic Data Protection Authority paid particular attention to the credit reporting sector. The HDPa issued several decisions reiterating the basic data protection principle of keeping personal data for only as long as needed for the purposes for which they were collected.²⁶ The Authority also issued an order prohibiting the posting of tenants' debts for operational costs in their blocks of flats.²⁷ Schengen-related issues were also popular with the HDPa.²⁸

In 2007, DPA's members collectively resigned after a heated dispute with the police, the Attorney General of the Supreme Court, and the Ministry of Justice regarding the application of the Data Protection Act to personal information gathering by CCTV cameras.²⁹ The HDPa issued a statement "charging that the police 'flagrantly violated' the data protection regulations, which require the cameras to be used only for monitoring traffic and not people."³⁰ New HDPa members, including a new director, were elected in early 2008.

In 2008, the HDPa fined an insurance company €60.000 for illegally accessing the personal records of a gay man and deciding against providing him with life insurance. The HDPa considered this to be a breach of the person's privacy.³¹ It also fined Microsoft for not following the lawful procedure in establishing a database of copyright infringers of its software packages. Probably the HDPa's most notable decision was issued in March 2008, allowing crime prevention authorities (this time, the port police) to acquire phone records from telecommunications operators while carrying out their investigations without notifying the individuals concerned.³²

In 2009, in its Opinion 3/2009, the HDPa attempted to address the issue of the conditions under which copies of public documents containing personal information may be disclosed if so ordered by the public attorney. In practice, this decision takes one of the following forms. Either: state authorities deny access to public documents to individuals on the grounds that the requested documents include personal information about third parties and the applicants then request the intervention of the public attorney. This path leads to uncertainty on the part of those same state authorities about how to respond. Or: state authorities do grant access to public documents including personal information of third parties to those lawfully requesting them, but the third parties affected then refer the

²⁶ HDPa, Decisions 12 to 18/2006 on data controllers who did not delete personal information according to the Data Protection Act, available in Greek at <http://www.dpa.gr/decs.htm>.

²⁷ Decision 35/2006, available in Greek at <http://www.dpa.gr/decs.htm>.

²⁸ Decisions 19, 20, 46, 51/2006, available in Greek at <http://www.dpa.gr/decs.htm>.

²⁹ See *supra* and *infra* in the text.

³⁰ Christine Pirovolakis, *supra*.

³¹ "Insurance Firm Fined for Using Records to Deny Coverage to Gay Man", Kathimerini, 15 March 2008, available at http://www.ekathimerini.com/4dcgi/_w_articles_politics_100028_15/03/2008_94459.

³² Decision No. 19/2008, available in Greek at <http://www.dpa.gr/decs.htm>.

matter to the HDPa because their right to data protection has been infringed. In its legal opinion the HDPa acknowledged the binding effect of orders issued by the public attorney; however, it requested that state authorities, when in doubt, should consult the HDPa before granting applicants any access to any personal information, especially if sensitive personal data have been divulged in any way.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The relevant case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Law No. 2225/94 requires police wishing to conduct telephone taps to obtain court permission.³³ In accordance with Law No. 3666/2008 (Article 2 paragraph 7(a)), the list of crimes for which lawful interception of electronic communications is permitted is amended to include child pornography and its preliminary acts, bribery for the election of members of the parliament and other superior civil officers, civil servants, and judges, and coercion of minors to lechery and its preliminary acts.³⁴

The Hellenic Authority for the Information and Communication Security and Privacy (ADAE) was established pursuant to the constitutional revision of 2001 under the second paragraph of Article 19.³⁵ The ADAE replaced the erstwhile National Commission for the Protection of Communication Security and Privacy. The ADAE is charged with safeguarding the privacy and security of communications according to its founding Law No. 3115/2003.³⁶ The ADAE also issued regulations that protect communication privacy relating to electronic communications and postal services. In addition to these duties, the ADAE's responsibility includes supervising the Hellenic National Intelligence Service and carrying out audits of intelligence installations and archives as well as areas of the civil sector.³⁷ ADAE is subject to parliamentary examination in ways and procedures that follow current parliamentary rules.³⁸

³³ Law No. 2225/94 (last amended 2003).

³⁴ Law No. 3666/2008, Article 2 paragraph 7(a).

³⁵ The Hellenic Authority for Communication Security and Privacy (ADAE)'s website, at <http://www.adae.gr/portal/index.php?id=1&L=1>.

³⁶ *Id.*

³⁷ ADAE letter to Privacy International, 11 September 2008, Registration Number 2077, on file with Privacy International and the Electronic Privacy Information Center.

³⁸ *Id.*

ADAE came under the spotlight in early 2006, when it became public that the mobile phones of a number of ministers and politicians (including the Prime Minister) were tapped for a period from the 2004 Olympic Games through March 2005.³⁹ All together, more than 100 mobile phones were tapped, all of them numbers operated by Vodafone Greece using Ericsson's software. These same companies first revealed the case, when "they were made aware of it". The antennas through which the above mobile phones were tapped were all located in the area around the American Embassy in Athens, but no Embassy connection was established. The case received a tremendous amount of publicity. A Parliamentary Special Committee was also established, but none of the investigations or state initiatives produced any tangible results. ADAE fined Vodafone €76 million for failing to protect the network from the unknown hackers⁴⁰ and fined Ericsson Hellas €7.36 million. This decision was, however, overturned in 2010 by the Constitutional Court's (*Conseil d'Etat*) decisions No. 3319 and No. 3320/2010.

Following this case, Law No. 3674/2008 was introduced in 2008 to reinforce the privacy of telephone calls.⁴¹ According to the main provisions of this law each telecommunications service provider must adopt a security policy whose content must be approved by the ADAE and also communicated to the HDPA and the Regulatory Authority for Telecommunications and Post (EETT). The telecommunications service provider has a duty to take all necessary measures to ensure the privacy of all communications, and to carry out regular audits of their systems and infrastructure. All voice communications taking place by means located outside the provider's direct supervision must be protected by encryption. ADAE should perform regular inspections/audits of the provider's hardware and software infrastructure of the provider regulatory compliance. In the case of a security breach or risk of a security breach, the employee charged with ensuring secrecy must notify the provider or its legal representative, the public prosecutor, the ADAE and any subscribers who may be affected. The notification should be made in writing, and where direct communication is not possible, any other convenient method may be used.

The new law required amendments to the Greek Penal Code. Violations of the secrecy of telephone calls, including content, traffic, and location data, are considered summary offences, while the evidence obtained through these violations is not admissible in court in criminal matters.⁴² Also, a new article was added to the Penal Code, which refers to crimes relating to the security of telecommunications. Under the new article 292A users illegally accessing a network or software system used for telecommunications purposes will be sentenced to at least one year and subject to a €20.000 to €50.000 fine.

³⁹ "Greek Privacy Watchdog Fines Vodafone over Wiretapping Scandal", International Herald Tribune Europe, 14 December, 2006.

⁴⁰ *Id.*

⁴¹ Article 29 Data Protection Working Party, 12th Annual Report for the year 2008, 16 June 2009, at 45, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

⁴² Greek Penal Code, Art. 370A.

Telecommunications service providers may be held liable if they do not undertake all necessary measures to protect the telecommunication services they provide.⁴³

Finally, a National Security Plan will be developed to protect electronic communications (not only telephone calls) of the public sector and the providers of networks and services for electronic communications. Those affected are required to implement these measures within six months. The Security Plan also provides for a legislative committee for this purpose, on which the HDP is also represented. However, so far no action has been taken by the Greek Government.

National security legislation

Nonetheless, the Greek government has adopted certain measures to enhance its own surveillance capabilities.⁴⁴ On 22 December 2008, the Greek government contracted Science Applications International Corporation ("SAIC") to design a security command system to enhance the security capabilities of the Greek police, Fire Brigade, Coast Guard, and Ambulance Service.⁴⁵ The system was originally delivered in July 2004 in time for the 2004 Summer Olympics in Athens. SAIC has since improved the system, "addressing Greek post-Olympic security needs." The contract has a value of \$322 million.⁴⁶ In addition to providing the system, under its contract SAIC will provide integrated logistics support for the security command system along with cellular network services until 2014.⁴⁷

Data retention

Pursuant to Article 15(3) of the EU Data Retention Directive, Greece postponed the application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony, and Internet email until 18 months after the expiration of the period provided for in Article 15(1).⁴⁸ This Directive obligates member states to enact legislation requiring electronic communications services or public communications networks to retain traffic and location data for a minimum of six months up to a maximum of two years to assist law enforcement in serious crimes cases.⁴⁹ As of

⁴³ *Id.*, Art. 292A

⁴⁴ "Greece Fully Accepts SAIC Upgrade of Greek C4I Security Command System," SecurityInfoWatch.com, 6 February 2008 available at <http://www.securityinfowatch.com/root+level/greece-fully-accepts-saic-upgrade-greek-c4i-security-command-system>.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006, OJ L 105 13 April 2006, at 54, available at <http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf>.

⁴⁹ *Id.*

mid-2010, Greece has not yet harmonised its national law with the Data Retention Directive. Presently, the retention periods for mobile, fixed telephony, and Internet data vary drastically from two to five years.⁵⁰

National databases for law enforcement and security purposes

In 2001, the HDPA issued an opinion expressing concern about the methods and effects of the collection of citizens' sensitive data, especially with respect to DNA analysis for the purpose of criminal investigation and prosecution. . According to this opinion, genetic analysis must be limited to the "non-codified section of DNA" and identity verification.⁵¹ The HDPA also advised that any methods allowing conclusions to be drawn about the personality traits of individuals from their DNA should be forbidden, including personality profiling.⁵² DNA should only be used to verify offenders' and victims' identities and for criminal investigations, and should be destroyed as soon as the intended aim has been achieved. Finally, the HDPA does not support any effort to collect and analyse genetic material for preventive purposes.⁵³

In 2009 the HDPA issued Opinion No. 2/2009 on DNA analysis and the creation of a database of DNA profiles.⁵⁴ In effect, the HDPA commented on a draft Bill amending the Greek Code of Criminal Procedure. The proposed amendment provided for the creation of a DNA database for crime investigation purposes, describing the conditions under which collection of a DNA sample would be mandatory. The same amendment also regulated the operation of the DNA database, in effect placing it outside the controlling power of the HDPA. In this opinion, the HDPA outlined its objections which, most notably, pertained to its authority in supervising the proposed DNA database as well as to the operation details of such database.

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

While the current Greek Penal Law does address some cybercrimes, the penalties for violators are generally not severe, and when Greece tries to reduce cybercrime, the laws it

⁵⁰ Art. 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, 13 July 2010, at 22, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf.

⁵¹ HDPA. Opinion. 15/2001, available in English at http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

⁵² *Id.*

⁵³ *Id.*

⁵⁴ See http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

passes generally do not correct the problem.⁵⁵ One example of this can be seen in the government's attempt in the summer of 2002 to restrict electronic games. The primary goal was to stem the flow of illegal online gambling, but the law as drafted led to economic hardship for many arcade owners, Internet cafés, and computer games stores. Many closed or were forced to pay big fines for violations of the law. A side effect was to increase support for the illegal distribution of pirated copies of games. This ultimately led to its repeal.⁵⁶

On 25 January 2008, the Greek authorities arrested a hacker in Greece who broke into the computer systems of France's Dassault Group and stole sensitive weapons technology data and sold it to a variety of countries.⁵⁷

In 2007 the Child's Rights Protection Protocol became law. According to its provisions, the names of individuals who have allegedly committed crimes relating to child pornography may be published upon General Attorney's approval.⁵⁸

In late 2009 General Attorney of Supreme Court published an expressed opinion; although it does not apply as law, it is followed *in rem* by the police authorities and the courts. According to this expressed opinion, in cases of defamation or verbal assault, personal communications data must be declassified in order to uncover the offender, even though the law does not order declassification in such cases.⁵⁹

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

Law No. 3471/2006 prohibits communication through email, fax, or other electronic media without the data subject's prior consent.

Cybersecurity

No specific information has been provided under this section.

⁵⁵ Christos Panageas, *Computer Crime and Misuse: The Case of Greece and the EU* (2003) (unpublished B.S. thesis, City College of the University of Sheffield) (on file with EPIC).

⁵⁶ Id.. See also Amanda Castleman, "More Fallout Over Greek Game Ban," *Wired.com*, 13 February 2003, available at <http://www.wired.com/news/games/0,2101,57305,00.html>.

⁵⁷ Jim Carr, "Hacker Arrested in Greece for Stealing, Selling Weapons Data," *SC Magazine*, 30 January 2008, available at <http://www.scmagazineus.com/Hacker-arrested-in-Greece-for-stealing-selling-weapons-data/article/104718/>.

⁵⁸ Law No. 3625/2007, Art. 8.

⁵⁹ Expressed Opinion No. 12/2009 of General Attorney of Supreme Court I. Tentes.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

The Greek Awareness Centre *Saferinternet.gr* was set up under the auspices of the European Commission and within the framework of the "Safer Internet" programme. The main goals of *Saferinternet.gr* are: to protect minors from illegal and harmful content, contact, and conduct; create awareness and educate parents about the ways they can protect themselves and their children from the potential dangers of the improper use of online technologies; educate teachers about the safe use of the Internet; encourage dialogue between minors and parents on the proper use of online technologies and safety issues; and promote online safety and critical thinking. In order to achieve these goals, the Greek Awareness Centre is organising a variety of awareness activities such as informative seminars aimed at the wider public, train-the-trainers workshops for educators, mass media promotion of Internet safety issues, and the creation of multimedia materials for use online, in print, and on TV and radio. The Awareness Centre collaborates with representatives of the government, the online technology industry, and NGOs in Greece and abroad whose primary goal is the provision of a safer online environment.⁶⁰

SafeLine started operations on 14 April 2003. It is the only Internet hotline in Greece that accepts reports of illegal online content, and as of 18 October 2005 is an official member of INHOPE (International Association of Internet Hotlines). *SafeLine*'s first priority is to eliminate photographic and audiovisual material that portrays the ill-treatment of minors and to safeguard children's right of safe online surfing. Also of primary concern to *SafeLine* is children's harassment via the Internet or mobile phone, as well as violence, racism, xenophobia, and in general anything that can be considered illegal under Greek Legislation.⁶¹

TERRITORIAL PRIVACY

Video surveillance

In September 2000, the HDPa set out guidelines prohibiting the recording, use, monitoring, and retention of personal information from CCTV on a regular, continuous, or permanent basis.⁶² Recording is only lawful when it is done to protect individuals or

⁶⁰ See <http://www.saferinternet.gr>.

⁶¹ *Id.*

⁶² HDPa Directive on Closed Circuit Television Systems, 1122-26.09.2000, available in English at http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

goods, or for traffic violations, and in any case only under the principles of necessity and proportionality. In these exceptional cases, the HDPa must grant permission, and the rules on accuracy and notification must be followed. With respect to crime prevention or repression, the HDPa must grant special permission to judicial and legal authorities to use cameras, with strict guidelines for the use and retention of the images.

In May 2004, the HDPa approved a police request to operate CCTV cameras on the streets during the "operational phase" of the Olympics, as long as the cameras are not used after the Games.⁶³ According to the HDPa's decision, the cameras could legally operate only from 1 July until 4 October 2004. Other conditions were that the cameras not be set up in such a way that they film the entrances or interiors of homes or that they record the conversations of passers-by, that the HDPa also requires adequate signposting informing citizens they are entering surveillance areas. The legal preconditions to using the video cameras include: (a) there is no receipt or record of images of the entrance or the interior of private homes; (b) the receiving and hearing of conversations of inhabitants or passing people is not possible; (c) the person is informed in a convenient and adequate way before he enters the range of the video camera (there must be an adequate number of distinguishable signboards in visible places) both that he is entering a place that is video recorded and the purpose of the video recording; (d) the rules of both security system and data storage are strictly followed; and (e) the data is only retained for seven days.⁶⁴

Tough security measures, including military patrols, special commando units, and more than 1.000 surveillance cameras, were put in place for the 2004 Athens Olympic Games.⁶⁵ Greek law enforcement authorities were provided with training and intelligence assistance from seven countries: Australia, Britain, France, Germany, Israel, Spain, and the United States.⁶⁶ There was little concern about the violation of citizens' privacy through the use of these cameras.

In November 2004, the HDPa extended permission for the use of CCTV on the streets for another six months, as long as it was used only for traffic monitoring. All non-traffic uses were barred, including crime control. The use of cameras was allowed only in high-traffic locations and not in areas of low traffic or at places, squares, parks, pedestrian-precincts, and public assembly areas (e.g. theatre entrances). The cameras were to be set

⁶³ "Privacy Watchdog Approves Use of Street Cameras, But Only During Games," *Kathimerini*, 5 May 2004.

⁶⁴ Email from Fereniki Panagopoulou, *supra*. See also Hellenic Data Protection Authority, Decision 28/03.05.2004, available in Greek at <http://www.dpa.gr/decs.htm>.

⁶⁵ "Athens to Be on Full Alert for Games," *The Ottawa Citizen*, 24 November 2000.

⁶⁶ "Olympics: More to It than Games," *The New York Times*, 24 July 2001.

up in such a way that they did not film the entrances or interiors of homes, and sound pick-up should not be possible.⁶⁷

In 2006, the police asked the HDPa for yet another extension to the use of this same surveillance system that had been operating in Athens since the 2004 Olympic Games. The HDPa extended its use until 24 May 2007 (Decision 39/2006), but also imposed a penalty (of €3,000) when it established that the police had breached the terms set by the HDPa (Decision 57/2006).

As noted above, in 2007 an amendment excluding CCTV cameras from the scope of the Data Protection Act was passed as Law No. 3625/2007.

The HDPa was informed that CCTV systems had been installed in two secondary schools in the prefecture of Karditsa. The HDPa considered the processing of pupils' and teachers' personal data, which was taking place in the school courtyard and the corridors, as unlawful. It deemed that such processing did not conform to the principle of proportionality, as its purpose (securing the premises and controlling vehicle/third party access) could be achieved using less intrusive means.⁶⁸

In 2009 after a surge of robberies, practically all Greek banks installed surveillance entrance control systems, some of which retained the photographs of all customers who entered a specific bank branch on a given date. When a relevant case was brought to the HDPa's attention, it granted the bank an evaluation period of 12 months in order for the bank to justify its actions with concrete data.

Location privacy (GPS, mobile phones, location based services, etc.)

In May 2009, the HDPa decided to prohibit Google from photographing areas of Greece for use in Street View.⁶⁹ In doing so, the HDPa prohibited vehicles manned by Google Street View drivers from entering the country.⁷⁰ The agency did, however, offer to allow Google to take photographs if it was supplied with information concerning the length of time Google planned to store the photographs taken for use in Street View and explain how it intended to notify individuals who were liable to be photographed of their privacy rights.⁷¹ The agency indicated that Google's previous attempts to inform residents that they might be photographed were inadequate.⁷² The HDPa cited the protection of privacy

⁶⁷ HDPa, Decision 63/2004, available in English at http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

⁶⁸ Article 29 Data Protection Working Party, 12th Annual Report for the year 2008, *supra*.

⁶⁹ Helena Smith, "Google Street View Banned from Greece: Greek Authorities Ban Google Street View Camera Cars Over Fears of Becoming a 'Big Brother' Society," *The Guardian*, 12 May 2009 available at <http://www.guardian.co.uk/technology/2009/may/12/google-street-view-banned-greece>.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *Id.*

rights as the basis for its action against Google.⁷³ For similar reasons, the HDPa also prohibited the Greek surveillance company ISP Kapou from surveilling areas within Greece.⁷⁴

For the purposes of national security and serious crime prevention/investigation, all anonymous mobile users were obliged to register with their mobile service providers by July 2010. Under the new law, anonymous users who refuse to register will have all mobile services terminated.⁷⁵

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

No specific information has been provided under this section.

NATIONAL ID & SMART CARDS

On 4 May 2000, in a controversial but important ruling, the HDPa ruled that religious affiliations must be removed from State-issued identity cards. The decision was opposed by the Greek Orthodox Church and led to massive protests and challenges to the ruling.⁷⁶ The strong connection between the Greek Orthodox Church and the State is notable as there is no separation between Church and State.⁷⁷ In March 2001, Greece's highest administrative court upheld the ruling, finding that stating citizens' religious affiliation on the compulsory identity cards was unconstitutional.⁷⁸ Prior to that, Greece was the only member of the European Union to require citizens to list their religious beliefs on citizen identity cards. The new Greek identity cards do not include religion, even on a voluntary basis. In addition to the removal of religious affiliation, new identity cards also no longer include fingerprints, names, or surnames of the cardholder's spouse, maiden names, professions, home addresses, or citizenship.

RFID tags

No specific information has been provided under this section.

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ Law No. 3783/2009.

⁷⁶ "Greek Church at War Over Plans to Change ID Cards," *The Guardian*, 24 May 2000.

⁷⁷ Email from Fereniki Panagopoulou, to Cédric Laurant, Policy Counsel, Electronic Privacy Information Center, 25 June 2004 (on file with EPIC).

⁷⁸ "Greek Church Causes Fresh Identity Crisis," *The Guardian*, 29 August 2001. See also HDPa, Decision 134/31.10.2001, available in English at http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

BODILY PRIVACY

In 2003, the HDPa struck down the use of biometric identity verification at Athens International Airport.⁷⁹ The biometric system was intended to ensure that the passenger who checked in was the same person who actually boarded the airplane. While observing that such cases should be decided on a case-by-case basis, the HDPa ruled that collecting and processing iris and fingerprint data to verify passengers' identity was not permissible. Under the Greek Data Protection Act, gathering biometric data was unlawful because it exceeded its purpose. The HDPa noted that passenger identity could be ascertained in a "milder way" by requiring passengers to show an identity card along with their airplane tickets.⁸⁰

WORKPLACE PRIVACY

In 2008, the HDPa received a request from an investment bank to grant a permit to install and operate a biometric system using the fingerprints of employees for access control to specific electronic banking applications.⁸¹ The HDPa decided that while this system is not in principle contrary to the provisions of Law No. 2472/1997, as it is aimed exclusively at access control for specific employees executing transactions involving large funds. The HDPa decided that where the purpose of the processing is aimed at securing the execution of transactions and preventing money laundering or other illegal actions, it is lawful.⁸²

HEALTH & GENETIC PRIVACY

Medical records

No specific information has been provided under this section.

Genetic identification

No specific information has been provided under this section.

FINANCIAL PRIVACY

Information related to citizens' taxation is classified. Nevertheless, attempting to fight tax evasion, the Greek government allowed the posting on the site of General Secretary of Information Systems (www.gsis.gr) of information such as the name, surname, net income, and applied tax of tax payers.⁸³

⁷⁹ HDPa, Decision 52/05.11.2003, available in English at http://www.dpa.gr/portal/page?_pageid=33,43590&_dad=portal&_schema=PORTAL.

⁸⁰ *Id.*

⁸¹ Article 29 Data Protection Working Party, 12th Annual Report for the year 2008, *supra*.

⁸² See also HDPa, Decision 52/2008, available in Greek at <http://www.dpa.gr/decs.htm>.

⁸³ Law No. 3842/2010, Art. 8.

Tiresias SA is an unlimited company established by banks, who are also its shareholders. Tiresias SA specialises in the collection and supply of credit profile data about corporate entities and private individuals and the operation of a consumer credit risk consolidation system. Additionally, the company develops interbanking information systems and provides information and communication services to the parties directly concerned. In fact, every credit card debt, loan, bounced cheque, bankruptcy, etc., is reported to and archived by Tiresias for banks operating in Greece to access.

E-GOVERNMENT & PRIVACY

The Greek Ministry of the Interior is actively engaged in the delivery of e-government projects, including the creation of a data and voice network connecting approximately 2,000 public bodies via the National Public Administration Network. "Additionally, we are promoting the further development of the Citizen Service Centres (KEP), developing information technology infrastructure and introducing contemporary tools in various government organisations," said Mr. Pavlopoulos, then Minister of the Interior. The Minister spoke at the E-Government Forum organised by *The Economist* in Athens on 19 October 2004.⁸⁴

In 2006 Greece was still trying to implement an efficient e-government policy, and to keep up with rapid EU data protection developments. As far as its e-government policy is concerned, attempts have focused on strengthening and generalising the use of KEPs (see above); additionally, emphasis was given to increasing broadband connections. Data protection has been developing rapidly. Greece, which has traditionally had strict privacy policies, is moving rather cautiously towards the necessary legislative steps for the ratification or adoption of these documents.⁸⁵

As of 2010, the most widely used e-government services are its tax administration (TAXISnet)⁸⁶ and social security-related services (in particular, IKA).⁸⁷

It seems as though the HDPA has not yet been consulted by the Greek government regarding these and other new initiatives in the field such as the "transactions card" or the "citizen's card" that will replace the compulsory ID card.

⁸⁴ "E-government a Priority for Greece, Says Minister of the Interior," epractice.eu, 22 October 2004, available at <http://www.epractice.eu/en/news/283210>.

⁸⁵ Email from Vagelis Papkonstantinou, PKPartners, Greece, to Allison Knight, Research Director, Electronic Privacy Information Center, 6 July 2007 (on file with EPIC).

⁸⁶ See <http://www.taxisnet.gr/index2.html>.

⁸⁷ IKA is the largest Social Security organisation in Greece. For more information see <http://www.ika.gr/en/home.cfm>.

OPEN GOVERNMENT

According to Article 5 of the Greek Code of Administrative Procedure,⁸⁸ citizens have the right to access administrative documents created by government agencies.

According to the Law No. 3861/2010, most legislation and public acts have to be published on the Internet when they are enacted. Moreover, every ministry and all public services must post their budget on the Internet, along with many other acts of public interest such as nominees for ministry positions such as General Secretary and other superior public officers, the membership of committees, announcements of competitive examinations for public sector jobs and public works commissions. Acts that consist of sensitive personal data or governmental and national secrets will not be posted on the Internet and nor will secrets of intellectual property or company secrets.

OTHER RECENT FACTUAL DEVELOPMENTS (WITH AN IMPACT ON PRIVACY)

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

No specific information has been provided under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Greece acceded to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol, which establishes an individual complaint mechanism.⁸⁹

Greece is a member of the Council of Europe (CoE) and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)⁹⁰ and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).⁹¹ In November 2001, Greece signed the CoE Convention on Cybercrime.⁹²

⁸⁸ Artikel 5 des Griechischen Verwaltungsverfahrenskodex (Gesetz 2690/1999), available at <http://www.rz.uni-frankfurt.de/~sobotta/greecenew.htm> (in German).

⁸⁹ Greece acceded to the ICCPR and to its First Optional Protocol on 5 May 1997. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁹⁰ Signed 28 November 1950; ratified and entered into force 28 November 1974. Text and relevant information on all the Conventions adopted within the Council of Europe are available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

⁹¹ Signed 17 February 1983; enacted 11 August 1995; entered into force 1 December 1995.

⁹² Signed 23 November 2001.

Greece is also a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Greece has been a member of the EU since 1 January 1981.

* Updates to the Greek Report published in the 2010 edition of EPHR have been provided by: Vagelis Papakonstantinou, PKpartners, Greece; Elena Spiropoulou, Spiropoulou Law Firm, Greece.

REPUBLIC OF HUNGARY

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 59 of the Constitution of the Republic of Hungary provides that "everyone has the right to the good standing of his reputation, the privacy of his home and the protection of secrecy in private affairs and personal data."¹ It also says: "Everyone in the Republic of Hungary shall have the right to good reputation, the inviolability of the privacy of his home and correspondence, and the protection of his personal data."² In 1991, the Supreme Court ruled that a law creating a multi-use personal identification number violated the constitutional right of privacy.³

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

The Hungarian law on data protection follows the model of general and sector-specific regulation. The most important principles of data protection, along with the conditions and guarantees of limiting the right to the protection of personal data, are laid down in a single, so-called general act. This law does not contain explicit authorisations for processing information. The mandatory rules associated with various types of data and different data controllers are collected in sector-specific acts. Without these sector-specific acts the content of the general act could not be put into effect and the principles defined in the general act would be translated into practice only to a minimal extent. Today, Hungary has nearly 1,000 laws and regulations that contain provisions regarding the processing of personal data, more than 150 of them explicitly citing the combined Data Protection and Freedom of Information Act.⁴

Comprehensive law

The Hungarian Data Protection Act of 1992 (the Act), covers the collection and use of personal information in both the public and private sectors. It is a combined data protection and freedom of information act.⁵ Its basic principle is informational self-determination. As regards data protection, the Act sets out general provisions on the

¹ Constitution of the Republic of Hungary, Chapter XII, Article 59, available in English at <http://www.mkab.hu/index.php?id=constitution>.

² *Id.*

³ Constitutional Court Decision No. 15/1991 (IV. 13.) AB.

⁴ Act No. LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest, available at http://abiweb.obh.hu/dpc/index.php?menu=gyoker/relevant/national/1992_LXIII.

⁵ Act No. LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest, *supra*.

request, collection, handling, and transfer of personal information and provides legal remedies to individuals whose rights are violated.

The Hungarian data protection system follows the "opt-in" regime. Under the Act personal data may only be collected and processed with the freely given, specific, and informed consent of the individual or if it is required by law. The individual must be fully informed of the purpose of the data processing. Only the data necessary to accomplish this purpose may be collected, and it may only be stored until that purpose is fulfilled. The data must be accurate, complete, and up to date. Individuals are granted the right to access their personal information and, where necessary, to request its correction or even deletion. Special protections are set out for "sensitive data", which is defined as data relating to "racial origin, nationality, and ethnic status, political opinion or party affiliation, religious or other conviction" or "medical condition, abnormal addiction, sexual life, trade-union membership, and criminal record". These kinds of data may only be processed where the subject has consented in writing or if it is based on an international agreement or required by law for the purpose of enforcing a constitutional right, national security purposes, crime prevention, or a criminal investigation.⁶ The Act also expressly prohibits the use of all-purpose identification numbers or codes.

Hungary, as a member of the European Union (since 2004), allows personal data to flow freely across borders within the EU, as if the data remained in the territory of Hungarian Republic. Personal data from other member states of the EU may be transferred to Hungary under the same conditions. Earlier, in July 2000, the European Commission considered Hungary as a country that ensures an adequate level of protection within the meaning of Article 25(6) of the EU Data Protection Directive.

On 1 January 2004 the amendment of Act LXIII of 1992 on the Protection of Personal Data and Disclosure of Data of Public Interest entered into force, which harmonised the law with applicable EU Data Protection Directive (1995/46/EC), also included changes regarding the classic role of the ombudsman in protecting privacy, and opened a new chapter in the history of the institution.⁷ As a consequence of the implementation of the Directive, decisions relating to the regulation of data protection are partly outside of the competence of Hungarian authorities. On 1 May 2004, Hungary also became a full member of the European Commission's Article 29 Data Protection Working Party – an independent consulting body operating on the side of the Commission, made up by the member States' privacy commissioners and/or other authorities.⁸

⁶ See Zita Orb, "Amended Rules on Data Protection," World Data Protection Report, Volume 1, Issue 1, January 2001 at 22.

⁷ Email from Attila Péterfalvi, Parliamentary Commissioner for Data Protection and Freedom of Information, to Ula Galster, International Policy Fellow, Electronic Privacy Information Center (EPIC), 26 May 2005 (on file with EPIC).

⁸ Email from Attila Péterfalvi, *supra*.

Sector-based laws

Many sector-specific acts contain rules for processing personal data including addresses,⁹ sector-specific identification codes,¹⁰ medical information,¹¹ police information,¹² public records,¹³ employment,¹⁴ telecommunications,¹⁵ and national security services.¹⁶ The Direct Marketing Act authorises companies to process individuals' names and addresses for marketing purposes on an "opt-out" basis, but requires consent for the processing of other information such as telephone numbers or email addresses.¹⁷ One of the most recent sector-specific acts regulates the protection of human genetic data and the operation of biobanks.¹⁸ The law does not expressly prohibit the use of such data by employers and insurance companies. The Criminal Code also includes privacy provisions.¹⁹

DATA PROTECTION AUTHORITY

The Parliamentary Commissioner for Data Protection and Freedom of Information (DP&FOI Commissioner or Commissioner) oversees the 1992 Act.²⁰ Besides supervising the implementation of the Act and acting as an ombudsman for both data protection and freedom of information, the Commissioner's tasks include investigating complaints, maintaining the Data Protection Register, and providing opinions on draft legislation. Until 2004, the Commissioner's only effective power was provided by the Secrecy Act of 1995. Under this Act, the Commissioner is entitled to review and propose changes to the classification of state and official secrets. Since 2004, the Commissioner has also been empowered to order the blocking, deletion, or destruction of unlawfully processed data; to prohibit the unlawful processing or technical processing of data; and to suspend the

⁹ Act No. LXVI of 1992 on the Register of Personal Data and Addresses of Citizens.

¹⁰ Act No. XX of 1996 on the Identification Methods Replacing the Universal Personal Identification Number, and on the Use of Identification Codes.

¹¹ Act No. XLVII of 1997 on the Use and Protection of Medical and Related Data.

¹² Act No. XXXIV of 1994 on the Police (Chapter VIII: "Data Processing by the Police").

¹³ Act No. LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archives (Restricting Rules on the Publicity of Documents Containing Personal Data).

¹⁴ Act No. IV of 1991 on Furthering Employment and Provisions for the Unemployed.

¹⁵ Act No. C of 2003 on Electronic Communications, available at <http://www.nhh.hu/dokumentum.php?cid=10617>.

¹⁶ Act No. CXXV of 1995 on the National Security Services.

¹⁷ Act No. CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing.

¹⁸ Act No. XXI of 2008 on the Protection of Humangenetic Data, the Humangenetic Examinations and the Operation of Biobanks.

¹⁹ Criminal Code, Sections 177-178/A.

²⁰ Homepage at <http://www.obh.hu/>.

transfer of data to foreign countries. The data controller concerned may institute court proceedings against these measures by the Commissioner.

The Commissioner has been very active reviewing cases involving personal information. The great majority of the cases involve data protection, while cases involving freedom of information represent only about 10 percent of the cases on average. The Commissioner opened 122 cases in the first half-year of his term in 1995; 597 cases in 1996; 937 cases in 2000; 2,350 cases in 2005, 2,724 cases in 2007, 2,115 cases in 2008 and 3,953 cases in 2009. In 2009, 3,981 petitions were submitted to the Commissioner's Office by email. Complaints represented 63 percent of the cases related to data protection in 2009, while consultations initiated by data controllers were 35 percent, and the Commissioner acted on his own initiative in 2 percent of the cases.²¹

Towards the end of his six-year term in office, the first Commissioner, László Majtényi, issued several recommendations directly blocking interests of the prevailing power-holders. In response, there was pressure from some political institutions to propose abolishing the office of the Data Protection and Freedom of Information Commissioner altogether. Finally, after negotiations lasting almost six months, in December 2001 the National Assembly succeeded in electing the country's second DP&FOI Commissioner, Attila Péterfalvi, a lawyer from the first Commissioner's office. In 2008 a similar situation occurred. In December 2007 the Parliament failed to re-elect the DP&FOI Commissioner. After ten months of unsuccessful political negotiations and several attempts to nominate the Commissioner's successor, at the end of September 2008 András Jóri, again a lawyer from the first Commissioner's office, was elected as the third DP&FOI Commissioner. His term of office will expire in 2014. Dr. Jóri declared his intent to lay more emphasis on freedom of information than his predecessor,²² so as to reduce the imbalance of the two main areas of activity of the Commissioner. He also firmly supported the idea of extending the administrative powers of the Commissioner.²³

However, in 2009 and again in 2010 there were political attacks against the institution of parliamentary commissioners, including the DP&FOI Commissioner: instead of independent commissioners, cooperating with each other only at the professional level, the concept of a centralised, hierarchical system has been promoted.²⁴ In such a system the DP&FOI Commissioner would have only a subordinate position.

²¹ See the Annual Reports of the Parliamentary Commissioner for Data Protection and Freedom of Information, available at <http://abiweb.obh.hu/dpc/index.php?menu=reports>.

²² See, for example, his interview (in Hungarian) at <http://www.jogiforum.hu/interju/46#axzz13mQniH6X>.

²³ Dr. Jóri already expressed his view in his *Adatvédelmi Kézikönyv* (Data Protection Handbook) published in 2005 by Osiris, Budapest, at. 301.

²⁴ The first significant declaration of this concept was published in a controversial interview with the Parliamentary Commissioner for Civil Rights on 1 April 2009, in which he also talked about "gypsy crime", a statement he later withdrew. See http://www.fn.hu/belfold/20090401/szabo_mate_figyelmeztetni_kell/ (in Hungarian).

MAJOR PRIVACY & DATA PROTECTION CASE LAW

Hungary's first high-profile privacy controversy was the "lottery jackpot affair."²⁵ In October 1995, somebody won the biggest prize in the history of the Hungarian lottery, which had been accumulating for a long time. *Szerencsejáték Rt.*, the State Gambling Company, had the television crew of a news programme named *Objektív* and photographers from *Népszabadság*, one of the largest-circulation dailies, do several "takes" of the "discovery" of the winning ticket. Using the footage, the TV crew managed to identify the name and address of the winners from the reverse of the ticket, and called on their family late at night. Despite the wishes of the winners, who requested anonymity, the interview with them was aired the following day. The imperfect distortion of sound and video, along with the airing of their personal data, made their identity publicly known. The DP&FOI Commissioner investigated the case and this resulted in a judgment against *Szerencsejáték Rt.*'s processing of the data and the TV crew's conduct. Sadly, the TV crew never really admitted any wrongdoing. The case divided the media industry itself, with some journalists arguing that alert TV journalists should have the right to delve into private events of interest to viewers.

In 1998, a 13-year-old girl applied for an abortion with the consent of her mother. Her case, which came to be known as the "Case of the Girl from Dávod," received wide exposure due to TV coverage, and triggered an investigation brought by the Commissioner. This case proved even more divisive, as it forced everyone familiar with it to take a stand on the boundaries of privacy and, by implication, also on questions of ethics and ideology. Having learned of the pregnancy, a family rights advocacy group initiated an official process to stop the abortion, and helped to publicise the case. The mother lodged a complaint with the Commissioner in order to identify the person guilty of having abused her daughter's sensitive data. The abortion, which was performed in the meantime, rendered the debate between pro-choice activists and their detractors pointless, even as the continued publicity deprived the family of their privacy. Remarkably, the pro-life commentators never acknowledged the subjects' right to privacy or the legal provisions governing it as legitimate concerns.

A case known as the "VIP list scandal" triggered social debate over another area of privacy. It cantered on Postabank, one of Hungary's major commercial banks. Postabank offered loans and investment opportunities to certain leading politicians, public officials, and celebrities at much more favourable rates than the prevailing market terms. Having acquired a list of names of parties and the benefits they received, the press assumed that improprieties had occurred. Not only did they hold that the bank had offered preferential treatment in the hope of improving its lobbying position, they also charged several of the individuals involved of abuse of office. In his position statement, the Commissioner cited a number of resolutions by the Constitutional Court, which established narrower constitutional protections for the privacy of public officials than for the ordinary citizen.

²⁵ For a more detailed description of this and other cases reported here, see Ivan Szekely, "Hungary," in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation* (Edward Elgar Publishing Ltd. 2008).

The Commissioner was unable to prevent the publication of the VIP list, which also featured the data of several individuals without public roles, including actors.

High-profile privacy cases are increasingly political. In 2001, the so-called "National Image Centre" illegally obtained from the Ministry of the Interior's central records the data of at least one person in practically every Hungarian household, and proceeded to mail them issues of the magazine entitled *Millenniumi Országjáró* (Millennium Country Rambler). The aim was to promote the policies of the conservative government in power. In response to a barrage of complaints, the Commissioner called on the cabinet members in charge to stop the unlawful circulation of the magazine, but to no avail: the government continued to mail the publication to citizens until it lost the next election, in 2002. Attacks on the government's abuse of citizens' data in a political direct marketing campaign was high on the agenda of the political opposition. Ironically, a year later the socialist party, which had led the opposition, availed itself of very similar means when it mailed a campaign letter by its candidate for prime minister to addresses processed in violation of the law. Hungarian laws prohibit political parties from engaging in direct marketing activities. Pursuant to the Election Procedure Act,²⁶ political parties may not legally acquire citizens' addresses until 20 days prior to Election Day. The Commissioner responded by calling on the party to destroy the list in question. Although the Party Chairman insisted that the party had acted within the law, he destroyed the databases publicly, on the record. Similar cases happened in the electoral campaigns of 2010 when one of the parties was able to send a letter to every senior citizen receiving pension. It was also discovered that the political parties possessed illegal lists on citizens' political views. These cases have not yet been resolved.²⁷

The case spurring the greatest debate after the second Commissioner took office broke out around the website *Hálapénz.hu* in 2004. *Hálapénz* in Hungarian means an informal payment or gratuity given to doctors and health care workers. Operated by private individuals, the site featured "a searchable nationwide database of obstetricians" from which the user could access patient evaluations and learn the amount of the informal payment expected by each physician for care supposedly financed in full by social security – hence theoretically free of charge to the patients. Visitors typically accessed the site to learn how much it would cost them to give birth under the supervision of a specific obstetrician and precisely what services they could expect in return. The advocates of disclosure proposed that the freedom of communication and opinion entitled expectant mothers and their relatives to share their experiences with obstetricians online. They argued that in conducting childbirths financed by social security doctors used public funds and fulfilled a public function – and that therefore their data relevant to these activities did not merit protection under privacy regulations. As for patients referred to a "private practice," they typically received care using institutions and equipment financed

²⁶ Act No. C. of 1997 on the Election Procedure, abstract issue available at http://www.valasztas.hu/en/onkval2010/347/347_1_4.html.

²⁷ See Section "Other Recent Factual Developments," *infra*.

by public funds as well. By contrast, the proponents of privacy stressed their perception of the doctor-patient relationship as a strictly confidential one, adding that the physicians involved had never abused their office. According to their view individuals who did not offer a gratuity received equally conscientious care, and gratuities were normally expected only for certain extra services, such as the obstetrician personally attending and conducting the childbirth even when off duty. The DP&FOI Commissioner came out in support of this latter opinion. As a result, the operator removed the site from the Web.

Other relevant case law concerning privacy and data protection is categorised and discussed under the corresponding section.²⁸

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

In June 2004, the Constitutional Court ruled²⁹ that the provisions on control of personal data in the Act regulating the work of security guards³⁰ are unconstitutional and furthermore annulled the right of security guards to search anyone's package or vehicle in a private area open to the public. The Constitutional Court called upon the Parliament to amend the Act by 31 December 2004. The Parliament exceeded the deadline and it was only in 2005 that a new Act was enacted³¹. In the meantime, security guards continued working on the basis of the annulled provisions, with the explicit support of the Ministry of the Interior.³² Although the new Act complies with at least some aspects of the Constitutional Court decision, it also gives several surveillance powers to private security enterprises. It allows private companies to store CCTV records as a main rule for three working days, in special cases (e.g. for counter-terrorism purposes) for about 30 days, and in post offices, banks, and similar institutions for 60 days, without any legal purpose.³³

²⁸ *Cfr.* Section "Constitutional Privacy and data Protection Framework," *supra* and Sections "Wiretapping, access to, and interception of communications," "Data retention," "E-Commerce," "Video surveillance," "Medical records," "Other Recent Factual Developments," *infra* in this Report.

²⁹ Decision No. 22/2004 (VI.19.) AB.

³⁰ Act No. IV of 1998 on Security Guards.

³¹ Act No. CXXXIII of 2005 on Security Services and the Activities of Private Investigators, promulgated in the Official Gazette No. 155 30 November 2005. It is available in Hungarian at http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A0500133.TV.

³² Letter from the Legal Department of the Ministry of Interior to Balázs Dénes, Executive Director of Hungarian Civil Liberties Union, 17 January 2005.

³³ Act No. CXXXIII of 2005, Section 31 (2).

A controversial position³⁴ of the DP&FOI Commissioner in November 2007 and several subsequent court decisions exposed a paradoxical relationship between law enforcement and privacy. According to these rulings, the face of a policeman performing his duty is not allowed to be published/disclosed in the media without his consent. Although the arguments supporting these rulings are questionable since they may confuse the individual's private and official capacities, most journalists exercise self-censorship in such situations.

Wiretapping, access to, and interception of communications

In 2005, the Parliament passed the Act on Security Services and the Activities of Private Investigators.³⁵ This law defines the purposes of surveillance and the rights of surveillance subjects, as well as the conditions of recording and archiving the images.³⁶ Surveillance by police requires a court order and is limited to investigations of crimes punishable by more than five years' imprisonment.³⁷ Surveillance by national security services requires the permission of a specially appointed judge or the Minister of Justice, who can authorise surveillance for up to 90 days.³⁸ In April 1998, the government issued a decree ordering phone companies that offer cellular service to modify their systems to ensure that they could be intercepted. The cost was estimated to be HUF10 billion (approximately €36,500,000).³⁹ It has been reported that the National Security Service (NSS) regularly installs black boxes on Internet Service Providers' (ISP) networks and intercepts communications without warrants. Furthermore, signing a contract to allow full access to data by the NSS is a precondition for obtaining an ISP operating licence.⁴⁰

In January 2007 the Constitutional Court stated that the current judicial guarantees in the criminal procedure law and in the national security sector were inadequate to provide efficient protection to the right to privacy of the citizens.⁴¹ The secret surveillance and other secret data collection activities of law enforcement and national security bodies require prior authorisation by appointed judges, but the oversight of this process did not meet the required level of constitutionality. The Constitutional Court ordered the Parliament to establish conditions of the proper judicial overview of these applications.

³⁴ The position has been left out from the Commissioner's Annual Report for 2007. An interview in which the Commissioner stated that his intent had been distorted is available in Hungarian at http://abiweb.obh.hu/abi/index.php?menu=mediaszemle/aktualis/2007/11/28&dok=mefi_20071128_???_0833_1.

³⁵ Act No. CXXXIII of 2005.

³⁶ Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2005, *supra*.

³⁷ Act No. XXXIV of 1994 on Police.

³⁸ Act No. LXXV of 1995 on the National Security Services.

³⁹ "Technical Costs of Phone Tapping Estimated at HUF10bn," *MTI Econews*, 17 April 1998.

⁴⁰ Act No. C of 2003 on Electronic Communications, *supra*.

⁴¹ Decision 940/B/2003 AB.

National security legislation

No specific information has been provided under this section.

Data retention

An amendment to the Act on Electronic Communications in 2008 implemented the EU Directive 2006/24/EC (Data Retention Directive).⁴² The new Act did not include many modifications as those data retention provisions were already in place. The retention period varies depending on internal orders of the service provider.⁴³ The only novelties were the retention of Internet communications data and the elimination of the legal purposes of data processing. The new rules establish that data controllers must keep personal data stored in databases without previously defined purposes. Such data processing was prohibited by a 1991 decision of the Constitutional Court. The Act on Protection of Personal Data (1992) also contains this ban. Therefore the Hungarian Civil Liberties Union filed a complaint to the Constitutional Court requesting an *ex-post* examination for unconstitutionality and the annulment of the data retention provisions of the Act. The case is still pending. In another case a court ruled that statistics on the usefulness of retained data are not available to the public.⁴⁴ The DP&FOI Commissioner took an active part in the evaluation of the national implementation of the Data Retention Directive. The evaluation coordinated by the Article 29 Working Party resulted in a report pointing out, among other issues, that statistics on the use of retained data are generally missing in the member states.⁴⁵

National databases for law enforcement and security purposes

Hungary joined the group of Schengen countries in 2008. The Schengen accession required, among other things, the setup of the legal and technical framework for the operation of the Schengen Information System (SIS), which required significant amendments to the immigration law, the Act on police, the Act on border control and others. Throughout 2006 and the first half of 2007 numerous acts of Parliament were amended in order to provide the SIS with relevant information stored in the Hungarian databases on law enforcement, immigrants, on passports and visas, on the search of

⁴² Act No C. of 2003, *supra*.

⁴³ Art. 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, 13 July 2010, at 22, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_annex_en.pdf.

⁴⁴ Case No. 38 P.24.903/2009, available in Hungarian at http://tasz.hu/files/tasz/imce/NBH_%C3%ADt%C3%A9let.pdf.

⁴⁵ Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the E-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the E-Privacy Directive, wp 172, 13 July 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

persons, objects, vehicles, etc. The Republic of Hungary also joined the Prüm Convention, a data-sharing initiative between some EU countries.⁴⁶ Part of the Prüm Convention provisions, falling under the former third pillar of the EU, were later subsumed into the police and judicial cooperation provisions of European Union law by 2008 Council Decisions commonly referred to as the Prüm Decision.⁴⁷

National and international data disclosure agreements

The Hungarian Government concluded data protection agreements with the Israeli and US Governments in 2001 and 2003 respectively, concerning the processing of personal data included in the Holocaust-related documents preserved in Hungarian archives and transferred to the Yad Vashem Authority in Jerusalem and the Washington Holocaust Museum, and about the rights of the persons concerned.⁴⁸

In December 2006, the President of Hungary decided not to sign a national law regarding the promulgation of the EU-US PNR (Passenger Name Records) agreement and sent it back to the Parliament for reconsideration. According to the President "it is necessary that the Parliament make possible the forwarding of data in the act on promulgation of the international agreement only in the case that the person in question has explicitly consented to it." Parliament re-discussed the bill and completed it with a rule that requires the explicit consent of the person in question to forwarding of his data abroad.⁴⁹

Cybercrime

No specific information has been provided under this section.

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

In the area of direct marketing, the provisions of the amended Direct Marketing Act⁵⁰ – along with the new provisions of the Electronic Communications Act⁵¹, the Electronic

⁴⁶ Act No. CXII of 2007 on the Transformation to the National Law of the Prüm-Treaty.

⁴⁷ Council Decision 2008/615/JHA of on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008 OJ L 210, 6 August 2008, at 1-11, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0615:EN:NOT>.

⁴⁸ Promulgated by Government decrees 231/2004. (VIII. 6.) and 13/2002. (I. 31.)

⁴⁹ Act No. CXXVIII. of 2006 on the Transformation to the National Law of the "Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security".

⁵⁰ Act No. CXIX on the Management of Name and Address Data for Research Direct Marketing Purposes.

⁵¹ Act No. C on Electronic Communications, *supra*.

Commerce Act,⁵² and the Commercial Advertising Activities Act⁵³ – entered into force in September 2008, and clearly separated online and offline direct marketing activities. According to these provisions, "opt-out" based direct marketing possibilities are restricted to traditional (mail based) direct marketing while direct marketing by electronic means can only be conducted on an "opt-in" basis.

In 2006, the DP&FOI Commissioner started an investigation of Philip Morris Hungary Ltd. regarding the processing of personal data related to a direct marketing campaign. The collected personal data was further used to send personalised brochures providing information on tobacco products. The Commissioner requested an opinion from the Hungarian Competition Authority whether such direct marketing methods can be considered as advertising of tobacco products, which – according to Act LVIII of 1997 on Business Advertising Activity⁵⁴ – is forbidden in Hungary. Since the Hungarian Competition Authority confirmed that it was "advertising of tobacco products," the Commissioner came to the conclusion that personal data shall not be collected and further used for the purpose of sending personalised brochures advertising those products, even with the consent of the data subject. Therefore, the Commissioner advised the data processor to cease the operation and ordered, by resolution, that unlawfully processed data be blocked, deleted, or destroyed. Philip Morris Hungary Ltd. brought a lawsuit against the resolution before the competent Court. According to the decision of the Court "as the addressee requested the information himself/herself to be sent in a closed envelope, therefore the information cannot be considered as an advertisement." Having regard to the decision of the Court the Commissioner revoked the resolution and the case was dismissed by the Court.⁵⁵

Later on, the Commercial Advertising Activities Act came into force.⁵⁶ In light of the new act, the Commissioner deemed it necessary to reopen the case and examine the data processing activity. According to the new act, information sent unequivocally to the addressee is considered to be forbidden advertising of a tobacco product; therefore, the collected data is further processed in a way which is incompatible with the specified, explicit, and legitimate purposes. As a consequence, the Commissioner banned the processing activity by resolution. This time Philip Morris Hungary Ltd. did not appeal the decision.⁵⁷

⁵² Act No. CVIII of 2001 on Certain Issues of Electronic Commerce Services and Informations Society Services, available at <http://www.nhh.hu/dokumentum.php?cid=11961>.

⁵³ Act No. XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, available at <http://www.nhh.hu/dokumentum.php?cid=20371>.

⁵⁴ 2002 amended version available at http://www.aeforum.org/reg_env/estonia_2.PDF.

⁵⁵ See 12th Annual Report of Art. 29 Data Protection Working Party for the Year 2008, 16 June 2009, at 48, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

⁵⁶ Act No. XLVIII of 2008, *supra*.

⁵⁷ 12th Annual Report of Art. 29 Data Protection Working Party for the year 2008, *supra*.

Cybersecurity

The first major phishing attack against Hungarian banks took place in November and December 2006. The target was Raiffeisen Bank, whose customers received an email informing them that they were unable to be contacted by phone during the last routine account check. The email then requested that the individual click on a link to confirm some personal information, and provide more. The given link was redirected to a fake portal site where some 200 customers gave their account details. Only one collaborator was caught by the investigating agencies. The leaders of the attack are still unknown.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

No specific information has been provided under this section.

TERRITORIAL PRIVACY

Video surveillance

In 2003, the deployment of closed circuit television (CCTV) systems by public authorities, primarily in Budapest, was in the headlines. Although it is mandatory to inform citizens about the installation and use of video surveillance cameras by notices on the walls of the buildings of the monitored areas, the authorities did not comply with that rule in 82 percent of the cases. Surveillance cameras now monitor almost every street and square of the downtown area. It has been reported that some of them have night-time vision and face recognition capabilities. Authorities have claimed that video cameras are efficient tools against crime. However, authorities planned to use their camera systems for purposes different from the ones that justified their original installation.⁵⁸ The Commissioner investigated the case of the Budapest neighbourhood of Terézváros where the mayor wanted to give rights to a private company to run the CCTV network, even though only the police have the right to process personal data collected by cameras on public areas. The mayor later complied with the Commissioner's opinion.⁵⁹

⁵⁸ As an example, a camera system monitoring payment on a highway was used later to identify those who had not fastened their safety belts.

⁵⁹ Kiss Gábor, "Megfigyelt megfigyelők" ("Watching the Watchers"), *Tech-tudomány*, 18 January 2003, at <http://www.index.hu/tech/jog/urbaneye/>; "Szabadtéri Big Brother Budapesten - nem önkéntes alapon" ("Open-air Big Brother in Budapest - Not on a Voluntary Basis"), *Korridor*, 29 July 2002; Sándor Tünde, "Minden sarkon térfigyelő. Erzsébetváros teljes területét kamerák pásztázzák" ("There Is a Surveillance Camera at Every Corner. The Whole Area of Erzsébetváros Is Full of Cameras"), *Népszabadság Online*, 24 July 2002, at <http://web.archive.org/web/20031122210633/http://www.nol.hu/Default.asp?DocCollID=63989&DocID=61783>.

The relevant law was modified several times. First, in 2008, the Act on Police was amended in order to give a more precise provision on video surveillance in public spaces. One year later, the Act on Public Space Supervision authorised local governments to install video surveillance systems without the participation of police forces. The amendment was heavily debated since it significantly broadens the possibility of surveillance without a clear strategy.

On 7 May 2009, the DP&FOI Commissioner issued a press release in which he drew the attention of the public to the fact that neither legal grounds of data processing, nor the possibility for data subjects to exercise their rights, are clarified where streets and other public spaces in Budapest are being recorded by Google Street View.⁶⁰ As a result, Google has suspended recording images in Hungary. Nevertheless, a similar service is freely available at "norc.hu".⁶¹ On 2 June 2010, the Commissioner wrote a letter to Google, Inc. and demanded information about the covert collection of communications data emitted by WiFi systems.⁶² His letter was part of the joint investigation of data protection commissioners coordinated by the EU Article 29 Working party.⁶³

A decision by the DP&FOI Commissioner related to camera surveillance in a block of flats. There is no special provision on video surveillance in houses consisting of several flats. Therefore, the general rule of the Data Protection and Freedom of Information Act applies. According to the general rule, if no sectoral act provides otherwise, the processing of personal data may only be allowed if all data subjects involved have given their consent to it. In the case at stake, this criterion was missing since not even the majority of flat owners had consented to the installation of the CCTV system. The Commissioner ordered the cessation of the processing. The representative of the block of flats challenged the decision of the Commissioner but the court rejected the action in its final ruling.⁶⁴

Location privacy (GPS, mobile phones, location based services, etc.)

Employees of the Hungarian subsidiary of international mobile telephone service provider Vodafone discovered that the company had used its employees to test the company's new Mobil Flotta positioning system without informing them. For several months in 2005 the company secretly followed the movement of its employees 24 hours a day, including weekends, through their cell phones, and recorded the data in personally identifiable form. The company's computer system's lists contained data about the employees' physical location in the country at 15-minute intervals. The employees sued

⁶⁰ In Hungarian at http://abiweb.obh.hu/abi/index.php?menu=0/Sajtokozlemenyek&dok=20090507_ABI_1.

⁶¹ At <http://www.norc.hu/street-view/>.

⁶² The letter is available at http://abiweb.obh.hu/dpc/index.php?menu=cases/DP/2010&dok=1545_H_2009-4.

⁶³ See <http://epic.org/privacy/streetview/>.

⁶⁴ The ruling was issued by Fővárosi Bíróság on 20 October 2010.

the company. The company admitted to the tracking but insisted that the employees had been informed about, and consented to, the tracking in advance. Both the lower court and the appellate court decided in favour of the plaintiffs. Vodafone had to publicly apologise for the case and declare that it would do its best to avoid such infringements of rights from happening again in the future. In addition, the court ordered the discontinuance of the test and ordered Vodafone to delete the data.⁶⁵

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Since August 2006, Hungary has been issuing e-passports containing a chip with biometric information about the passport holder, namely the facial image and digital fingerprints. The new type of passport was required by the European Union Council Regulation on standards for security features and biometrics in passports and travel documents issued by member states.⁶⁶

NATIONAL ID & SMART CARDS

No specific information has been provided under this section.

RFID tags

No specific information has been provided under this section.

BODILY PRIVACY

No specific information has been provided under this section.

WORKPLACE PRIVACY

Neither the Labour Code, which regulates employment relationships, nor any other sector-specific legislation mention the protection of the privacy of employees, since the only provision laid down in the Labour Code in connection with data protection regulates the admission of new employees.⁶⁷ According to this provision, an employee may be asked to fill out forms, make statements, or take aptitude tests only on condition that these do not violate his privacy rights and are relevant to his job duties.⁶⁸ Therefore, this

⁶⁵ Email from Ivan Szekely, OSA Archivum and Budapest University of Technology and Economics, Hungary, to Allison Knight, Research Director, Electronic Privacy Information Center, 11 June 2007 (on file with EPIC).

⁶⁶ European Union Council Regulation EC 2252/2004 of on standards for security features and biometrics in passports and travel documents issued by Member States, 13 December 2004, OJ L 385, 29 December 2004, at 1–6 available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:NOT>.

⁶⁷ For a detailed analysis, see Mate Daniel Szabo and Ivan Szekely, Privacy and Data Protection at the Workplace in Hungary, in S. Nouwt, B. R. de Vries (eds.), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, IT & Law Series, (T. M. C. Asser Press, The Hague 2005).

⁶⁸ Labour Code §77 para (1).

enactment merely implements the data protection principle of purpose specification, which in this case is the procedure of selecting among job applicants for a certain position. Due to the lack of regulation specially designed for employment relations,⁶⁹ the general rules of data protection should also be applicable to employment relationships, not only with respect to data processing but also, for reasons explained previously, to the privacy of employees at work.

The weakness of data protection law in employment relations also explains why not a single judgment has been pronounced in connection with cases concerning monitoring at work. In view of their vulnerable position, employees would probably be averse to resorting to legal action against their employers, even with experts' opinions and references "to prop up their case." The lack of solid legal grounds in data protection covertly encourages employers to take further advantage of their position of power on the one hand, while at the same time putting a damper on the supervisory authorities' work in the area of employment privacy on the other.⁷⁰ In this situation, it is the DP&FOI Commissioners' body of case law that has come to constitute a case law to complement the courts' application of the law.⁷¹

HEALTH & GENETIC PRIVACY

Medical records

In 2007, after many public hospitals and polyclinics were dissolved, the legislators had neglected to solve the problem of handling medical files in these medical institutions.⁷² Another important issue in 2007 was the new methodology of investigating enrichment, introduced by the Hungarian Tax and Financial Control Administration. As prescribed by the law, if, according to the findings of the tax authority, the total amount of the taxpayer's tax-exempt received income is not congruous with the taxpayer's enrichment and lifestyle, the tax authority determines the tax base by estimation. In this case the taxpayer has to verify any deviations from the tax base established by estimation by producing credible and reliable evidence. The novelty of this procedure caused many concerns, including privacy concerns in Hungary.⁷³

⁶⁹ In all fairness, labour law contains other chapters related to data protection; however, these concern very special situations, mostly data protection in health care.

⁷⁰ Andras Schiffer, *Anomalous Practices in the Handling of Medical Data in Employment*, in Mate Daniel Szabo (ed.), *Data Protection in Hungary* (HCLU, Budapest 2003).

⁷¹ Laszlo Solyom, *The Role of the Ombudsman: Interpreting Fundamental Rights and Controlling Laws*, in Laszlo Majtenyi (ed.), *The Door onto the Other Side* (The Office of the Data Protection Commissioner, Budapest 2001 – bilingual edition).

⁷² See file 903/H/2007.

⁷³ See file 225/P/2007.

The Commissioner also issued statements on data protection auditing and on the European Privacy Seal.⁷⁴

In 2008 the DP&FOI Commissioner issued an opinion related to a decree of the Ministry on Finance, which regulates the psychological aptitude test before entering into civil service at the Hungarian Tax and Financial Control Administration (APEH).⁷⁵ According to the decree, those persons who undergo psychiatric treatment, or supposedly (probably) suffer from psychiatric illness which obstructs their adaptation, integration into the entity, or impairs their efficiency in influencing the activity of the entity are prevented from occupying such a post. The Commissioner pointed out that special data categories such as health data may only be processed – if not ordered by the law – on the basis of the written consent of the data subject. However, the legal basis itself does not make the processing possible; other criteria should also be met, especially the purpose limitation. The fact that a person has undergone psychiatric treatment does not necessarily mean that he/she, by occupying a post, would influence or jeopardise the lawful activity of the entity. The DP&FOI Commissioner also stressed that one's human dignity is jeopardised if the person is prevented from occupying a post because of a probable illness. The provision of the decree in question may lead to discrimination, which is clearly against the Hungarian Constitution and the provisions of Act No. CXXV of 2003 on the promotion of equal treatment and equal chances. The Commissioner asked the Minister of Finance to repeal the decree.⁷⁶

Genetic identification

No specific information has been provided under this section.

FINANCIAL PRIVACY

The approach to insolvency lists is still an open debate in Hungary. Financial institutions set up a system of insolvency list based on their clients' consent. According to the Data Protection Commissioner, clients do not consent "freely" when they are under pressure. Indeed, without that consent, banks may reject their credit application. It is still unclear as to whether consent in this case is valid from the data protection law point of view. The Data Protection Commissioner suggests that the Parliament pass an act on the matter and establish a state body to be responsible for administering the insolvency list.⁷⁷

⁷⁴ See file 2585/H/2007.

⁷⁵ 12th Annual Report of Art. 29 Data Protection Working Party for the year 2008, *supra* at 48.

⁷⁶ *Id.*, at 49.

⁷⁷ The letter of the Data Protection Commissioner to the Ministry for National Economy is available in in Hungarian at http://www.adatvedelmibiztos.hu/abi/index.php?menu=aktualis/allasfoglalasok/2010&dok=1525_H_2010-3.

E-GOVERNMENT & PRIVACY

Both the e-Government 2010 Strategy⁷⁸ and the e-Government 2010 Programme⁷⁹ of the Prime Minister's Office aim at establishing a "Citizens' Public Information Utility" including the establishment of a national system of electronic identification of citizens and providing for interoperability with similar systems in the European Union. In 2007, commissioned by the National Development Agency, the Eötvös Károly Institute, an independent public policy organisation with special expertise in informational rights and freedoms,⁸⁰ worked out a comprehensive study on the privacy and data protection requirements in electronic identification systems.⁸¹

In 2009, Parliament adopted several Acts relating to e-government. These acts, including the amendments to the Code on the General Rules of Procedure in the Public Service,⁸² the new Act on Electronic Delivery of Official Documents and on the Electronic Delivery Record,⁸³ the Act on Electronic Public Services,⁸⁴ and the Act on the Order for Payment Procedure,⁸⁵ extended the range of procedures where the use of electronic means is obligatory.

OPEN GOVERNMENT

In terms of access to information, the 1992 Act on the Protection of Personal Data and Disclosure of Data of Public Interest guarantees access to "data of public interest", which is defined as any information being processed by government authorities except for personal information. Exemptions can be made for state secrets or official secrets and information related to national defence, national security, criminal investigations, monetary and currency policy, international relations, and judicial procedure. Personal data cannot be information of public interest, by definition, but they may fall under the category of "public information subject to disclosure". Unless otherwise prescribed by law, personal data of any person acting in the name of and on behalf of public agencies, shall be deemed public information subject to disclosure. Access to such data shall be governed by the provisions pertaining to information of public interest.

⁷⁸ In Hungarian at http://www.meh.hu/misc/letoltheto/ekozig2010strategia_0604.pdf.

⁷⁹ In Hungarian at http://www.meh.hu/misc/letoltheto/ekozig_programterv.pdf.

⁸⁰ See <http://www.ekint.org>, or in English http://www.ekint.org/ekint/ekint_angol.head.page?nodeid=27.

⁸¹ In Hungarian at http://www.ekint.org/ekint_files/File/tanulmanyok/e_szemelyazonositas_adatvedelem_ekint-1.pdf. An abstract is available in English at http://www.ekint.org/ekint/ekint_angol.news.page?nodeid=189.

⁸² Act No. CXL of 2004, available at <http://net.jogtar.hu/jr/gen/getdoc.cgi?docid=a0400140.tv&dbnum=62>.

⁸³ Act No. LII of 2009.

⁸⁴ Act No. LX of 2009.

⁸⁵ Act No. L of 2009.

The so-called Lustration Law (publicly known as the "Agent-Law"),⁸⁶ enacted in 1994, stipulates a compromise solution between the accessibility of data relating to persons who cooperated with the secret police of the past regime in an unconstitutional way, and data relating to subjects of secret police reports on the one hand, and the right to information privacy of all persons concerned on the other. Originally, the Hungarian solution was much less radical than the German model: the victims of surveillance could not learn the identity of the agents reporting on them, only the data reported about themselves, and the former agents fulfilling public functions in the new regime were allowed to resign without being subject to public scrutiny. Consequently, the maximum sanction, namely, the publication of the agents' names in the official gazette, could be applied only if they insisted on staying in office.

In June 2002, the Government announced that it would ask the Parliament to pass legislation authorising the further opening up of the secret police files from the Communist era.⁸⁷ The announcement came following an admission by the Prime Minister that he had been a counter-intelligence officer in the secret police during that time.⁸⁸ Hungary has enacted a law opening up secret service files and has been coordinating with the German Stasi archive to prosecute members of the communist regime. The law regulates access to files for both victims of spying and former spies. Victims can find out who spied on them, but to prevent recriminations and revenge-taking, they are not given access to the spy's files.⁸⁹

In 2003 a law was enacted (while the 1994 law remained in force) with provisions on the rights of victims of surveillance by the secret police of the past political regime, to learn the names of the agents reporting on them and the right to make these names public (but only in the cases where the former agents are presently public figures), and the establishment of the Historical Archives of State Security Services, replacing the Office of History, where documents relating to the activities of the former secret police are to be kept.⁹⁰ Despite these legislative developments, there has been a great deal of uncertainty concerning the contents, authenticity, and completeness of the former secret police documents, which gives rise to political blackmail and keeps the issue on the public agenda.

The 2005 Freedom of Information by Electronic Means Act makes it mandatory for every agency or organisation in attendance to proactively publish data on their organisational structure, operation, and financial management; requires electronic publication of

⁸⁶ Act No. XXIII of 1994 on Supervision of Personnel in Certain Important Positions.

⁸⁷ Radio Free Europe, 28 June 2002.

⁸⁸ Radio Free Europe, 20 June 2002.

⁸⁹ "Former Dictatorships Hoping to Learn from German Stasi Archive," *Deutsche Welle*, 12 May 2004, available at <http://www.dw-world.de/dw/article/0,,1197738,00.html>.

⁹⁰ Act No. III of 2003 on the Disclosure of the Secret Service Activities of the Past Regime and on the Establishing of the Historical Archives of State Security Services.

legislative projects and individual drafts, while also prescribing the provision of an interactive interface; mandates publication of the *Magyar Közlöny*, the official journal of the Hungarian government, and of the Electronic Compendium of Effective Laws and Regulations, in such a way that will make access to them free of charge and unencumbered by any other circumstance for everyone; and requires the Supreme Court and courts of arbitration to post all of their verdicts, judgments, and rulings on the Internet.⁹¹

OTHER RECENT FACTUAL DEVELOPMENTS (WITH AN IMPACT ON PRIVACY)

Public disturbances from the fall of 2006 until September 2007 raised questions concerning the privacy rights of citizens, policemen, and judges.⁹² Following the public disturbances, the names, home addresses, home and mobile telephone numbers of the judges and prosecutors presiding over the related criminal cases were published on an internet site, www.kuruc.info. It was clear that according to the law, the name and position of judges and prosecutors are public. However, as the data protection commissioner stated, home addresses and phone numbers are confidential personal data, even if some are published in public registers such as the phone directory, because the original purpose of the publication in the directories and the purpose of the publication on the website were different. The disclosure of these latter data would have been lawful only with the consent of the judges and prosecutors concerned. However, the data could not be removed from the site because the site was hosted on a foreign server, and had listed false contact data.⁹³ Later, the operators of the site had to face the concerns of the foreign ISPs and they switched off the site several times due to privacy-related infringements.

As mentioned above, in 2005 and 2006, the Commissioner dealt extensively with problems of political direct marketing conducted by telephone, email, and short text messages (SMS), as well as with databases set up by political parties containing data relating to the supposed or existing political views of individual voters.⁹⁴ The most significant scandal involved activists adding information relating to political views of voters to the list of voters (which is legally obtainable for election purposes and can be used for a limited time period before the elections). Based on this information, voters were classified into three categories, indicated with letters E (Enemy), S (Sympathiser) and B (for Undecided in Hungarian). Protesting against this practice, local representatives of the socialist party attended the meetings of the local self-government with a big letter

⁹¹ Freedom of Information by Electronic Means Act, *supra*.

⁹² See generally <http://news.bbc.co.uk/2/hi/europe/6209958.stm>.

⁹³ Email from Ivan Szekeley, *supra*.

⁹⁴ Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2005, *supra*; email from Ivan Szekeley to Allison Knight, *supra*.

E on their suits. Unfortunately, neither the Commissioner, nor the police investigators could establish the origin of the data, nor could they prove the actual use of the database.

Registering and processing of personal data relating to ethnic origin has been a source of recurring controversy in both professional and political circles. The freedom of affirming minority identity is addressed by the Minority Act.⁹⁵ The individual's minority identity and right to be treated in that capacity rest on the principle of freedom of identity. The Act declares that "The admission and acknowledgement of the fact that one belongs to a national or ethnic group or minority [...] is the exclusive and inalienable right of the individual," and that, as a rule of thumb, "No-one is obliged to make a statement concerning the issue of which minority one belongs to."⁹⁶ However, the Constitutional Court found it constitutionally acceptable to make it mandatory by the force of law to declare minority affiliation if such a restriction of a fundamental constitutional right is inescapably demanded by other constitutional rights and values, executed by the most appropriate method, and is limited to the minimum extent required. The decision⁹⁷ affirms that the right to elect national and ethnic minority governments may indeed justify a reasonable restriction of self-determination in the context of mandating declarations of minority.

The present system of minority elections is based on a preliminary registration model: participation in the minority self-government elections requires citizens to declare and register themselves as members of a national minority. However, nobody has the right to "check" the declared identity of those registered themselves, and the registers are destroyed after the elections.⁹⁸ This system, however, had not solved the problems of the so-called "ethno-business", namely that in the hope of gaining various benefits, people may declare themselves members of a minority without actually qualifying as such. The Eötvös Károly Policy Institute published an edited volume in English on this subject,⁹⁹ including an internationally applicable solution offering organisational and technological

⁹⁵ Act No. LXXVII of 1993 on the Rights of National and Ethnic Minorities, unofficial translation available at <http://www.kisebbsegombudsman.hu/data/files/128317683.pdf>. The Minority Act taxatively lists the recognized minorities living in the territory of the Republic of Hungary, as Armenian, Bulgarian, Croatian, German, Greek, Polish, Roma (Gipsy), Romanian, Ruthenian, Serbian, Slovakian, Slovenian, and Ukrainian. The largest minority is the Roma, comprising 7 to 10 percent of the population, according to various estimations.

⁹⁶ Act No. LXXVII of 1993 on the Rights of National and Ethnic Minorities, *supra* at § 7 (1).

⁹⁷ Decision No. 45/2005 (XII. 14.) AB.

⁹⁸ The relevant provisions are included in Act No. CXIV on the Election of Minority Self-government Representatives; see also Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2005, *supra*.

⁹⁹ Máté Dániel Szabó (ed.), *Privacy Protection and Minority Rights* (Eötvös Károly Policy Institute, Budapest 2009). The complete volume can be downloaded at http://www.ekint.org/ekint_files/File/kiadvanyok/privacy_minority.pdf.

guarantees in order to provide the means for monitoring individual subsidies granted on ethnic minority basis without the need of maintaining a central minority register.¹⁰⁰

In November 2009 the Data Protection Commissioner and the Commissioner for Ethnic Minorities issued a joint recommendation¹⁰¹ in which they declared acceptable the registering of ethnic data by the state for various purposes. They would take "objective criteria", such as colour of skin, given or family name typical for the ethnic group, or origin of parents as the basis of adjudging someone's ethnic origin.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

The two most important non-governmental organisations advocating privacy and data protection are the Eötvös Károly Policy Institute (EKINT)¹⁰² and the Hungarian Civil Liberties Union (HCLU).¹⁰³ EKINT, an institution deeply committed to the liberal interpretation of constitutionality, is a respected professional organisation whose areas of activity includes privacy and data protection as well as transparency and freedom of information. HCLU is a human rights watchdog NGO, focusing on patients' rights, data protection, freedom of speech, drug policy, and minority issues. Both organisations are composed of a handful of dedicated professionals and activists who are able to organise public events and attract the attention of the media.

Among the few but significant civil society initiatives and developments, HCLU, together with the experimental amateur performance group TÁP Theatre, organised a street performance at one of the most crowded places in Budapest, Moszkva Square, in May 2008, to protest against surveillance and data retention practices.¹⁰⁴ The HCLU submitted a complaint to the Constitutional Court about telephone and internet data retention regulation in force. In March 2008 an independent, not-for-profit website, run by a professional community, was launched and introduced to the media. The International PET Portal and Blog has become a high quality forum of Privacy Enhancing Technologies in Hungarian, English, and Dutch languages.¹⁰⁵

In the early 2000s, the annual presentation of the Hungarian Big Brother Awards¹⁰⁶ was a popular manifestation of radical civilian censure. Ironically, the most intense controversy

¹⁰⁰ Ivan Szekely, "Positive Discrimination and Data Protection: A Typology of Solutions and the Use of Modern Information Technologies", in Máté Dániel Szabó (ed.), *Privacy protection and Minority Rights*, *supra*.

¹⁰¹ Available in Hungarian at http://www.adatvedelmibiztos.hu/abi/index.php?menu=aktualis/ajanlasok&dok=20100204_ABI_1.

¹⁰² http://www.ekint.org/ekint/ekint_angol.head.page?nodeid=27.

¹⁰³ At <http://www.tasz.hu/en>.

¹⁰⁴ See video recording at http://hvg.hu/kultura/20080530_tasz_tap_szinhez.

¹⁰⁵ At <http://pet-portal.eu>.

¹⁰⁶ See <http://www.hu.bigbrotherawards.org>.

has surrounded the person of the Commissioner himself. In 2002, he was among those nominated for the Big Brother Award on account of the cameras installed on his official premises. In 2004, he received another nomination – anyone may anonymously nominate individuals through the Internet for the first round – this time for his lenient position on cameras installed in department store fitting rooms. In this case, the Commissioner found himself among the finalists and, after the online votes given to the finalists had been counted, actually ended up receiving the Audience Award. Attila Péterfalvi, the second DP&FOI Commissioner in office, not only appeared at the awards ceremony, but – unlike other recipients to date – accepted the award, although he made a point of voicing his disagreement with the rationale for his own selection.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Hungary has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol, which establishes an individual complaint mechanism.¹⁰⁷

Hungary has been a member of the Council of Europe (CoE) since 1990 and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁰⁸ It has also signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹⁰⁹ Hungary ratified the CoE Convention on Cybercrime in late 2003, and it entered into force in July 2004.¹¹⁰

Hungary became a member of the Organisation for Economic Cooperation and Development (OECD) in 1996 and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Hungary became a member of the European Union in 2004.

** Updates to the Hungarian Report published in the 2010 edition of EPHR have been provided by: Ivan Szekely, Open Society Archives at Central European University, Hungary; Máté SzaBó, Office of the Commissioner for Educational Rights at Ministry of Education, Hungary; Endre Győző Szabó, Department of Judicial Cooperation and Private International Law of the Ministry of Public Administration and Justice, Hungary.*

¹⁰⁷ ICCPR has been signed on 25 March 1969 and ratified on 17 January 1974. Hungary acceded to the First Optional Protocol on 7 September 1988. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁰⁸ Signed 6 November 1990, ratified 5 November 1992, entered into force 5 November 1992. Text and relevant information on all the Conventions adopted within the Council of Europe are available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

¹⁰⁹ Signed 13 May 1993, ratified 8 October 1997; entered into force 1 February 1998.

¹¹⁰ Signed 23 November 2001, ratified 4 December 2003; entered into force 1 July 2004.

REPUBLIC OF IRELAND¹

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Although there is no express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled that an individual may invoke the personal rights provision in Article 40.3.1 to establish an implied right to privacy.² Article 40.3.1 provides:

"The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens."

It was first used to establish an implied constitutional right in the case of *McGee v. Attorney General*,³ which recognised the right to marital privacy in the context of the importation of contraceptive products, which were then illegal in Ireland. In that case, Mr. Justice Budd stated that "it is scarcely to be doubted in our society that the right to privacy is universally recognised and accepted with possibly the rarest of exceptions". The case has been followed by others such as *Norris v. Attorney General*⁴ and *Kennedy and Arnold v. Ireland*.⁵ In the latter case, the Supreme Court ruled that the illegal wiretapping of two journalists was a violation of the constitution, stating:

"The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This cannot be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with."

While earlier cases such as *McGee* and *Norris* dealt with the right to privacy as against the state, it is now clear that the constitutional right also has horizontal effect and may be invoked as against private persons or entities such as media organisations.⁶

¹ The EPHR 2010 "Ireland" report was updated in June 2009 by Colin Irwin (Electronic Privacy Information Center, Washington, DC, USA), in July 2010 by Rossa McMahon (Patrick G. McMahon Solicitors, Ireland), and in August 2010 by TJ McIntyre (School of Law, University College Dublin, Ireland).

² Constitution of Ireland, available at [http://www.taoiseach.gov.ie/attached_files/html%20files/Constitution%20of%20Ireland%20\(Eng\)Nov2004.htm](http://www.taoiseach.gov.ie/attached_files/html%20files/Constitution%20of%20Ireland%20(Eng)Nov2004.htm).

³ 1974 I.R. 284.

⁴ 1984 I.R. 36.

⁵ 1987 I.R. 587.

⁶ See in particular *Herrity v. Associated Newspapers (Ireland) Ltd.* [2009] 1 IR 316.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Data Protection Acts of 1988 and 2003 implement the 1981 Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.⁷ The Acts regulate the collection, processing, storage, use, and disclosure of personal data processed by both the private and public sectors. As originally adopted, the Act applied only to automatically processed information – excluding, for example, manual files – but has since been extended. Individuals have a right to access and correct inaccurate information. Information can only be used for specified and lawful purposes and cannot be improperly used or disclosed. Additional protections apply to sensitive personal data, defined as information relating to racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, physical or mental health, sexual life, the commission or alleged commission of an offence, and any proceedings arising therefrom.⁸ Except in extreme circumstances, data controllers must get explicit consent before processing sensitive data, and must provide additional safeguards.⁹ Criminal penalties can be imposed for certain violations. There are broad exemptions for national security, tax, and criminal purposes. Unlawful access to data is also criminalised in certain situations by the Criminal Damage Act 1991.

The 2003 Act amends the existing law in several ways. The definition of "data" is extended to manual data as well as automated files, although this extension did not take full effect until 24 October 2007). Not all manual data is covered, however: the Act applies only to manual data which is part of a "relevant filing system", meaning any set of information relating to individuals which is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Under this definition, archived files may not be readily accessible and therefore not part of a "relevant filing system".¹⁰

⁷ Ireland was late to transpose the Directive 95/46/EC: although it should have amended the Data Protection Act of 1988 by extending its scope in order to implement the Directive by 1st October 1998, it did not do so until 2003. In January 2000, the European Commission initiated a case before the European Court of Justice against Ireland and four other countries for failure to implement the Directive on time. In December 2001, certain provisions of the Directive were implemented by the European Communities (Data Protection) Regulations, 2001. The regulations took effect in April 2002 and governed the transfer of personal information to third countries (i.e. non- European Economic Area countries). The Data Protection (Amendment) Act of 2003 (the Act) was finally enacted in July 2003, repealing the regulations and purporting to give full effect to the EU Data Protection Directive.

⁸ Section 2(a)(i).

⁹ Section 2B as inserted by the 2003 Act.

¹⁰ See Data Protection Commissioner, "What is Manual Data and What is a Relevant Filing System", available at <http://www.dataprotection.ie/viewdoc.asp?DocID=211>.

The Act also broadens the definition of "processing" to performing "any" operation on the data.¹¹ The rights of individuals in the areas of notice, access, and consent are also improved. Section 6B of the Acts provides that decisions that significantly affect a data subject (such as work performance, creditworthiness, reliability, or conduct) may not, in the absence of consent, be made automatically without human input.

Sector-based laws

Directive 2002/58, which applies the principles of the EU Data Protection Directive (95/46/EC) to the electronic communications sector, was transposed into Irish law by the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003. The Regulations prohibit unsolicited communications to individuals by means of fax, SMS, or automated calling, unless the individual opts into receiving such. In the case of corporate recipients, the requirement is to opt out. For telephone communications, individuals can opt out by registering with the National Directory Database (NDD).¹²

In 2006, the Irish Government presented the Defamation Bill 2006 and the Privacy Bill 2006 to the Houses of the *Oireachtas* (the Parliament) as part of a complementary package of reforms to the law on defamation and privacy. While the former piece of legislation has now been enacted as the Defamation Act 2009, no progress has been made with the Privacy Bill. However, the Office of the Press Ombudsman has been established, which can deal with complaints under a code of practice applicable to the press. Principle 5 of the Code deals with privacy and provides that while the right to privacy should not prevent publication of matters of public record or in the public interest, persons (including public persons) are entitled to privacy. It states that sympathy and discretion must be shown at all times in seeking information in situations of personal grief or shock. It also states that taking photographs of individuals in private places without their consent is not acceptable, unless justified by the public interest. The Ombudsman cannot award compensation but can direct the publication in question to publish a notice of his decision.

The Privacy Bill would provide for a specific tort of the invasion of privacy which would be actionable without proof of special damage (i.e., could be litigated without evidence of loss). It would provide that an individual would be entitled to such privacy as is reasonable in all the circumstances having regard to the rights of others and to the requirements of public order, public morality, and the common good. The Bill lists the following specific instances of violating privacy:

1. to subject an individual to surveillance;
2. to disclose information obtained by surveillance;

¹¹ Section 2(a)(v).

¹² <http://www.dataprotection.ie/viewdoc.asp?DocID=907>.

3. to use the name, likeness, or voice of the individual, without the consent of that individual for the purpose of advertising, promotion, or financial gain;
4. to disclose letters, diaries, medical records, or other documents concerning the individual or information obtained therefrom; or
5. to harass another person (within the meaning of section 10 of the Non-Fatal Offences against the Person Act 1997).

Certain limited rights to privacy are already provided for in specific pieces of legislation. For example, the Consumer Credit Act 1995¹³ restricts communications between creditors and consumers, the Refugee Act 1996¹⁴ protects the identity of refugee applicants, and the Criminal Law (Human Trafficking) Act 2008¹⁵ protects the privacy of human trafficking victims.

DATA PROTECTION AUTHORITY

The Data Protection Commissioner (DPC or Commissioner) is the Irish data protection authority and oversees the enforcement of data protection laws. The Commissioner has powers to investigate complaints, prosecute offenders, sponsor or publish codes of practice, and supervise the registration process of data controllers and data processors.¹⁶ Under Section 10 of the Data Protection Acts, the DPC must investigate any complaints that it receives from individuals who feel that personal information about them is not being treated in accordance with the Acts unless it is of the opinion that such complaints are frivolous or vexatious. The DPC notifies the complainant in writing of its decision regarding the complaint. The DPC's decision can be appealed to the Circuit Court. The DPC may also of its own initiative carry out investigations or privacy audits it considers appropriate to ensure compliance with the Data Protection Acts.

The Office of the DPC consists of 22 staff members.¹⁷ It has the power to obtain information to carry out its functions by serving a written "information notice" on any person.¹⁸ The DPC also has the power to enforce compliance with the Acts by serving an "enforcement notice" on any data controller or data processor to take whatever steps it considers are necessary for compliance.¹⁹ This may include correcting data, blocking access to data, supplementing data with an explanatory statement, or deleting data

¹³ See <http://www.irishstatutebook.ie/1995/en/act/pub/0024/index.html>.

¹⁴ See <http://www.irishstatutebook.ie/1996/en/act/pub/0017/print.html>.

¹⁵ See <http://www.irishstatutebook.ie/2008/en/act/pub/0008/print.html>.

¹⁶ See generally Data Protection Commissioner <http://www.dataprivacy.ie>.

¹⁷ Data Protection Commissioner, "Organisation Chart" <http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/about/1e.htm&CatID=60&m=a>.

¹⁸ Section 12.

¹⁹ Section 10.

altogether. Failure to comply with either an information notice or an enforcement notice is an offence. The DPC also has the power to appoint an authorised officer to enter and examine the premises of a data controller or data processor where this is necessary for carrying out his functions.²⁰ The obstruction of an authorised officer is an offence.

Unless specifically exempted by the Data Protection Acts, or under regulations issued by the Minister for Justice and Law Reform, all data controllers and data processors are required to register with the DPC, at which point their details are entered into a publicly available register.²¹

The extent of mandatory registration was, however, significantly reduced in 2007 when the Minister issued regulations which greatly expanded the categories of exemptions from registration.²² The net effect of that change is that the majority of data controllers and processors will now be exempt from registration. However, certain particularly important categories of data controllers and processors were not included in this change and are under an obligation to register: financial institutions (including credit institutions and insurance undertakings); persons whose business consists wholly or mainly in direct marketing, providing credit references, or collecting debts; Internet access providers; electronic communications network or service providers; data controllers who process genetic data; data processors who process personal data on behalf of data controllers who fall under one or more of the above categories.

Provision is made for "prior checking" of applications for registration involving sensitive personal data and the DPC may refuse to accept such an application where it is not satisfied that adequate safeguards will be provided for such data.²³ It is an offence for a person who is obliged to register to process data while unregistered.²⁴

The number of complaints received by the DPC grew significantly since the foundation of the department, though in 2009 there was a slight decrease in complaints (to 914, from 1,031 in 2008²⁵). In 2007 there were 1,037 complaints,²⁶ and 658 in 2006.²⁷ A substantial number of these complaints, especially in 2007, relate to unsolicited direct marketing text

²⁰ Section 24.

²¹ Section 16.

²² Statutory Instrument No. 657 of 2007.

²³ Section 17.

²⁴ Section 19.

²⁵ Annual Report of the Data Protection Commissioner 2009 <http://www.dataprotection.ie/documents/annualreports/AR2010.pdf>.

²⁶ Data Protection Commissioner, Twentieth Annual Report of the Data Protection Commissioner 2008, April 2009, <http://www.dataprotection.ie/documents/annualreports/AR2008.pdf>.

²⁷ "Annual Report of the Data Protection Commissioner 2007, PRN. A8/0298", available at <http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf>.

messages, phone calls, fax messages, and emails ("spam"), principally to mobile phones, though this has decreased in recent years from 538 in 2007 to 262 in 2009. The main reason behind this reduction in complaints is likely to be the series of criminal prosecutions brought by the DPC against premium rate text messaging and fax sending companies, most of which reached court in 2009. Other complaints concerned the right to access personal information.²⁸

The overall profile of complaints in 2009 was as follows:²⁹

Access Rights	29 %
Electronic Direct Marketing	28 %
Disclosure	17 %
Unfair obtaining of data	5 %
Failure to secure data	4 %
Unfair processing of data	3 %
Accuracy	2 %
Use of CCTV footage	2 %
Excessive data requested	2 %
Postal Direct Marketing	2 %
Unfair retention of data	2 %
Other	4 %

The Data Protection Acts 1988 to 2003 allow for the statutory rules governing the use of personal data to be supplemented by sectoral codes of practice. Under the 1988 Act the role of the DPC in this area was reactive, in that it was limited to approving or rejecting codes prepared by trade associations. Since the 2003 Act, the DPC has been given a more proactive role and may propose and draw up a code of practice on its own initiative.³⁰ To date codes of practice have been approved by the DPC in relation to *An Garda Síochána* (the police force), the Injuries Board, the insurance sector, and personal data security breaches.³¹

Such codes of practice may also be laid by the Minister for Justice and Law Reform before the *Oireachtas* (Parliament) for approval. If approved by both Houses of the *Oireachtas* then a code of practice will have the force of law.

²⁸ See Data Protection Commissioner, Twenty-First Annual Report of the Data Protection Commissioner 2009, available at <http://www.dataprotection.ie/documents/annualreports/AR2010.pdf>.

²⁹ *Id.*, at 11.

³⁰ Section 13.

³¹ See Data Protection Commissioner, "Self Regulation and Codes of Practice," available at <http://www.dataprotection.ie/ViewDoc.asp?CatID=25&fn=/documents/enforcement/5y.htm&m=e> ; Data Protection Commissioner, "Breach Notification Guidance", available at http://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm.

A significant trend in recent years, reflected internationally, is the increase in reported data security breaches (119 in 2009). As already noted, the DPC has responded by publishing a Code of Practice on data security breaches.

In 2009, the Minister for Justice established a Data Protection Review Group to consider the effectiveness of the Data Protection Acts.³² The terms of reference of the group are largely concerned with data security breaches and, among other things, require the group to consider: whether the legislation needs to be amended to deal with data breaches; the potential formats of mandatory reporting; the likely impact of the scope and timing of the forthcoming ePrivacy Directive, revised EU Data Protection Directive, and other relevant international legislative developments; as well as the role and level of penalties in any mandatory regime.

The group published a consultation paper in March 2010 which suggests that the options are to further develop the DPC's Code of Practice or to strengthen the legislative provisions.³³ That Group issued a report in March 2010 which rejected self-regulatory notification schemes as impractical and recommended that legislation provide criminal sanctions for deliberate or reckless acts or omissions in relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents – and that the requirement to report breaches to data subjects should not be provided for in the legislation but rather be set out in a binding statutory Code of Practice including a provision for mandatory reporting to the DPC.³⁴ The Commissioner already has the power to issue an enforcement notice requiring a data controller to inform data subjects of a breach which affects that data subject.

The DPC has become more active in conducting privacy audits of public and private organisations. In 2009 it published guidelines on such audits which are aimed at assisting organisations selected for auditing,³⁵ and during 2009 completed 30 of them. These included a detailed audit of the Revenue Commissioners – one of the largest holders of personal data in Ireland – and various private companies.

The 2008 report detailed the first instance of the DPC bringing a prosecution against an entity for failing to respond to an Information Notice. Iarnród Éireann was successfully prosecuted for failing to respond to the Commissioner's repeated request for information and the subsequent Information Notice. Clarion Marketing Limited was also successfully prosecuted for sending unsolicited text messages.³⁶ The report also outlined the increased

³² See <http://www.justice.ie/en/JELR/Pages/WP09000015>.

³³ At <http://www.justice.ie/en/JELR/DPRG%20Consultation%20Doc%201.1.pdf/Files/DPRG%20Consultation%20Doc%201.1.pdf>.

³⁴ Department of Justice and Law Reform, "Report of the Data Protection Review Group," March 2010, at 29-30, available at [@@http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwith....](http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwith....) See also http://www.justice.ie/en/JELR/Pages/dprg_rpt_2010.

³⁵ See <http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf>.

³⁶ Twentieth Annual Report of the Data Protection Commissioner 2008, *supra* at 16.

sanctions and powers introduced by Statutory Instrument No. 526 of 2008.³⁷ This increased the financial penalty for summary offences relating to unsolicited communications, and also created an indictable offence for a contravention of the regulation relating to unsolicited communications. The Statutory Instrument also allows for the prosecution of an officer of a body corporate, whether or not any action has been taken against it. It was also established that the onus rests on the defendant to prove that a subscriber consented to receive an unsolicited communication in cases relating to a contravention of unsolicited communication regulations.³⁸

The annual 2007 report contains a number of case studies arising from complaints and investigations during the previous year. Some of the cases for that year included the right of rectification of personal data held by a data controller, inappropriate use of CCTV footage, marketing activities by NewTel Communications, RyanAir, Tesco, and Eircom, disclosure of employee information by Aer Lingus, and need for consent to use biometrics in the workplace. Unsolicited cold calling and direct marketing, and persistent direct marketing compliance with access requests by the *Garda Síochána* formed the majority of the cases.³⁹ The 2007 report also contained guidance notes regarding electronic communications service providers about direct marketing telephone calls, data controllers about purpose limitation and retention, and biometrics in schools, colleges, and other educational institutions.⁴⁰ Many complaints were filed regarding the conduct of both public and private sectors. The complaints in the public sector were improper access to personal information by civil servants and unlawful release of personal information to third parties. In the private sector, poor standards were detected in the financial, insurance and service industries. Unlawful disclosures of data were mostly the result of inadequate security procedures, low standards of staff training, and a failure to take data protection considerations into account when setting up business systems. The 2007 report also contained 21 case studies that included the disclosure of an email address by a financial institution, several cases relating to unsolicited text messages, faxes, calls, and emails, the Credit Union using insecure methods to transfer personal information, the retention of data provided online, access to personal information denied by a data controller, and the attempted use of CCTV footage for disciplinary measures by an employer.⁴¹

³⁷ European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations, 2008, S.I. No. 526 of 2008, available at <http://www.irishstatutebook.ie/2008/en/si/0526.html>.

³⁸ Twentieth Annual Report of the Data Protection Commissioner 2008, *supra* at 16.

³⁹ Eighteenth Annual Report of the Data Protection Commissioner 2006, *supra*.

⁴⁰ "Annual Report of the Data Protection Commissioner 2007, PRN. A8/0298", available at <http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf>.

⁴¹ Twentieth Annual Report of the Data Protection Commissioner 2008, *supra* at 16.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

Privacy is protected not only by the Constitution but also, under Irish law, by virtue of Article 8 of the European Convention on Human Rights (ECHR). Although the Convention is not itself directly effective in Ireland, it has been given limited effect in domestic law by virtue of the European Convention on Human Rights Act 2003. Under that Act, a court in interpreting and applying any statutory provision or rule of law shall do so, so far as is possible, in a manner consistent with the State's obligations under the ECHR.⁴² Similarly, every organ of the State is placed under an obligation to perform its functions in a manner compatible with the State's obligations under the ECHR, and damages may be awarded to a person who has suffered as a result of a failure to do so.⁴³

Under the Act the High Court and the Supreme Court are given the power to make a declaration that statutory provisions or rules of law are incompatible with the State's obligations under the ECHR.⁴⁴ Such declarations have been made in a number of cases concerning Article 8 ECHR.⁴⁵ Unlike a finding of unconstitutionality, such a declaration shall not of itself affect the validity or enforcement of the law in question, although it may lead to an *ex gratia* payment of damages by the state. Instead, the effect of a declaration being made is largely political – its real significance lies in the pressure it will create for legislative reform.

Following this implementation of the ECHR into national law, recent privacy litigation almost invariably involves Article 8 and jurisprudence from the European Court of Human Rights, as well as the constitutional guarantee of privacy and domestic case law.⁴⁶

In 2006, the Circuit Court awarded €6,500 to a Gaelic footballer against a newspaper that published photographs of him playing in a match, one of which depicted him with his genitals accidentally exposed. It appears that the newspaper was not aware that the picture depicted his genitals until after publication, and the newspaper appealed to the High Court.⁴⁷ The High Court controversially upheld the decision,⁴⁸ finding that the newspaper had invaded the footballer's privacy and was negligent in doing so, by publishing the photograph.

⁴² Section 2.

⁴³ Section 3.

⁴⁴ Section 5.

⁴⁵ See *Foy v. An t-Ard Chláraitheoir*, Ireland and the Attorney General [2007] IEHC 470 and *Donegan v. Dublin City Council and others* [2008] IEHC 288.

⁴⁶ See for two recent examples *Herrity v. Associated Newspapers (Ireland) Ltd.* [2009] 1 IR 316 and *Murray v. Newsgroup Newspapers Ltd. and others* (unreported, High Court, Irvine J., 18 June 2010).

⁴⁷ *Sinnott v. The Nationalist and Leinster Times Limited* [2008] IEHC, *Irish Times*, 31 July 2008.

⁴⁸ O'Dell E, "What is the right to privacy for?", available at <http://www.cearta.ie/2007/01/what-is-the-right-of-privacy-for/>.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Interception of the content of communications is a criminal offence under section 98 of the Postal and Telecommunications Services Act 1993,⁴⁹ while the lawful interception of communications by state authorities is regulated under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.⁵⁰ The latter Act followed a 1987 decision of the Supreme Court ruling that wiretaps of journalists violated the Constitution.⁵¹ In October 2001, the *Taoiseach* (Prime Minister) publicly apologised on behalf of the State to three journalists whose phones were tapped during the 1980s as part of an effort to control leaks from the government. The *Taoiseach* apologised for "the inappropriate invasion of their privacy and interference by the State with their role as journalists."⁵²

Under the 1993 Act interception of postal packets or telecommunications may be authorised by the Minister for Justice and Law Reform on foot of an application by either the Commissioner of the *Garda Síochána* or Chief of Staff of the Defence Forces. Authorisations may be granted for criminal investigations in relation to serious offences or in relation to the security of the State, subject to a balancing exercise where the Minister must be satisfied that other investigations are inadequate, and that the importance of obtaining the evidence or information is sufficient to justify the interception.

Oversight of this system is provided by a Designated Judge of the High Court, who keeps the general operation of the Act under review, and by a complaints procedure whereby a Complaints Referee is empowered to hear complaints of interceptions other than in

⁴⁹ As amended and applied by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 6 June 1993, available at <http://www.irishstatutebook.ie/1993/en/act/pub/0010/index.html>; section 7 of the Postal and Telecommunications Services (Amendment) Act, 1999 and the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (Statutory Instrument 306 of 2003).

⁵⁰ See generally Collins, "Telephone Tapping and the Law in Ireland," (1993) 3 *Irish Criminal Law Journal* 31.

⁵¹ *Kennedy and Arnold v. Ireland* [1987] IR 587.

⁵² "Apology for Phone Tapping," *The Irish Times*, 26 October 2001.

accordance with the Act.⁵³ It should be noted that the oversight regime has been criticised for a lack of transparency. While the Designated Judge is obliged to produce an annual report, since the start of the system that report has consisted of no more than a single page containing essentially no substantive content. In particular, and unlike the practice in other jurisdictions, the annual report provides no details as to the internal procedures which were followed to ensure compliance, the number of intercepts carried out, or the steps which were taken to guard against and remedy mistaken intercepts.⁵⁴

State surveillance – other than the interception of communications and data retention – has until recently been largely unregulated in Irish law.⁵⁵ For example, the use of audio bugging devices, car tracking devices, and long lenses to look inside buildings were all without any statutory basis. Indeed, in 1996 the Law Reform Commission described the result as being surveillance in a "legal vacuum" which was incompatible with Ireland's obligations under the ECHR.⁵⁶ In 1998 therefore the Law Reform Commission recommended substantial reform to include systems of authorisation of surveillance and judicial oversight.⁵⁷

Reform did not, however, come about until 2009, prompted by two events: a high profile "gangland" murder and a judicial investigation into police misconduct, which found that police had been "recording persons, including their colleagues and senior officers, at will,

⁵³ It should be noted, however, that both the interception offence and oversight regime are limited in their scope. In particular, the interception offence under section 98 applies only to telecommunications messages which are being transmitted by an "authorised undertaking" – limiting it to those bodies which are the subject of authorisation under Irish and European telecommunications laws. Interception of messages being transmitted by other bodies will not be prohibited by section 98. This would include, for example, calls carried by VoIP (Voice over Internet Protocol) providers who do not need authorisation, telephone calls, or emails which are transmitted internally within a workplace, or messages sent between members of an online forum. This presents two difficulties. First, eavesdropping by private parties on such messages will not be a criminal offence under section 98. Secondly, state intercepts of such messages would not be "interceptions" subject to the 1993 Act and may avoid regulation. A similar problem arises from the fact that the interception offence applies only to messages which are "being transmitted". This suggests that access to stored communications such as voicemail or webmail (at least where they have already been listened to or read) is not "interception" under the 1983 Act. (See, e.g., Denis Kelleher, *Privacy and Data Protection Law in Ireland* (Dublin: Tottel, 2006), at 454-458.) If so, this would again mean that state access to such messages would not be subject to the oversight mechanisms established by the 1993 Act. As Irish law does not have an equivalent of the US Stored Communications Act 1986 (18 U.S.C. §§ 2701-2712); this would mean there would be no special protections for such communications. See full discussion in TJ McIntyre, "Cybercrime in Ireland," in Pauline C. Reich (ed.), *Cybercrime and Security* (Oxford University Press, 2008).

⁵⁴ Mark Tighe, "Judges' Phone Tap Report 'is laughable'," *The Sunday Times*, 23 May 2009 available at <http://www.timesonline.co.uk/tol/news/world/ireland/article6350866.ece>.

⁵⁵ See Alisdair Gillespie, "Covert Surveillance, Human Rights and the Law," (2009) 19 *Irish Criminal Law Journal* 71.

⁵⁶ Law Reform Commission, Consultation Paper on Privacy: Surveillance and the Interception of Communications (1996), 221, available at http://www.lawreform.ie/publications/data/lrc91/lrc_91.html.

⁵⁷ Law Reform Commission, Report on Privacy, Surveillance and the Interception of Communications (1998), available at http://www.lawreform.ie/publications/data/lrc99/lrc_99.html.

or contemplating or carrying out covert surveillance using electronic devices without any statutory guidance or regulation and without any internal...guidelines".⁵⁸

The result was the Criminal Justice (Surveillance) Act 2009, which introduced for the first time a statutory basis for covert surveillance. However, it should be noted that it is limited in its scope. The bill allows for the *Gardaí* to carry out surveillance of suspected criminals with the District Court's permission, or in certain emergency situations without any permission. The Act also extends the admissibility of information obtained in surveillance operations. It has been pointed out that the approach taken by the Act applies only to a relatively narrow class of surveillance: i.e., surveillance by the *Garda Síochána*, Revenue, or Defence Forces, which make use of (restrictively defined) surveillance devices. As such it does not apply to covert following or observation without such devices, which will continue to be essentially unregulated, subject only to the judicial guidance given in *Kane v. Governor of Mountjoy Prison*.⁵⁹ Nor will it apply to covert surveillance by other state agencies with investigative functions, nor to the use of informants."⁶⁰

This narrow scope therefore still leaves many forms of surveillance without a statutory basis, and it has been argued by a legal scholar that those other types of surveillance may still be vulnerable to challenge under the ECHR.⁶¹

Under the 2009 Act the general rule is that covert surveillance devices may only be planted and used on the basis of of an authorisation from a judge of the District Court.⁶²

The oversight mechanism under the 2009 Act mirrors the one established for interception and data retention by establishing two levels of review: a Complaints Referee to hear individual complaints of wrongful surveillance and a Designated Judge of the High Court tasked with keeping the operation of the Act under review.

National security legislation

The Offences Against the State Act 1939 is the primary piece of anti-terrorist legislation in Ireland. Part 2 of the Act defines certain offences that are considered to be offences against the state. Part 3 introduced the concept of an illegal organisation, a provision that

⁵⁸ Report on the Detention of 'Suspects' Following the Death of the Late Richard Barron on the 14th of October 1996 and Related Detentions and Issues, Vol. 3, pp. 1249-1252. For background see TJ McIntyre, "Criminal Justice (Surveillance) Act 2009," (2009) *Irish Current Law Statutes Annotated* 15.

⁵⁹ [1988] 1 IR 757.

⁶⁰ TJ McIntyre, "Criminal Justice (Surveillance) Act 2009," (2009) *Irish Current Law Statutes Annotated* 15.

⁶¹ Alisdair Gillespie, "Covert Surveillance, Human Rights and the Law" (2009) 19 *Irish Criminal Law Journal* 71.

⁶² However, there are two significant exceptions where judicial authorisation is not required: in relation to tracking devices (which can be installed for up to four months based on internal approval) and in cases of urgency (in which case internal approval can be given for use for up to 72 hours). (Sections 7 and 8.)

has seen much use though the years in securing the conviction of members of the provisional IRA and other organisations involved in the conflict in Northern Ireland.

Section 52 of the Offences Against the State Act 1939 has also been subjected to additional judicial scrutiny in recent years. It provides that a person suspected of an offence under the Offences Against the State Act must account for his movements or actions during any specified period and divulge all information relating to the commission or intended commission of an offence. Although the section was found to be constitutional in *Heaney v. Ireland*,⁶³ the European Court of Human Rights found the defendants, who received six-month sentences for failing to account for their movements, had been denied the right to a fair trial (Section 6.1 of the Convention) and the presumption of innocence (Section 6.2 of the Convention). In *Quinn v. O'Leary & Ors*,⁶⁴ a case with similar facts, it was held by a judge that the plaintiff was entitled to have his conviction set aside on the basis of the European Convention of Human Rights, although the government was not obliged to repeal the offending legislation. The issue has not been yet been considered in light of the implementation of the European Convention on Human Rights Act 2003.

While privacy groups, such as Digital Rights Ireland⁶⁵ and the Irish Council for Civil Liberties,⁶⁶ raised questions over the constitutionality of the emergency surveillance provision, which effectively avoids the judicial approval process, they generally favoured the Act. The bill is widely perceived as a warranted invasion of privacy as it provides the *Gardaí* with the necessary tools to disrupt organised crime, yet is confined by the requirement of judicial authorisation as well as strict limitations.

Data retention

Data retention – the storage by communications providers of traffic data about the telephone calls, text messages, emails, location, etc. of their customers – has been a controversial issue in Ireland since 2001. In that year it was revealed by the journalist Karlin Lillington that Irish mobile phone operators were holding customer records (including locator records tracking their movements) for six years, without any legal basis. This prompted intervention by the DPC which would have required that information to be deleted. However, in 2002 the government responded by imposing a requirement for telecommunications service providers to retain customers' communications data, using a secret Ministerial order that received no parliamentary

⁶³ [1996] 1 IR 580.

⁶⁴ High Court, 23 April 2004, available at <http://www.bailii.org/ie/cases/IEHC/2004/103.html>.

⁶⁵ Digital Rights Ireland, Time to Take a Close Look at Surveillance, 28 November 2008) <http://www.digitalrights.ie/2008/11/28/time-to-take-a-close-look-at-surveillance/>.

⁶⁶ Irish Council for Civil Liberties, "Intelligence Led Policing Is the Way to Tackle Gangland Crime Says the ICCL," 17 April 2009) <http://www.iccl.ie/news-intelligence-led-policing.php>.

consideration.⁶⁷ In January 2003, the DPC, which itself operates under the auspices of the Department of Justice, Equality and Law Reform, initiated proceedings for judicial review on the basis that the government was "using an 'invalid' Ministerial Directive to unconstitutionally store citizens' phone, fax, and mobile phone data."⁶⁸ The DPC agreed to delay instituting proceedings on the basis of a government commitment that stand-alone legislation would be introduced to regulate the storage of this data.

Three years later, however, no legislation had appeared. In response, the DPC issued enforcement notices in January 2005 which would have required telecoms companies to delete this data after 12 months. This finally brought about government action, and shortly afterwards the Criminal Justice (Terrorist Offences) Act 2005 introduced a three-year period of data retention for telephone traffic and location details.

The Criminal Justice (Terrorist Offences) Act 2005 largely has its origins in the European Union Framework Decision on Combating Terrorism. As a result they share an overly broad and vague definition of "terrorist activity."⁶⁹

In the course of debate the previous Minister for Justice, Michael McDowell, stated: "The Bill is largely to do with the introduction of provisions into Irish law to extend our law in an adequate way to deal with international terrorism, as is required by various international instruments to which we are party." Such language is unfortunate as no international instruments as yet require data retention for a period of 36 months, and proposals put forward for such during the Irish Presidency of the EU were rejected. Given the length of time the government had to publish legislation on the issue, and despite repeated promises of dedicated legislation, they chose nevertheless to insert the provisions as a last-minute amendment into a largely unrelated bill.⁷⁰

Current Irish data retention law is, therefore, contained in Part 7 of the 2005 Act. Under that Part the Commissioner of the *Garda Síochána* may require telecommunication providers to retain traffic and location data for a period of three years.

Access to this data is based entirely on internal approval procedures within the *Garda Síochána* or Defence Forces – a member of the police force or army officer of a sufficient rank can make an access request to a telecommunication provider without any need for external approval. Data can be accessed for the purposes of the "prevention, detection, investigation or prosecution of crime" or "the safeguarding of the security of the State".⁷¹

⁶⁷ See TJ McIntyre, "Data Retention in Ireland: Privacy, Policy and Proportionality," (2008) 24(4) *Computer Law & Security Report* 326.

⁶⁸ See McIntyre, "Data Retention: History and Current Developments," (2007) 2 *Data Protection Law and Policy* 14.

⁶⁹ Section 4.

⁷⁰ Karlin Lillington, "McDowell's Sneaky Data Law Heralds Surveillance State," *Irish Times*, 25 March 2005.

⁷¹ Sections 63-64.

There is no proportionality requirement – data can be accessed in respect of any crime, or indeed possible future crime, not merely serious crime, and it is not required that access to data be necessary or proportionate in the context of the particular case. In addition, under section 64, data can be accessed by a court order in the context of civil proceedings.

An oversight mechanism is established in sections 65 and 66, which extends the Designated Judge and Complaints Referee system established for the interception of communications to cover data retention also.

Although the Irish government initially supported data retention legislation at a European level, the 2006 Data Retention Directive,⁷² which was eventually adopted, was opposed by the government, which alleged that it had been passed using the wrong legal basis. Consequently Ireland brought a challenge to the validity of the directive – though only in relation to the procedure used to adopt the law, not the fundamental rights issues which it presented.⁷³

In June 2008, the European Court of Justice (ECJ) heard Ireland's action against the EC and Parliament for the annulment of the directive. The Advocate General published his opinion in October 2008 stating that Ireland's case challenging the directive should be rejected.⁷⁴ Subsequent to this opinion the ECJ rejected Ireland's challenge in February 2009.⁷⁵

In 2009, it emerged that a range of State agencies and the communications industry had adopted a private agreement on data retention, pending full implementation of the Data Retention Directive.⁷⁶ The agreement reportedly provides for the retention and sharing of data in excess of what is likely to be required by the Irish law, which will implement the Directive and was adopted without reference to the *Oireachtas*. The agreement is of

⁷² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

⁷³ Digital Rights Ireland, "Data Retention - Advocate General Recommends Irish Government Challenge Should be Rejected," 28 October 2008, <http://www.digitalrights.ie/2008/10/14/data-retention-advocate-general-recommends-irish-government-challenge-should-be-rejected/>.

⁷⁴ Press Release, "Advocate General, Advocate General's Opinion in Case C-301/06," 14 October 2008, available at <http://curia.europa.eu/en/actu/communiqués/cp08/aff/cp080070en.pdf>. See also *Ireland v European Parliament* [ECJ] C-301/06, 10 February 2009, available at <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-301/06>.

⁷⁵ *Ireland v European Parliament* Case C-301/06, 10 February 2009, available at <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-301/06>.

⁷⁶ K. Lillington, "Startling Memo on Retaining Data", *The Irish Times*, 25 September 2009, available at <http://www.irishtimes.com/newspaper/finance/2009/0925/1224255203480.html>.

particular concern to privacy advocates in light of revelations that Irish State agencies make very frequent requests for access to personal data.⁷⁷

It should be noted that the manner of passage into law of the the Criminal Justice (Terrorist Offences) Act 2005, which introduced, as said earlier, a three-year period of data retention for telephone traffic and location details, was heavily criticised by civil rights groups. In particular, despite the length of time the government had to publish legislation on the issue and despite repeated promises of dedicated legislation, the provisions were inserted as a last-minute amendment into a largely unrelated bill.⁷⁸

The Irish online civil rights group Digital Rights Ireland (DRI) commenced a High Court action against the Irish Government in 2006, challenging the Criminal Justice (Terrorist Offences) Act 2005 on the basis of Irish and European Law.⁷⁹ DRI believes that the type of data retention envisaged constitutes an infringement of the constitutional right to privacy as well as the right to respect for private life and correspondence under Article 8 of the European Convention on Human Rights, as it requires that the telephone and online communications of all individuals in the State be logged. DRI argues that domestic case law,⁸⁰ as well as case law from the European Court of Human Rights,⁸¹ have made it clear that telephone conversations are protected by these concepts. The European Court of Human Rights has also held that the keeping of logs of such communications (such as records of numbers dialled) falls within the scope of Article 8.⁸²

In July 2008, the Irish Human Rights Commission was accepted as an *amicus curiae* (friend of the court) in this litigation. The Human Rights Commission has stated that: "This case raises important issues about the extent to which laws and measures governing the monitoring of one's private life by the State in pursuit of tackling crime possess sufficient human rights safeguards".⁸³

⁷⁷ Digital Rights Ireland, "Leaked Report on Data Retention Directive Shows Fundamental Flaws", available at <http://www.digitalrights.ie/2010/05/14/leaked-assessment-of-data-retention-directive-shows-flaws/>.

⁷⁸ Karlin Lillington, "McDowell's Sneaky Data Law Heralds Surveillance State," *The Irish Times*, 25 March 2005.

⁷⁹ Digital Rights Ireland, "Data Retention - Advocate General Recommends Irish Government Challenge Should Be Rejected", 28 October 2008, available at <http://www.digitalrights.ie/2008/10/14/data-retention-advocate-general-recommends-irish-government-challenge-should-be-rejected/>.

⁸⁰ *Kennedy and Arnold v. Ireland*, 1987 I.R. 587.

⁸¹ *Klass v. Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978.

⁸² *Malone v. United Kingdom*, European Court of Human Rights, 8691/79 ECHR 10, 2nd August 1984.

⁸³ EDRI-gram, No. 6.2, Jan. 2008, "Key Privacy Concerns in Ireland 2007", available at <http://www.edri.org/edriagram/number6.2/privacy-ireland-2007>; see also Karlin Lillington, "E-Mail and Chat Data to be Stored 'Within a Month'," *The Irish Times*, 19 January 2008, available at <http://www.irishtimes.com/newspaper/frontpage/2008/0119/1200605160420.html>. EDRI-gram, No. 6.14, July 2008, "Irish Human Rights Commission added to data retention challenge", available at <http://www.edri.org/edriagram/number6.14/irish-human-rights-data-retention>.

In May 2010, the High Court decided that the DRI challenge be referred to the European Court of Justice (ECJ) under Article 267 of the Treaty on the Functioning of the European Union.⁸⁴ As of the end of July 2010, the High Court has not published the questions to be referred to the ECJ.

At the time of writing Ireland has not yet transposed the Data Retention Directive. Initially the government had expressed an intention to transpose the Directive by Ministerial order and without primary legislation.⁸⁵ However, following advice from the Attorney General it was accepted that primary legislation was necessary.⁸⁶ The Communications (Retention of Data) Bill 2009 is currently before the *Oireachtas* and proposes to transpose the directive by introducing a two-year retention period for telephony data and a one-year period for Internet data.

National databases for law enforcement and security purposes

In 2009, the DPC agreed a policy document with *An Garda Síochána* to govern the use of the automated number plate recognition (ANPR) system introduced by the *Gardaí*. The system involves the use of an in-car camera which recognises the vehicle registration number (VRN) of other road users. These VRNs are checked against a watch list of vehicles maintained by the *Gardaí* and, if the vehicle is on the list, details are provided to the *Gardaí*. The DPC noted that any large-scale recording of personal data must be proportionate and acceptable safeguards must be in place. The ANPR policy agreed with the *Gardaí*'s aims to balance the effective use of the system with respect for the rights and privacy of individuals.

National and international data disclosure agreements

Nothing to report.

Cybercrime

Nothing to report.

Critical infrastructure

Nothing to report.

⁸⁴ *Digital Rights Ireland Ltd. v. Minister for Communication, Marine and Natural Resources and others* (unreported, High Court, McKechnie J., 5 May 2010), available at <http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs>.

⁸⁵ Karlin Lillington, "E-Mail and Chat Data to be Stored 'Within a Month'," *The Irish Times*, 19 January 2008.

⁸⁶ See Department of Justice and Law Reform, "Regulatory Impact Analysis", 2009, available at <http://www.justice.ie/en/JELR/09%20-%20Amended%20RIA.pdf/Files/09%20-%20Amended%20RIA.pdf>.

INTERNET & CONSUMER PRIVACY

Online copyright enforcement

The Copyright and Related Rights Act 2000 permits surprise searches and enacts stiff penalties against software theft. In 2005, a number of record companies used the provisions of the act to require Internet service providers to turn over details of customers whom the record companies believed had been involved in illegal file sharing.⁸⁷ Irish ISPs refused to reveal this information to plaintiffs without a court order. The High Court ordered disclosure of identities in several cases.⁸⁸ However, the court also imposed safeguards, directing that the information disclosed could only be used to seek redress for the users' alleged copyright infringement activities, and the identities of the alleged infringers could only be made public after the plaintiffs had started proceedings.⁸⁹

In March 2008, some major music companies took action against Ireland's largest ISP, Eircom, demanding that it install filters to prevent users from illegally sharing or downloading music.⁹⁰ Eircom replied that it was not on notice of specific illegal activity that infringed the rights of the companies and had no legal obligation to monitor traffic on its network.⁹¹ Previously, the Internet Service Providers Association of Ireland (ISPAI) had stated that it opposes any filtering of this sort.

The case was settled and did not reach judgment, with Eircom agreeing to introduce a "graduated response" approach to Internet users accused of illegal file sharing.⁹² In accordance with this agreement the Eircom will be provided with IP addresses which the music industry has identified as being involved in illegal file sharing.⁹³ Warnings will be issued by Eircom to the respective subscriber which, if ignored, will result in disconnection for seven days. On a subsequent alleged infringement, service will be withdrawn for 12 months.

⁸⁷ Digital Rights Ireland, "ISPs Ordered to Hand over User Details – Users not Notified of Case or Given Chance to Make Submissions", 25 January 2006, available at <http://www.digitalrights.ie/2006/01/25/isps-ordered-to-hand-over-user-details-to-record-labels/>.

⁸⁸ *EMI v. Eircom*, [2005] IEHC 233; *Maguire v. Gill*, Unreported, ex tempore, High Court, Hannah J., 5 October 2006.

⁸⁹ *EMI v. Eircom*, *supra*; *Ryanair v. Johnston*, Unreported, Smyth J., 12 July 2006. Outlined in "High Court Rejects Ryanair Bullying Claim," *The Irish Times*, 13 July 2006.

⁹⁰ EDRI-gram, No. 6.5, March 2008, "Ireland: Music Industry Sues ISP, Demands Filtering", available at <http://www.edri.org/edriagram/number6.5/ireland-isp-filtering>.

⁹¹ *Id.*

⁹² John Collins and Mary Carolan, "Internet Users Face Shutdown over Illegal Music Downloads", *The Irish Times*, 29 January 2009, available at <http://www.irishtimes.com/newspaper/frontpage/2009/0129/1232923373331.html>.

⁹³ At <http://www.eircom.net/notification/legalmusic/intro>.

While privacy groups approve of the move away from filtering subscribers' content they contend that this settlement is also highly problematic.⁹⁴ The agreement has been described as unreliable as the companies employed by the music companies to identify offenders have a history of being inaccurate. The agreement is also secretive, and has been labelled disproportionate and undemocratic.⁹⁵ Nevertheless, the agreement was referred to the High Court to evaluate compliance with the Data Protection Acts and was approved by Mr. Justice Charleton.⁹⁶ The same record companies are pursuing similar legal actions against other ISPs to force them to adopt the graduated response system.⁹⁷

Identification of Internet users in civil litigation

Ireland has recently seen a number of cases in which plaintiffs seek to identify anonymous or pseudonymous Internet users – usually in the context of defamation or file sharing.⁹⁸ Irish ISPs have generally taken the view that the Data Protection Acts preclude them from providing this information except in relation to a request from the *Garda Síochána* in the context of a criminal investigation, or as required by a court order.⁹⁹

The first case to consider this issue was *EMI Records (Ireland) Ltd. and others v. Eircom Ltd. and BT Communications Ireland Ltd.*,¹⁰⁰ in which the plaintiffs sought to identify a number of subscribers who were alleged to be infringing copyright by uploading music. In this decision the High Court confirmed that the *Norwich Pharmacal*¹⁰¹ precedent

⁹⁴ Digital Rights Ireland, "Three Unproven Accusations and You're Out - Why the Eircom / IRMA Deal Is Bad for Internet Users", 29 Jan 2009. At <http://www.digitalrights.ie/2009/01/29/three-unproven-allegations-and-youre-out/>.

⁹⁵ *Id.*

⁹⁶ *EMI Records (Ireland) Limited & others v. eircom Limited* [2010] IEHC 108, at <http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d8840802577070035082f?OpenDocument>. The case was noteworthy for the fact that the questions addressed to Charleton J. were formulated by the DPC but his office did not appear at the hearing due to cost concerns. In addition, Charleton J. made no reference to the position of the EU Article 29 Data Protection Working Party, which has commented on IP address. See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

⁹⁷ Mary Carolan, "UPC File-sharing Court Action Begins", *The Irish Times* <http://www.irishtimes.com/newspaper/breaking/2010/0618/breaking50.html>.

⁹⁸ For background see TJ McIntyre, "Online Anonymity: Some Legal Issues," (2004) 11 *Commercial Law Practitioner* 90 and Denis Kelleher, *Privacy and Data Protection Law in Ireland* (2006), Ch. 21.

⁹⁹ Section 8 of the Data Protection Acts 1988 and 2003 exempts disclosures which are "required for the purpose of preventing, detecting or investigating offences...in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid" or which are "required by or under any enactment or by a rule of law or order of a court".

¹⁰⁰ [2005] IEHC 233.

¹⁰¹ *Norwich Pharmacal v Commissioners for Customs and Excise* [1974] AC 133. The principle of such orders had previously been confirmed in Ireland by *Megaleasing (UK) Limited v Barrett* [1993] ILRM 497.

applied and that the court had jurisdiction to order ISPs to disclose the identities of their subscribers.¹⁰²

In doing so, it accepted that ISPs owed a duty of confidentiality to their subscribers but went on to hold that a balancing exercise had to be carried out against the rights of the plaintiffs and that "[t]he right to privacy or confidentiality of identity must give way where there is *prima facie* evidence of wrongdoing". However, it approved of the earlier decision, which held that "the remedy should be confined to cases where very clear evidence of a wrong doing exists." The court also noted that the plaintiffs did not have any other means of acquiring this information.

The court therefore ordered disclosure of the identities of the subscribers, subject to safeguards built into the order. In particular, the plaintiffs were required to undertake not to disclose those identities to the public unless and until they started proceedings, on the basis that "it may turn out that they were not in fact guilty of any wrongdoing or that the named person was not the operator at the time when any wrongdoing was in fact carried out."

EMI v. Eircom has therefore been relied upon in a number of applications to court to disclose user identities. There is, however, a significant limitation to that judgment from a privacy perspective – it does not require that the user be notified in advance. In this it differs from e.g. the US practice outlined in *Dendrite International, Inc. v John Doe No. 3*,¹⁰³ which requires that users should, as far as possible, be given notice of the application and a reasonable opportunity to oppose it. Consequently there is a real risk that hearings to disclose user identities will be determined based entirely on the case of the plaintiff, as there is generally no incentive for the ISP to fight such applications.¹⁰⁴

In March 2008, the major music labels sued Ireland's largest ISP, Eircom, demanding that it install filters to prevent users from illegally sharing or downloading music.¹⁰⁵ After initially fighting the action, Eircom settled out of court in January 2009 on the basis that

¹⁰² For background see Robert Clark, "Illegal Downloads: Sharing out Online Liability: Sharing Files, Sharing Risks," (2007) 2(6) *Journal of Intellectual Property Law and Practice* 402.

¹⁰³

¹⁰⁴ The significance of this point is demonstrated by another decision on identifying Internet users - *Ryanair v. Johnston* (Unreported, High Court, Smyth J, 12 July 2006). In this case the plaintiff airline sought to identify Ryanair pilots who had posted anonymously on a union-run website, alleging that they had been engaged in intimidation of other pilots. In this case, however, the union defended the action and the court refused to order disclosure. It referred to the need for "very clear and unambiguous establishment of wrongdoing" – which was not present – and examining the motives of the plaintiff found that the case was based on "a facade of concern on non-issues" and that "the real as opposed to the putative purpose of any investigation was to break whatever resolve there might have been amongst the captains to seek better terms".

¹⁰⁵ EDRI-gram, No. 6.5, March 2008, "Ireland: Music Industry Sues ISP, Demands Filtering," available at <http://www.edri.org/edriagram/number6.5/ireland-isp-filtering>.

it would introduce a "three strikes" system for Internet users accused of illegal file sharing, and would also block access to The Pirate Bay website.¹⁰⁶

This agreement envisages that Eircom will be provided with IP addresses which are claimed to be involved in illegal file sharing. The subscriber will then be issued a series of warnings before ultimately being disconnected if further accusations are received.¹⁰⁷ As with other "three strikes" systems, this agreement has been the subject of strong criticism on the basis that it jeopardises the fundamental right of Internet access. In this case, in addition, those criticisms are compounded by the fact that the system is established by a purely private agreement with no democratic or legislative basis and no judicial oversight.¹⁰⁸

Implementation of the system was delayed after the DPC raised concerns about the processing of IP addresses and user data involved in the system. Consequently the parties applied to the High Court to rule whether the intended operation of the system was in breach of data protection law. In particular, the High Court was asked to answer a number of questions including: whether IP addresses processed by the music industry constituted "personal data"; whether processing of IP addresses by Eircom would be unwarranted; and whether the "three strikes" process would involve the use of "sensitive personal data" or would involve finding that a person had committed a criminal offence – by uploading music.

In a significant judgment the High Court answered each question in the negative, holding that: IP addresses processed on behalf of the music industry were not personal data, as the subscriber could not be identified from the IP addresses or other information held by the music industry; terminating an Internet user's subscription was a legitimate action to protect the property rights of a third party; and operating the three strikes system did not involve either determinations of criminal liability or the use of sensitive personal data.¹⁰⁹

¹⁰⁶ John Collins & Mary Carolan, "Internet Users Face Shutdown over Illegal Music Downloads," *The Irish Times*, 29 January 2009, available at <http://www.irishtimes.com/newspaper/frontpage/2009/0129/1232923373331.html>.

¹⁰⁷ EDRI, "Irish ISP Settled to Introduce 3 Strikes", 11 February 2009, <http://www.edri.org/edri-gram/number7.3/3-strikes-ireland>.

¹⁰⁸ Digital Rights Ireland, "Three Unproven Accusations and You're Out – Why the Eircom / IRMA Deal Is Bad for Internet Users", 29 January 2009, at <http://www.digitalrights.ie/2009/01/29/three-unproven-allegations-and-youre-out/>.

¹⁰⁹ *EMI Records and Others v. Eircom Ltd.* [2010] IEHC 108.

Following this judgment, Eircom has now begun to implement this three strikes system.¹¹⁰ Litigation by the music industry against other Irish ISPs is pending with a view to forcing all the major ISPs to implement similar systems.¹¹¹

E-commerce

Ireland's implementation of the EU E-Commerce Directive (2000/31/EC) makes it one of the only European countries to place the burden of opting out of "spam" on the consumer.¹¹² However, this must be considered something of an anomaly in light of the implementation of the Directive on Privacy and Electronic Communications.

Unsolicited communications are governed by the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003¹¹³ which implement the E-Privacy Directive¹¹⁴ into Irish law. The regulations set out a number of rules concerning direct marketing. In particular, unsolicited communications to individuals by means of fax, email, SMS, or automated calling are prohibited unless the individual "opts in" to receiving such.¹¹⁵ Where the recipient of the call is a company, they may "opt out" by stating that they do not wish to receive the communications.¹¹⁶

In the case of unsolicited telephone calls made by human operators, persons may not be contacted if they have opted out, or if they have registered with the National Directory Database (NDD)¹¹⁷ that they do not wish to receive such calls.¹¹⁸ The regulations provide for an amended version of the NDD, which lists those unwilling to receive unsolicited telephone calls. On 21 July 2005, more than 12 months later than originally planned, the

¹¹⁰ John Collins, "Eircom to Cut Broadband over Illegal Downloads", *The Irish Times*, 24 May 2010, available at <http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html>.

¹¹¹ John Collins, "Three Strikes Rule Aims to Knock out Music Sharing", *The Irish Times*, 4 June 2010, available at <http://www.irishtimes.com/newspaper/finance/2010/0604/1224271811210.html>.

¹¹² "Republic Puts 'Spam' Burden on the Consumer," *The Irish Times*, 29 June 2001.

¹¹³ Statutory Instrument No. 535 of 2003.

¹¹⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

¹¹⁵ Regulation 13(1). There is a "soft opt-in" exception for email marketing where an individual's details have been collected in the context of the purchase of a similar product or service from the data controller – see regulation 13(7).

¹¹⁶ Regulation 13(2).

¹¹⁷ The central phone directory that lists subscribers from all the telecommunications companies in Ireland.

¹¹⁸ Regulation 14.

NDD became fully operational. The four mobile telephone operators in Ireland chose to opt all their customers out.¹¹⁹

The sanctions available for unsolicited communications were significantly enhanced by statutory instrument in 2008.¹²⁰ This increased the financial penalty for offences relating to unsolicited communications, which may now be tried on indictment as well as summarily.¹²¹ The statutory instrument also allows for the prosecution of an officer of a body corporate, whether or not any action has been taken against the body corporate. It also reverses the burden of proof regarding consent by providing that the onus rests on the defendant to prove that a subscriber consented to receive a communication. In addition, each unsolicited communication now constitutes a separate offence, so that the aggregate financial penalty may be very high.

The Data Protection (Amendment) Act 2003 provides for a number of measures concerning those involved in direct marketing. Under previous data protection legislation, information garnered from sources required by law to be publicly available (such as the electoral register or companies registration information) was exempt and could, therefore, be harvested for direct marketing.¹²² Following the 2003 Act, an individual now has the right to object to use of this data for direct marketing purposes, and the data controller must inform the individual of this right.¹²³

Cybersecurity

Between June and October 2007, the unencrypted personal data of about 10,000 customers of the Bank of Ireland were stolen.¹²⁴ They included medical history, life insurance details, bank account details, names, and addresses.¹²⁵ However, the bank did not notify the Data Protection Commissioner of the privacy breach until April 2008, ten months after the first theft, and only days before the European Data Protection Supervisor

¹¹⁹ Data Protection Commissioner, "Frequently Asked Questions about Marketing Calls and the National Directory Database Opt-Out Register" <http://www.dataprotection.ie/viewdoc.asp?DocID=908>.

¹²⁰ European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations, 2008, Statutory Instrument No. 526 of 2008.

¹²¹ The maximum penalties are now €5,000 if tried summarily; on indictment the maximum penalty is €50,000 for a natural person or for a corporate defendant either €250,000 or 10 percent of turnover, whichever is greater.

¹²² See e.g. Data Protection Commissioner, "Case Study 5/97", 2008, available at <http://www.dataprotection.ie/viewdoc.asp?DocID=160>.

¹²³ Section 2(8).

¹²⁴ EDRI-gram, No. 6.9, May 2008, "Important Personal Data Lost by the Bank of Ireland", available at <http://www.edri.org/edrigram/number6.9/personal-data-bank-ireland>.

¹²⁵ *Id.*

(EDPS) suggested the creation of a mandatory security breach notification system.¹²⁶ By that stage, the Bank of Ireland had still not warned individual customers whose information had been lost despite the obvious potential for abuse.¹²⁷

Before that event, Ireland did not have a mandatory data breach notification law, but in July 2010 the Data Protection Commissioner ("DPC") published a Personal Data Security Breach Code of Practice,¹²⁸ which will not be binding until it is approved by the *Oireachtas*. There is as yet no Government commitment to introducing criminal sanctions for deliberate or reckless acts in relation to the data protection principles.

The code provides that where there is a data security breach, the data controller must give immediate consideration to informing those affected and that, if appropriate, other organisations should be informed such as *An Garda Síochána* (the police force) and financial institutions. It states that if the data is encrypted to a high standard the data controller "may conclude that there is no risk to the data and therefore no need to inform data subjects". Data processors must report loss of control of personal data to the relevant data controller as soon as the processor becomes aware of the incident. All data security breaches should be reported to the DPC as soon as the data controller becomes aware of the incident, and at least within two working days of becoming aware, unless the breach affects less than 100 data subjects who have all been informed of the breach without delay, and where the data is not sensitive nor of a financial nature. The DPC may require a detailed report of the incident and may carry out its own investigation.

Developments at European level may overtake national laws in this area. In 2009 the e-Privacy Directive was revised to require data breach notification by telecommunications providers and Irish law will have to be amended to implement this obligation by 25 May 2011.¹²⁹ A review of the Data Protection Directive is also underway at the time of writing, and it seems likely that in the revised Directive mandatory data breach reporting will be included.¹³⁰

With respect to government departments and State agencies, the Government's Centre for Management and Organisation Development published guidelines on data protection in

¹²⁶ See generally EDRI-gram, No. 6.8, May 2008, "EDPS Endorses Data Breach Notification Provision in ePrivacy Directive", available at <http://www.edri.org/edriagram/number6.8/edps-data-breach-notification>.

¹²⁷ EDRI-gram, No. 6.9, May 2008, "Important Personal Data Lost by the Bank of Ireland", available at <http://www.edri.org/edriagram/number6.9/personal-data-bank-ireland>.

¹²⁸ Data Protection Commissioner, "Personal Security Breach Code of Practice," July 2010, available at http://www.dataprotection.ie/docs/7/7/10_-_Data_Security_Breach_Code_of_Practice/1082.htm. If the Code were approved by the *Oireachtas*, it would have the force of law and the Data Protection Acts specifically provide for an approved code to be taken into account in court proceedings. However, the Code has not been approved and is therefore guidance only.

¹²⁹ See "Report of the Data Protection Review Group," March 2010, at 6-7, available at <http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwithcover.pdf>.

¹³⁰ *Ibid.*, 10-11.

December 2008 which apply to the public service in Ireland.¹³¹ These include guidelines on data security breach management which are similar to the Code of Practice published by the DPC and which recommend immediate notification of a breach internally and to the DPC (along with *An Garda Síochána* if appropriate).

Online targeted advertising and search engine privacy

Nothing to report.

Online social networks and virtual communities

Nothing to report.

Online youth safety

Nothing to report.

TERRITORIAL PRIVACY

Video surveillance

Nothing to report.

Location privacy (GPS, mobile phones, location based services, etc.)

It is a criminal offence to harass another person. Pursuant to section 10 of the Non-Fatal Offences Against the Person Act 1997, the offence includes harassment by use of a telephone, by persistently following, watching, pestering, besetting, or communicating with the victim. Harassment occurs where a person seriously interferes with the other person's peace and privacy or causes alarm, distress, or harm to the other, and these acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.

In 2009, the DPC agreed a policy document with *An Garda Síochána* to govern the use of the automated number plate recognition (ANPR) system introduced by the *Gardaí*. The system involves the use of an in-car camera which recognises the vehicle registration number (VRN) of other road users. These VRNs are checked against a watch list of vehicles maintained by the *Gardaí* and, if the vehicle is on the list, details are provided to the *Gardaí*. The DPC noted that any large-scale recording of personal data must be proportionate and acceptable safeguards must be in place. The ANPR policy agreed with the *Gardaí*'s aims to balance the effective use of the system with respect for the rights and privacy of individuals.

Irish law has since 2006 made provision for the electronic tagging of certain convicts and, since 2007, for the electronic tagging of certain persons released on bail pending

¹³¹ At <http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf>.

trial.¹³² At the time of writing, however, these systems have yet to be deployed. The implementation of electronic tagging is currently being considered by a Project Board appointed by the Minister for Justice and Law Reform in January 2009.¹³³

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The Irish government had previously chosen to comply with the US requirement of a biometric passport for visa waiver countries by providing a "secure printed digital photograph" without encoding any information electronically on the card. At the time it was the only European government to take this minimalist approach.¹³⁴ Since then, however, the Irish government has introduced ePassports which are described by the Department of Foreign Affairs as follows: "While the new biometric passport will look much the same as its predecessor, it will have a microchip embedded in it which contains the digitised facial image and personal details of the passport holder as they appear on the data page. The microchip can be read electronically at border controls. The Government has no plans, at this stage, to include a citizen's fingerprints."¹³⁵

NATIONAL ID & SMART CARDS

In 1998 a unique personal identification number system for use in dealing with public agencies was established. The Personal Public Service Number (PPSN) replaced the "Revenue and Social Insurance" (RSI) number that, for years, was used only for social welfare and tax purposes. The use of the PPSN has expanded considerably since 1998 and it is arguably becoming a national identity system "by stealth".¹³⁶ The PPSN is used as a unique personal identifier in communications between the individual and specified state agencies, such as government departments, hospitals, local authorities, and educational institutions. Employers may also use the PPSN for interaction with state bodies (most notably the Revenue Commissioners), while some state agencies have used

¹³² See Tanya Moeller, "Game of Tag", *Gazette of the Law Society of Ireland*, March 2008, at 34, available at <http://www.lawsociety.ie/Documents/Gazette/Gazette%202008/March2008.pdf>. The relevant legislative provisions are contained in the Criminal Justice Act 2006 and the Criminal Justice Act 2007.

¹³³ Department of Justice and Law Reform, "Electronic Monitoring", available at <http://www.justice.ie/en/JELR/Pages/WP09000043>.

¹³⁴ "US Lawmakers Question the Need for Microchips in European Passports," IDABC e-Government News, 26 April 2005, available at <http://ec.europa.eu/idabc/servlets/Doc?id=21683>; however, it should be noted that the new type passport announced on 10 December 2004, will have a polycarbonate page capable of holding a chip of some description if one is introduced. See <http://foreignaffairs.gov.ie/home/index.aspx?id=25621>.

¹³⁵ Department of Foreign Affairs, "ePassports Press Release", 4 October 2006, available at <http://www.dfa.ie/home/index.aspx?id=3029>.

¹³⁶ Cian C. Murphy, "From RSI to National Identity Number?: Tracking the Development of the Personal Public Service Number", Irish Association of Law Teachers Annual Conference 2006, available at <http://ssrn.com/abstract=917661>.

the PPSN as a unique identification number for their own employees.¹³⁷ Most recently, landlords have been permitted to seek tenants' PPSNs for the purposes of registering with the Private Residential Tenancies Board, although there is no obligation on tenants to provide it.¹³⁸

The Act allows for the exchange of personal data between prescribed bodies in certain circumstances, and its provisions in this respect are expressly exempt from the Data Protection Act. However, it is clear from the Social Welfare Acts and the PPSN Code of Practice published by the Department of Social Protection¹³⁹ that a PPSN can be requested or used only by specified public bodies or persons authorised by those bodies to act on their behalf. It is a criminal offence to request or hold a PPSN without the requisite legal authority.

The Register of users of the PPSN maintained by the Department of Social Protection bears testament to the zeal with which various state agencies have engaged in data matching and exchange exercises.¹⁴⁰ The DPC criticised this scheme while it was debated, stating that "the proposed sharing of personal data, obtained and kept by legally separate entities, for such diverse purposes is fundamentally incompatible with...the basic tenets of data protection law."¹⁴¹ In February 2004, the Department of Social Protection issued a Code of Practice on the use of the PPSN, and recognises its potency and its status as personal data under the Data Protection Acts, but does not attempt to unduly constrain its use.

The DPC has repeatedly pointed out his concerns about the PPSN system, noting the increased use of the PPSN as an identifier in his 2009 report. The DPC "availed of every opportunity during 2009 to highlight [its] serious concerns as to the suitability of the PPSN as a national Unique Health Identifier (UHI)" and a 2009 report by the Health Information and Quality Authority on UHIs reached the conclusion that the PPSN is not fit for purpose as a UHI.¹⁴² The Department of Health is due to publish a Health Information Bill which will provide a legal basis for the use of health information and which should address privacy concerns. It is expected that the bill would provide further responsibilities to the DPC in relation to health information.

¹³⁷ The Department of Education uses the PPSN as the main identifier on primary and post-primary teacher payrolls, while Cork County Council intends to use it for similar purposes.

¹³⁸ Residential Tenancies Act of 2004, at s. 136(f), available at <http://www.oireachtas.ie/viewdoc.asp?DocID=3183>.

¹³⁹ Department of Social Protection, Personal Public Service Number Code of Practice <http://www.welfare.ie/EN/Topics/PPSN/Pages/cop.aspx>.

¹⁴⁰ Register of users of the PPSN, available at <http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx>.

¹⁴¹ Irish Data Protection Commissioner, Annual Report, at 35 (1996); see also "Remarks by the Data Protection Commissioner on the Bill to the *Dail* Select Committee on Social, Community and Family Affairs" (4 March 1998).

¹⁴² At http://www.hiqa.ie/media/pdfs/Unique_Health_Identifier_Report.pdf.

The *Gardaí* and armed forces, at present, are prohibited from collecting and using the PPSN for matters other than those related to their own members. The Immigration Act 2003, however, gives power to *An Garda Síochána* to use the PPSN in relation to non-EU nationals.¹⁴³

Although at present the system does not incorporate an ID card *per se*, a public services card (PSC) has been under development for a number of years. The PSC would use the PPSN as a unique identifier and would include a photograph and signature as identification mechanisms.

In 2009, the *Oireachtas* Joint Committee on Social & Family Affairs published a report on social welfare fraud, recommending that the development of an integrated services card be fast-tracked.¹⁴⁴

"To this end, the Committee believes that biometric information should be incorporated into the public services card in order to eliminate the possibility of fraud and to facilitate this card becoming a national identity card. The Committee supports the introduction of a national identity card and believes that it is fundamental that the public services card which is currently in development be designed in such a way that it will later be able to incorporate data from other government departments and agencies."

The report shows no evidence of having considered the human rights or data protection implications of introducing such a system of national ID cards, not to mention the desirability of such a system and the possibility of further function creep.¹⁴⁵

RFID tags

Nothing to report.

BODILY PRIVACY

The Criminal Justice (Forensic Evidence and DNA Database System) Bill 2010, before the Houses of the *Oireachtas* at the time of writing, is a bill that will authorise the taking of bodily samples from those suspected of certain criminal offences and those who volunteer to have such samples taken from them for the purpose of the investigation of offences, or incidents that may have involved the commission of offences. If enacted, it will establish a statutory system for the collection of DNA samples, the creation of DNA profiles and the establishment of a DNA database against which profiles can be matched. (*See more details under the "Genetic privacy" section.*)

¹⁴³ Immigration Act 2003, available at <http://www.irishstatutebook.ie/2003/en/act/pub/0026/index.html>.

¹⁴⁴ See http://www.oireachtas.ie/viewdoc.asp?fn=/documents/Committees30thDail/J-SocialFamilyAffairs/Reports_2009/20091021.doc.

¹⁴⁵ Such arguments have been rehearsed in detail in the United Kingdom, for example, where the ID card system has been abolished by the new Conservative/Liberal Democrat government.

WORKPLACE PRIVACY

Statutes governing the processing of genetic data and its use in testing have an impact on privacy in the workplace: the Data Protection (Processing of Genetic Data) Regulations 2007 provide that the processing of genetic data in relation to the employment of a person can only take place with the DPC's prior approval. Then the Disability Act 2005 places certain restrictions on genetic testing and the use of data resulting from it. Consent to such testing must be obtained and the results cannot be used in relation to employment, insurance, pensions or housing loans.

(See more details under the "Genetic privacy" section.)

HEALTH & GENETIC PRIVACY

Health privacy

Nothing to report.

Genetic privacy

There is, at the time of writing, no statutory DNA database in Ireland although Irish law does permit the collection of genetic samples for evidential use at trial, based in part on both common law police powers and in part on the Criminal Justice (Forensic Evidence) Act 1990.¹⁴⁶

In 2005 the Law Reform Commission published a report which recommended the establishment of a DNA database on a legislative basis.¹⁴⁷ That report was followed by the publication of proposals for a Criminal Justice (Forensic Sampling and Evidence) Bill 2007. These proposals were, however, the subject of strong criticism from the Irish Human Rights Commission, which expressed concern over a number of features of the proposed Bill, particularly the provisions which would allow indefinite retention of samples.¹⁴⁸

However, before those proposals could progress any further the decision of the European Court of Human Rights in *S. and Marper v. UK*¹⁴⁹ intervened. That decision, which found the law on DNA collection and retention in England, Wales, and Northern Ireland to be in breach of the ECHR, forced a reconsideration of the Irish proposals, which appeared to share many of the same failings. Consequently, the 2007 proposals were not taken further. Instead, after further consideration in light of *S. and Marper*, a substantially revised

¹⁴⁶ Liz Campbell, "Development of a DNA Database in Ireland – Assessing the Proposed Legislation" (2010) 7 *Irish Law Times* 106.

¹⁴⁷ Law Reform Commission, Report on the Establishment of a DNA Database (2005), available at http://www.lawreform.ie/_fileupload/Reports/rDNADatabase.pdf.

¹⁴⁸ Irish Human Rights Commission, "Observations on the General Scheme of the Criminal Justice (Forensic Sampling and Evidence) Bill 2007", available at <http://www.ihrc.ie/download/doc/observationsonthednabill.doc>.

¹⁴⁹ (2009) 48 EHRR 50.

scheme was put forward in 2010 in the Criminal Justice (Forensic Evidence and DNA Database System) Bill 2010.

This 2010 bill is before the Houses of the *Oireachtas* at the time of writing and, if enacted, will establish a statutory system for the collection of DNA samples, the creation of DNA profiles, and the establishment of a DNA database against which profiles can be matched. It is described as a bill which will authorise the taking of bodily samples from those suspected of certain criminal offences and those who volunteer to have such samples taken from them for the purpose of the investigation of offences, or incidents that may have involved the commission of offences.

Although a detailed consideration of the 2010 Bill is beyond the scope of this country report – and in any event would be premature as the Bill is likely to be amended in the course of being passed – it should be noted that the Bill in many ways is improved over the 2007 proposals. In particular, it reverses the earlier presumption in favour of indefinite retention, and instead establishes default periods for the destruction of samples (three years) and the deletion of profiles (ten years), except in the case of convicted offenders.

The Irish Human Rights Commission has however expressed some concern about aspects of the 2010 Bill¹⁵⁰ as such legislation obviously raises significant data protection issues. The DPC has made submissions to the Minister for Justice relating to the Bill in light of the European Court of Human Rights decision in *S. and Marper v. United Kingdom*.¹⁵¹

Outside of the law enforcement field, the Data Protection (Processing of Genetic Data) Regulations 2007 provide that the processing of genetic data in relation to the employment of a person can only take place with the DPC's prior approval.

The Disability Act 2005 places certain restrictions on genetic testing and the use of data resulting from it. Consent to such testing must be obtained and the results cannot be used in relation to employment, insurance, pensions or housing loans.

FINANCIAL PRIVACY

Between June and October 2007, the unencrypted personal data of about 10,000 customers of the Bank of Ireland were stolen.¹⁵² They included, in addition to medical history, life insurance details, names, and addresses, customers' bank account details.¹⁵³ However, the bank did not notify the Data Protection Commissioner of the privacy

¹⁵⁰ Irish Human Rights Commission, "Observations on the Criminal Justice (Forensic Evidence and DNA Database System) Bill 2010", available at <http://www.ihrc.ie/download/doc/obscriminaljusticednabillmarch10.doc>.

¹⁵¹ 4 December 2008 (application nos. 30562/04 and 30566/04).

¹⁵² EDRI-gram, No. 6.9, May 2008, "Important Personal Data Lost by the Bank of Ireland", available at <http://www.edri.org/edriagram/number6.9/personal-data-bank-ireland>.

¹⁵³ *Id.*

breach until April 2008, ten months after the first theft.¹⁵⁴ (*See more details under the "Internet & Consumer Privacy" section.*)

E-GOVERNMENT & PRIVACY

In relation to electoral records, the Electoral Amendment Act 2001 makes specific provision for the establishment of an edited electoral register similar to a system already deployed in the United Kingdom. Local authorities must now prepare two versions of the electoral register, a full one that can only be used for electoral and statutory purposes, and an edited version that will contain the names and addresses of those who have indicated their willingness to be contracted by commercial entities.¹⁵⁵ It is an offence to use information from the edited register for any purpose other than an electoral or statutory purpose.¹⁵⁶

Voting is a right for all those 18 years or older, but is not obligatory.¹⁵⁷ In February 2002, the government allowed the use of electronic voting to be tested in public elections. An Interim Report of the Commission on Electronic Voting, dated 29 April 2004, rejected the use of direct recording electronic (DRE) voting machines in the upcoming elections.¹⁵⁸ The report states that "publication of ballot results in full...can in theory...allow voters to identify themselves in a context of corruption or intimidation,"¹⁵⁹ which could undermine the integrity of an election. This e-voting technology report led to the decision to abandon electronic voting in Ireland for the June 2004 EU elections.¹⁶⁰ Voting machines were once again not used in the 2007 parliamentary elections. After a period of uncertainty as to the future of electronic voting, in 2009 the decision was taken to scrap the electronic voting system¹⁶¹ and dispose of the voting machines.

¹⁵⁴ See generally EDRI-gram, No. 6.8, May 2008, "EDPS Endorses Data Breach Notification Provision in ePrivacy Directive", available at <http://www.edri.org/edriagram/number6.8/edps-data-breach-notification> and EDRI-gram, No. 6.9, May 2008, "Important personal data lost by the Bank of Ireland", available at <http://www.edri.org/edriagram/number6.9/personal-data-bank-ireland>.

¹⁵⁵ Section 4.

¹⁵⁶ Section 13A, Electoral Act 1992 as inserted by section 4, Electoral Amendment Act 2001.

¹⁵⁷ CIA Country Fact Book, January 1, 2004, available at <http://www.cia.gov/cia/publications/factbook/>.

¹⁵⁸ Interim Report of the [Ireland] Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, 29 April 2004, available at <http://www.cev.ie/htm/report/V02.pdf>.

¹⁵⁹ *Id.*

¹⁶⁰ Mark Hennessy & Mark Brennock, "E-voting Abandoned for Elections in June," *The Irish Times*, 1 May 2004, available at <http://www.irishtimes.com/newspaper/frontpage/2004/0501/1083224453260.html>.

¹⁶¹ "Electronic Voting System to Be Scrapped", RTE News, 23 April 2009, available at <http://www.rte.ie/news/2009/0423/evoting.html>.

OPEN GOVERNMENT

The Freedom of Information Acts 1997 and 2003 create a presumption that the public can access documents created by government agencies and requires that government agencies make internal information on their rules and activities available. The Office of the Information Commissioner enforces the Act. The 2003 amendments to the legislation were widely criticised by the opposition, press, and, indirectly, by the Ombudsman. The amendments resulted in more central control over information and the restriction of all information, instead of just a subset. Specifically, the amendment: doubled the time restriction on government records, regardless of content; introduced processing fees on information requests under the Act; broadened the definition of "government" under the Act; increased government exemptions to information requests; and granted ministers the ability to suppress information release, without appeal, by another ministry or public body. However, Emily O'Reilly, current Ombudsman and Information Commissioner, is an outspoken critic of the amendments to the FOI Act. Ms. O'Reilly, a well-respected journalist, is the first replacement commissioner since the office was created. The Commissioner publishes an annual report describing her activities in the previous year, and reports are available on the Commissioner's website.¹⁶²

In a review of the operation of the amending legislation issued in June 2004, Ms. O'Reilly found that overall use of the Act had fallen by 50 percent while requests for non-personal information fell by 75 percent. In relation to journalists using the FOI Act, there had been an 83 percent drop in requests. The fees structure introduced by the amendment can largely be blamed for this sharp decline. The Information Commissioner has called for a reappraisal of the fees, which can amount to €240 when retrieval, internal appeal, and appeal to the Information Commissioner are considered.¹⁶³

Ms O'Reilly has often criticised the scope of the FOI Acts on the basis that it is too limited and that the acts should be extended to cover institutions such as the Central Bank, the Financial Services Regulatory Authority of Ireland, National Asset Management Agency, and the National Treasury Management Agency.¹⁶⁴ Journalists accounted for 15 percent of the requests submitted, requests to the Department of Finance increased by 131 percent and requests to the Department of Enterprise, Trade, and Employment grew by 37 percent.¹⁶⁵

¹⁶² Freedom of Information Commissioner Annual Reports, available at <http://www.oic.gov.ie/en/MediaandSpeeches/PressReleases/Archive/>.

¹⁶³ Review of the Operation of the Freedom of Information (Amendment) Act 2003, available at <http://www.oic.gov.ie/en/Publications/SpecialReports/InvestigationsComplianceReportsSection36/File,571,en.pdf>.

¹⁶⁴ Paul Cullen, "Requests for Information on Rise, Says Ombudsman," *The Irish Times*, 29 April 2009, <http://www.irishtimes.com/newspaper/ireland/2009/0429/1224245598316.html>.

¹⁶⁵ *Id.*

OTHER RECENT FACTUAL DEVELOPMENTS (WITH AN IMPACT ON PRIVACY)

In its June 1998 Report on "Privacy, Surveillance and the Interception of Communications,"¹⁶⁶ the Law Reform Commission recommended legislation to make illegal the invasion of a person's privacy through secret filming, taping and eavesdropping, and the publication of information received from such surveillance.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

The manner of the passage into law of the Criminal Justice (Terrorist Offences) Act 2005, which introduced a three-year period of data retention for telephone traffic and location details, was heavily criticised by civil rights groups. In particular, despite the length of time the government had to publish legislation on the issue and despite repeated promises of dedicated legislation, the provisions were inserted as a last-minute amendment into a largely unrelated bill.¹⁶⁷

The Irish online civil rights group Digital Rights Ireland (DRI) commenced a High Court action against the Irish Government in 2006, challenging the Criminal Justice (Terrorist Offences) Act 2005, on the basis of Irish and European Law.¹⁶⁸

In May 2010, the High Court decided that DRI's challenge should be referred to the European Court of Justice under Article 267 of the Treaty on the Functioning of the European Union.¹⁶⁹ As of the end of July 2010, the High Court has not published the questions to be referred to the ECJ.

(See more details under the "Data retention" section.)

¹⁶⁶ 1998 Report on "Privacy, Surveillance and the Interception of Communications (LRC 57 -1998), available at http://www.lawreform.ie/publications/data/lrc99/lrc_99.html.

¹⁶⁷ Karlin Lillington, "McDowell's Sneaky Data Law Heralds Surveillance State," *The Irish Times*, 25 March 2005.

¹⁶⁸ Digital Rights Ireland, "Data Retention - Advocate General Recommends Irish Government Challenge Should Be Rejected", 28 October 2008 <http://www.digitalrights.ie/2008/10/14/data-retention-advocate-general-recommends-irish-government-challenge-should-be-rejected/>.

¹⁶⁹ Digital Rights Ireland Ltd. v. Minister for Communication, Marine and Natural Resources and others (unreported, High Court, McKechnie J., 5 May 2010), available at <http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs>.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

On 10 December 1948 the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights.¹⁷² On 8 December 1989, Ireland ratified the International Covenant on Civil and Political Rights.¹⁷³

Ireland is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).¹⁷² It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁷³ Ireland has incorporated the Convention into domestic law by way of the European Convention on Human Rights Act 2003. In February 2002, Ireland signed the CoE Convention on Cybercrime.¹⁷⁴ In 2007, Ireland signed the CoE Conventions against Trafficking in Human Beings¹⁷⁵ and on the Protection of Children against Sexual Exploitation and Sexual Abuse.¹⁷⁶ In 2008, the Convention on Prevention of Terrorism was signed.¹⁷⁷ Ireland is also a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

¹⁷¹ International Covenant on Civil and Political Rights, 16 December 1966, available at <http://www2.ohchr.org/English/law/ccpr.htm>.

¹⁷² Signed 18 December 1986; enacted 25 May 1990; entered into force 1st August 1990.

¹⁷³ Signed 11 November 1950; enacted 25 February 1953; entered into force 3 September 1953.

¹⁷⁴ Signed 28 February 2002.

¹⁷⁵ Council of Europe Convention on Action against Trafficking in Human Beings, CETS No.: 197, available at <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=197&CL=ENG>, signed 13 April 2007.

¹⁷⁶ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No.: 201, available at <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=201&CL=ENG>, signed 25 October 2007.

¹⁷⁷ Council of Europe Convention on the Prevention of Terrorism, CETS No.: 196, available at <http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=196&CL=ENG>, signed 3 October 2008

ITALIAN REPUBLIC*

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Even though the Italian Constitution, adopted in 1948, protects the secrecy of communication and personal domicile, there is no explicit reference to a stand-alone right of privacy. Thus, the legal statute of privacy derives from the analysis of those constitutional provisions that implies its existence, as suggested by the Italian Constitutional Court jurisprudence since its Decision No. 38 from 14 April 1973.¹

Among the most relevant provisions we find Article 2 of the Italian Constitution: "The Republic recognises and guarantees the inviolable human rights, be it as an individual or in social groups expressing their personality, and it ensures the performance of the unalterable duty to political, economic, and social solidarity."² Then, Article 14 establishes, "(1) Personal domicile is inviolable. (2) Inspection and search may not be carried out save in cases and in the manner laid down by law in conformity with guarantees prescribed for safeguarding personal freedom. (3) Special laws regulate verifications and inspections for reasons of public health and safety, or for economic and fiscal purposes." Article 15 states, "(1) The liberty and secrecy of correspondence and of every form of communication are inviolable. (2) Limitations upon them may only be enforced by decision, for which motives must be given, of the judicial authorities with the guarantees laid down by law."³

The legal status of privacy, meant as the right to obtain a correct and complete representation of "personal identity," also derives from Article 3 of the Italian Constitution that states, "All citizens have equal social status and are equal before the law, without regard to their sex, race, language, religion, political opinions, and personal or social conditions. It is the duty of the Republic to remove all economic and social obstacles that, by limiting the freedom and equality of citizens, prevent full individual development and the participation of all workers in the political, economic, and social organisation of the country".⁴

¹ See collection of articles published by Interlex, available at <http://www.interlex.it/675/indice1.htm>. See also Interlex, available at <http://www.interlex.it/675/indice2.htm>"><http://www.interlex.it/675/indice2.htm>.

² The Constitution of the Italian Republic promulgated in the extraordinary edition of Gazzetta Ufficiale No. 298, 27 December 1947, in force from 1 January 1948, Art. 2, available in English at http://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf.

³ *Id.* at Artt. 14 and 15.

⁴ *Id.* Art. 3.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Data Protection Code⁵ relating to the protection of personal data was enacted by a Legislative Decree of 30 June 2003.⁶ The Code replaced the Data Protection Act (which was enacted on 31 December 1996, after 20 years of debate,⁷ to fully implement the European Union (EU) Data Protection Directive 1995/46/EC as well as the various decrees enacted after 1996 to regulate data protection in specific sectors, such as security requirements,⁸ the processing of medical information,⁹ the processing of information for journalistic,¹⁰ scientific, or research purposes,¹¹ and personal data held by public bodies.¹² The new Data Protection Code (the Code) therefore covers all the requirements from previous data protection decrees, and from both the EU Directive 2002/58/EC on Privacy and Electronic Communications and the EU Directive 2006/24/EC on Data Retention, along with some codes of conduct already approved by the Italian Data Protection Authority.¹³ Among the most relevant amendments to the Code that have occurred in recent years, it is worth mentioning the Legislative Decree No. 207 that doubled the fines for all administrative violations.¹⁴ In 2009, the Law No. 15 integrated Article 1 of the Code by providing that "reports about the performance benefits of anyone employed on a public function and its evaluation are not subject to the protection of privacy".¹⁵

⁵ Decreto Legislativo No. 196. The consolidated text of the Code is available in Italian and English at <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FI+Codice+in+materia+di+protezione+dei+dati+personali>.

⁶ "Italy Enacts a New Privacy Code," BNA World Data Protection Report Vol. 3, Issue 9, September 2003, at 19.

⁷ Legge No. 675 (Law), 31 December 1996, amended by Decreto Legislativo No. 123 (Legislative Decree), 9 May 1997, and Decreto Legislativo No. 255, 28 July 1997, available at <http://www.privacy.it/dl1997123.html>; Legge No. 676, 31 December 1996, Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (Delegation to the Government on the Protection of Persons and Other Subjects Regarding the Processing of Personal Data).

⁸ Decreto del Presidente della Repubblica No. 318 (Decree of the President of the Republic), 28 July 1999. The cited decree and the other various decrees enacted after 1996 to regulate data protection in specific sectors are all available at <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FLeggi+e+decreti+legislativi>.

⁹ Decreto Legislativo No. 282 (Legislative Decree), 28 July 1999.

¹⁰ Decreto Legislativo No. 171 (Legislative Decree), 13 May 1998.

¹¹ Decreto Legislativo No. 281 (Legislative Decree), 30 July 1999.

¹² Decreto Legislativo No. 135 (Legislative Decree), 11 May 1999.

¹³ See <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana>.

¹⁴ Decreto Legislativo No. 207, 30 December 2008, Art. 44.

¹⁵ Legge No. 15, 4 March 2009, Art. 4 paragraph 9.

After strong criticism of the old law, the Code aimed to create, with little practical effect, a higher level of protection for data subjects while simplifying the applicable rules.¹⁶ The Code is arranged in three sections: the first one contains provisions dealing with the rules applicable to the processing of personal information in the public and private sector; the second section focuses on "special requirements" which would apply in those specific fields, such as debtors or the health sector; finally, the third section concerns administrative and judicial issues.¹⁷ Violators of the Code may also face harsh administrative or criminal penalties, as occurred in the Google-Vividown case decided by the Tribunal of Milan on 24 February 2010. On that occasion, three Google executives were sentenced to a six-month suspended jail for violation of the data protection law.¹⁸

Sector-based laws

Italy also has several laws relating to video and workplace surveillance,¹⁹ statistical information, electronic files, and digital signatures.²⁰

There are some important provisions about data protection in the field of electronic communications that are stated in other laws or regulations. The reference is to the anti-spam rules contained in the Italian Law of electronic commerce (Legislative Decree No. 70 of 9 April 2003) and to the secrecy of correspondence rules in the Italian Code of Electronic Communications (Legislative Decree No. 259 of 1 August 2003).

DATA PROTECTION AUTHORITY

The Supervisory Authority for Personal Data Protection (*Garante per la Protezione dei Dati Personali* or *Garante*) enforces the Italian Data Protection Code.²¹ The *Garante* maintains a register of databases, conducts audits and supervises the enforcement of the law. The *Garante* can also audit databanks not under its jurisdiction, such as those relating to intelligence activities. The Decree on the Internal Organisation of the *Garante*²² establishes the procedures for keeping the Register of Data Processes and regulates access to the register by citizens, or for investigations, registrations, and inspections.

¹⁶ See the extensive articles collection published by Interlex, *supra*.

¹⁷ *Id.*

¹⁸ See the section "Major Privacy & Data Protection Case Law," *infra*.

¹⁹ Legge No. 93, 29 March 1983.

²⁰ Decreto del Presidente della Repubblica No. 513 (Decree of the President of the Italian Republic), 10 November 1997, available at <http://www.privacy.it/dpcm19990208.html>.

²¹ "Garante per la Protezione dei Dati Personali," available at <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?solotesto=N>.

²² Decreto del Presidente della Repubblica No. 501 (Decree of the President of the Italian Republic), 31 March 1998, reprinted in Gazzetta Ufficiale No. 25, 1 February 1999, the decree was subsequently partly repealed by the Data Protection Code.

The *Garante* is responsible for carrying out many activities. As of May 2010, there are 33 different sectors in which the *Garante* has intervened. Among these sectors there are video surveillance, public transport, telemarketing and communications, spamming, minors and security measures, journalism and the health sector, biometrics, insurance and finance, and associations.

Enforcement actions the *Garante* carries out are mainly based on both the reaction to complaints lodged by data subjects for failure to exercise their rights (access, rectification, deletion), and on inspection or audit activities carried out either *ex officio* (based on an annual action plan identifying specific sectors and/or processing operations) or following complaints and reports.

Significant enforcement activities were carried out in the biometrics sector. The *Garante* stopped two initiatives by public bodies considering the use of fingerprint-based systems. In one case, the data controller required low-income university students and/or scholarship recipients to submit their fingerprints if they wanted to receive discounted access to restaurants and shops. In another, a local municipality required their employees to be fingerprinted to check their attendance at the workplace. The Italian DPA argued that the use of biometrics-based mechanisms was disproportionate compared with the purposes to be achieved, and that specific privacy safeguards (such as enhanced security measures) were necessary given the highly sensitive nature of biometric information.²³ In 2008 the *Garante* authorised several banks to use biometric systems for security purposes.²⁴ Recently, on 15 April 2010, the *Garante* authorised the bank Brescia to use fingerprints in order to allow access to clients' safe deposit boxes.²⁵

Some of the *Garante*'s decisions have had an impact on Italian public opinion. For example, in October 2006, the *Garante* blocked the broadcast of a media investigation revealing that an Italian Member of Parliament used cannabis extensively. This decision raised strong criticism, mostly based on the alleged lack of jurisdiction over the issue.²⁶

²³ "Recent Examples of Enforcement Actions Carried Out by Data Protection Authorities," Article 29-Data Protection Working Party, (Article 29 WP Report) January 2005, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

²⁴ See <http://www.garanteprivacy.it/garante/doc.jsp?ID=1490382> and <http://www.garanteprivacy.it/garante/doc.jsp?ID=1490463> (both in Italian).

²⁵ In Italian at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1719879> <http://www.garanteprivacy.it/garante/doc.jsp?ID=1719879>.

²⁶ See Andrea Monti, "Il caso 'Le Iene' e la funzione del Garante", available at <http://www.interlex.it/675/amonti87.htm>. A TV programme called *Le Iene* sent a make-up artist to the Parliament home that – posing as a TV journalist – swabbed MPs' eyebrows to collect droplets of perspiration. All the swabs were immediately anonymised so that it wasn't possible to match the swab with the MP's identity. The Data Protection Code doesn't allow the *Garante* to claim jurisdiction over human tissue samples because a sample – *per se* – doesn't meet the legal definition of Personal Data. Nevertheless the *Garante* blocked the show.

In May 2008, the Italian Revenue Office (*Agenzia delle Entrate*) released the fiscal records of Italian citizens online.²⁷ After a few days, the *Garante* tried to block the massive disclosure of personal information published on the Internet and through peer-to-peer networks.²⁸ In July 2008, a small company in Milan sold an online database with email addresses, fax, and telephone numbers – lawfully taken from public records, but the company did not inform the data subjects to whom those data belonged. The *Garante* prohibited the company from continuing to use, store, and sell that data.²⁹ On 6 October 2008, the *Garante* fined two marketing research firms for a breach of privacy. The companies carried out an opinion poll without informing the data subjects of the purpose for which their opinions were collected.³⁰ On the same day, the *Garante* ruled that access to personal data contained in records concerning a deceased person must be guaranteed free of charge to the deceased's family.³¹

On 15 January 2009, the *Garante* ordered a famous Italian publisher to redesign its own online database containing the articles of the most important Italian newspaper, *Il Corriere della Sera*, so as to prevent the possibility that that information could directly be traced back by a search engine. As a case of the individual's "right to be forgotten," the *Garante* aimed to strike a balance between personal data protection and people's right to be informed, so that the data subject's request to have his name deleted from the article was dismissed by the supervisory authority. Two other cases handled by the *Garante* during 2009 concerned newspapers and TV channels that had published pictures taken directly from Facebook when commenting on the death of two individuals, even though the pictures in question did not correspond to the deceased individuals but rather to namesakes. The *Garante* considered that publication of those pictures was in breach of data protection legislation as the accuracy of the information collected had not been checked thoroughly and erroneous personal information had been disseminated. Another important decision in this area reiterated that filming and using images of individuals within private premises without the individuals' consent was unlawful. The *Garante* prohibited the dissemination/publication by whomsoever of images acquired and/or obtained in breach of the safeguards applying to private premises, in particular

²⁷ Cfr. Section "Financial Privacy," *infra* in this Report.

²⁸ See "Vuoto normativo? La legge che vieta è già in vigore" ("Regulatory Gap? The Prohibiting Law is Already in Force"), *Il Sole24Ore*, 3 May 2008.

²⁹ *Garante per la Protezione dei Dati Personali*, "Vende dati on line, ma non informa gli interessati e scatta il divieto del Garante" ("The *Garante* prohibits Online Selling of Personal Data without Informing Data Subjects"), 29 July 2008, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1536569>.

³⁰ *Garante per la Protezione dei Dati Personali*, "No ai sondaggi 'occulti'" ("No Hidden 'Surveys'") *Notiziario Settimanale* No. 313, del 6 October 2008, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1553314><http://www.garanteprivacy.it/garante/doc.jsp?ID=1553314>.

³¹ *Garante per la Protezione dei Dati Personali*, "Conti correnti: è gratuito l'accesso ai dati personali dei familiari defunti" ("Bank Accounts: Free Access to Personal Data of Deceased Relatives") 6 October 2008, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1553314><http://www.garanteprivacy.it/garante/doc.jsp?ID=1553314>.

considering the privacy-intrusive techniques implemented to capture those images, the lack of consent by the relevant data subjects, and the exclusively personal nature of the activities shown in those images.³² However, on 11 September 2009, the *Garante* declared that other pictures of Mr. Berlusconi, namely on a pier and in his private beach in Villa Certosa, Sardinia, are legal and do not represent an illicit treatment of personal data, due to the nature of the places.³³

Along with enforcement actions and the ever-growing number of its case studies, the *Garante* carries out further functions with regard to data protection. These functions involve the drafting of guidelines and codes of conduct. Since 2001, the *Garante* issued a Code of Conduct and Ethics Regarding the Processing of Personal Data for Historical Purposes, including guidelines on the protection of personal data in election activities such as campaign literature and elections.³⁴ In 2005, the *Garante* issued guidelines on privacy issues related to RFID tags, loyalty cards, digital TV (e.g., pay-per-view) and video communications.³⁵ In 2006, the *Garante* released guidelines on the collection of personal information of employees in the workplace.³⁶ In 2006-2007, the *Garante* continued to work on the draft of a code of practice applying to the Internet with the participation of a large number of representatives from the private sector.³⁷ In 2007, the *Garante* promoted a round table with Internet Service Providers, access operators, and other concerned bodies to enforce the draft code of practice. As of June 2010, this self-regulation draft code is still a work in progress, with no prospect of a release date.³⁸ In 2008, the *Garante* established the legal framework for all of the electronic systems processing personal data. In November 2008, the *Garante* issued another Code of Conduct and Ethics Regarding the Processing of Personal Data for Private Investigations carried out by lawyers and their "private eyes".³⁹ In 2009, new guidelines were delivered

³² Garante per la Protezione dei Dati Personali, "Fotografie riprese all'interno di luogo di dimora privata: divieto di diffusione" (Photographs Taken in Private Residences: Disclosure Prohibited), 18 June 2009, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1623306>.

³³ Garante per la Protezione dei Dati Personali, "Le foto di Berlusconi sul pontile potevano essere pubblicate" ("Pictures of Berlusconi on the Pier Could Be Published"), Press Release, 11 September 2009, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1649435>.

³⁴ Garante per la Protezione dei Dati Personali, "Personal Data and Elections-Instructions for Use," 7 March 2001.

³⁵ Italian Data Protection Authority, Consultation on RFID, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1078227> <http://www.garanteprivacy.it/garante/doc.jsp?ID=1078227>.

³⁶ In Italian at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1368292>.

³⁷ 10th Annual Report of the Article 29 Data Protection Working Party (2006), 20 June 2007, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

³⁸ Email (report) sent by Andrea Monti, Vice President, ALCEI – Electronic Frontiers Italy to Katitza Rodriguez Pereda, EPIC International Privacy Project Director, 2008 (on file with EPIC).

³⁹ Available in English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1569165>.

in the health sector, concerning the management of health dossiers and e-files, as well as online medical reports.⁴⁰

On 27 November 2008, the *Garante* simplified the security measures contained in the technical specifications to the Data Protection Code (set out in Annex B).⁴¹ On the same day, the Authority adopted a Decision concerning Measures and Arrangements Applying to the Controllers of Processing Operations Performed with the Help of Electronic Tools in View of Committing the Task of System Administrator.⁴²

On 25 June 2009 the *Garante* reviewed and recast this decision to enhance the safeguards for data subjects in connection with the activities performed by "system administrators" – a concept that is actually not defined expressly by the Italian law.⁴³ The new text was meant to clarify various points, partly to take account of queries lodged with the *Garante*. The requirements set forth by the *Garante* had to do more specifically with access logging (systems must be in place to log accesses to processing systems and electronic databases as performed by system administrators); supervision by data controller on the activities performed by system administrators (to verify that they are compliant with the organisational, technical and security measures provided for in data protection legislation); drafting of a list of system administrators and their features (containing information to identify system administrators including a list of the functions committed to them), which should be reported by each data controller in an internal document that should be made available for inspection by the *Garante*.

Since 2003, the *Garante* has launched public information television campaigns to inform the public of their rights with regard to the collection of personal data.⁴⁴ In the same year, the *Garante* began work on a do-not-call strategy to deter unwanted marketing calls.⁴⁵ In addition, nearly every year the *Garante* hosts a conference in Rome. Topics have ranged from human genetics to the future of privacy.⁴⁶ During the 2009, the *Garante* decided to launch an initiative targeted to students on the occasion of European Data Protection Day

⁴⁰ Available in English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1683328> <http://www.garanteprivacy.it/garante/doc.jsp?ID=1683328> and <http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821>.

⁴¹ In English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1619241>.

⁴² In English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499>.

⁴³ In Italian at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1626595>.

⁴⁴ "Non e' una firmetta!" ("It's Not Only a Signature!"), Newsletter of the Garante per la Protezione dei Dati Personali, No. 163 (17-23 March 2003), available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=66974>.

⁴⁵ "Nuovi elenchi telefonici: chiarezza nelle informazioni agli abbonati" ("New Telephone Directories: Clear Information to Subscribers") Newsletter of the Garante per la Protezione dei Dati Personali, No. 163 (24 February -2 March 2003), available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=34804>.

⁴⁶ See generally, Garante per la Protezione dei Dati Personali, *supra*.

(28 January).⁴⁷ Additionally, a booklet was produced by the *Garante* in 2009 to provide guidance (especially to youth) in dealing with social networks and making a knowledgeable use of their potential.⁴⁸

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In addition to legislative action, there are several decisions on the judicial front that have crucially dealt with the right to privacy.⁴⁹ A decision by the Council of State (*Consiglio di Stato*) addressed the relationship between the right of access and the right to privacy, ruling that the laws in force do not provide general guidance on how to balance these two rights. The decision allows an administrative body holding sensitive data to assess each specific situation in order to determine whether access is necessary or not to establish or defend a claim that is at least equal to the data subject's claim to privacy.⁵⁰ In another decision concerning this issue, the Council of State ruled that the right of access, albeit in its "softened" version, i.e., as the right to inspect records, should override the right to privacy if knowledge of the information is required to exercise the right of defence with regard to circumstances amounting to a criminal offence.⁵¹ Furthermore, since two relevant decisions issued in 2003, the Court of Cassation has ruled that non-pecuniary damage should be construed as a wide-ranging category including all cases in which there is violation of a value pertaining to human beings. The use of unlawful means in collecting personal data was expressly mentioned among the cases the Court considered to entitle to protection against the damage caused by the violation of individual-related interests devoid of pecuniary value.⁵²

On 4 October 2006 the Court of *Brescia* ruled that it is a Constitutional violation if the Public Prosecutor seizes a computer belonging to a non-investigated person and collects data not related to the investigation itself.⁵³

On 1 August 2008, the Court of Bergamo issued a preliminary investigation order requesting the "seizure" of the Pirate Bay website. The Pirate Bay displayed a collection of links to allegedly copyright-infringing material; however, the website is hosted outside Italy. On 10 August 2008, the order was implemented by forcing Italian Internet

⁴⁷ *Cfr.* Sections "Online social networks and virtual communities" and "Online youth safety," *infra* in this Report. See <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FIniziativa%2FGiornata+europea+della+protezione+dei+dati+personali>.

⁴⁸ *Cfr.* "Online social networks and virtual communities," *infra* in this Report.

⁴⁹ Other relevant case law concerning privacy and data protection is categorized and discussed under the corresponding section. *Cfr.* Sections "Data Protection Authority", *supra*, "Wiretapping, access to, and interception of communications," *infra*, "Cybercrime," *infra*.

⁵⁰ Cons. Stato 4002/2003 Foro It. V. Stato.

⁵¹ Cons. Stato 9276/2003 Foro It. V. Stato.

⁵² Cass. 8827/2003, 8828/2003.

⁵³ Court of Brescia, Ordinanza 4 Ottobre 2006, at <http://www.ictlex.net/?p=566>.

providers to block the domain name of the website as well as its associated IP numbers. On 29 September 2009, the Court of Cassation (*Corte di Cassazione*), which is the highest court in Italy, declared the "seizure" legal pursuant to Article 171 *ter* (2 *a bis*) from Act No. 633/1941.

Then, on 16 August 2008, Electronic Frontiers Italy (ALCEI-EFI) reported the violations of law contained in the preemptive seizure order issued by the Judge for the preliminary investigation of the Bergamo Tribunal to the Italian Data Protection Authority.⁵⁴ ALCEI-EFI explained that the enforcement of the Court order exceeded what the Judge had said. "Users attempting to connect to the 'seized' site are redirected to the IP number 217.144.82.26, belonging to servers located in the United Kingdom and apparently registered by the *pro-music.org* domain, a music industry association protecting intellectual property rights. If the above is true, then a private association, outside the Italian jurisdiction, is collecting Internet traffic data that, when matched with those retained by the ISPs, will allow the identification and possible criminal investigation of third parties absolutely not involved in the Bergamo's criminal case."⁵⁵

On 7 October 2008, the Bergamo Criminal Court overruled the seizure. According to ALCEI-EFI, "The Bergamo Court had overruled the seizure, but only on a legal technicality. As it had been pointed out by ALCEI, that 'seizure' cannot be interpreted as 'traffic hijacking'."⁵⁶ Even after the aforementioned decision by the Court of Cassation from 29 September 2009, this crucial issue still seems controversial.

Among the most relevant recent cases is the aforementioned Google-Vividown case decided by the Tribunal of Milan on 24 February 2010. The reasons why three Google executives were sentenced to a six-month suspended jail hinge on Article 167 of the Code, i.e., illicit treatment of personal data, and Articles 23 and 26 on sensitive data. The defendants, in other words, were convicted because they would have obtained an illicit gain by participating in the processing of the video of a disabled teenager without either his consent or the authorisation of the *Garante*. Most scholars, however, argue that users should be personally held liable for what they do online, as confirmed by cases of defamation and privacy or copyright infringements, so that ISPs as well as social network services should be held liable only when they fail to remove illegitimate content after having been asked to do so by a judicial or administrative authority. The decision has sparked lively reactions while raising a number of hot legal issues, e.g., the applicability of the Italian law on data protection to this case, the distinction between data processor and data controller, ISPs duties of information on the Web 2.0, and the idea that cookies on people's PCs should be considered as an "equipment" pursuant to Article 4(1) of the

⁵⁴ Electronic Frontiers Italy, "An Update on the Piratebay Case," available at <http://www.alcei.org/?p=38>.

⁵⁵ See Italian justice wants to "seize" a foreign website, available at <http://www.edri.org/edrigram/number6.16/italy-blocks-piratebay>.

⁵⁶ "An Update on the Piratebay Case," *supra*.

EU Directive on data protection. A decision by the Court of Appeal in Milan is expected in 2011.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The constitutional principles of the secrecy of communication and the inviolability of the domicile have been enforced in the Criminal Code (*Codice Penale*). In particular, Section 615 *bis* – "Illegal Interference with Private Life" (*Interferenze illecite nella vita privata*) – establishes sanctions for whomever commits illegal interference into a third party's private life by means of video or audio recording tools. Further provisions establish sanctions for hacking into computer systems that under Italian law are protected as private domicile.⁵⁷

Wiretapping is regulated by Articles 266-271 of the Criminal Procedure Code (*Codice di Procedura Penale* or CPP) and may be authorised only for a "legal proceeding," except in the case of terrorism related investigations.⁵⁸ In fact, after 11 September 2001, "preemptive wiretapping" can be done even if no Public Prosecutor investigation is in progress.⁵⁹ In particular, in October 2001, the Italian Parliament passed a decree⁶⁰ in which the offence of criminal association for purposes of terrorism was redefined. However, the blanket surveillance of communications by law enforcement bodies was expressly ruled out. Telephone tapping and electronic surveillance were facilitated but only with due authorisation and under the supervision of judicial authorities. Additional safeguards apply to the use of investigatory findings and the prohibition to disclose such findings.⁶¹ The current legal framework establishes common provisions as well as special regimes for wiretapping and surveillance law. In November 2006 a Law was enacted

⁵⁷ *Codice Penale*, Section 615 *bis*, *ter et alia*.

⁵⁸ Decreto del Presidente della Repubblica No. 447 (Decree of the President of the Italian Republic), Approvazione del Codice Procedura Penale (Adoption of the Criminal Procedure Code), 22 September 1988.

⁵⁹ *Id.*

⁶⁰ Decree No. 374/2001, converted into Act No. 438/2001.

⁶¹ On 7 January 2003, Giuseppe Pisanu, the Italian Interior Minister, went before Parliament to address terrorism concerns. His testimony was supplemented by a "report in which he warned of a growing climate of 'widespread political illegality' which must be monitored and combated." See "Italy: Interior Minister Link Terrorism and Activists," Statewatch News Online, February 2003, available at <http://www.statewatch.org/news/2003/feb/02italy.htm>.

which allows magistrates to destroy illegal wiretaps if discovered by police.⁶² In Italy, the publication of legitimate wiretap transcriptions is regulated by the Code of Criminal Procedure, in particular by its Article 114 – that prohibits the publication of "acts covered by secret" (*atti coperti da segreto*) and regulates the publication of acts "no more covered by secret" (*non più coperti da segreto*) or "not covered by secret" (*non coperti da segreto*) –, Article 115 – that establishes criminal liability and the "disciplinary action" against civil servants that violate the prohibition on publication – and Article 329 regulating the "duty of secrecy".

Over the last few years, however, this subject matter has sparked a hot debate and, on 10 June 2010, the Italian Senate proposed a Bill (No. 1611) so as to modify current provisions on wiretapping. The Bill substantially curtails legal powers of Public Prosecutors and makes administrative and criminal penalties harsher for cases involving illegal wiretaps. One of the bill's provisions – heavily criticised by legal and police authorities – is the requirement that a three-judge panel approve successive three-day extensions to an initial 75-day warrant to wiretap conversations. The measure exempts Mafia and terrorism investigations. The law foresees a penalty of up to €450,000 for publishers and 30 days in jail and up to €10,000 for journalists who publish leaked material obtained through wiretaps before the beginning of a trial. In addition, documents related to ongoing investigations may not be published in full, but only as an abstract. According to the draft law, publishers who flout this ban face a fine of up to €300,000.⁶³ Whereas most of the new provisions are quite problematic, the Italian Parliament is expected to examine the Bill in autumn 2010. Italian supporters of the bill claim it is necessary in order to protect privacy and curb the excessive use of wiretaps. Major concerns are raised, in Italy and abroad, that this decree would harm most pending and future trials for major crimes, advantage criminals, and have the effect of harming or stopping a number of famous trials involving politicians and VIPs. In a speech given at the presentation of the 2009 Annual report, the *Garante* criticised the measure as being too unbalanced in favour of a general protection of privacy without specific references to specific cases.⁶⁴

On the other hand, search and seizure of Internet Service Providers storing digital information needed for criminal investigation purposes are subject to CPP.⁶⁵ While a search and seizure warrant is the Attorney's General decision, wiretapping needs an

⁶² Law No. 281, 20 November 2006 regulating the destruction of unlawfully wiretapped communication records and providing legal consequences for their illicit use. See also US Department of Commerce, Italian Report on Human Rights Practices, 11 March 2008, available at <http://www.state.gov/g/drl/rls/hrrpt/2007/100566.htm>.

⁶³ Barbara Trionfi, "Italian Senate Approves Restrictive Wiretap Law," 10 June 2010, International Press Institute, at <http://www.freemedia.at/singleview/4984/>.

⁶⁴ The speech is available in English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1738746>.

⁶⁵ Rules of Evidence and Criminal Trial Code, Section 254 and 254 bis.

Attorney General's request to the Judiciary for a "pre-emptive investigation". Only if the legal requirement is met may the Attorney General issue a wiretapping order.⁶⁶

In the specific field of privacy online or digital privacy, the law on computer crimes includes penalties for the interception of electronic communications.⁶⁷ Interception orders are granted for 15 days at a time and may be extended for the same length of time by a judge. The judge also monitors procedures for storing recordings and transcripts. Any recordings or transcripts that are not used must be destroyed. The conversations of religious ministers, lawyers, doctors, or others subject to professional confidentiality rules cannot be intercepted. There are more lenient procedures for anti-Mafia cases.

On 18 March 2008, the Italian Parliament enforced the Convention of Budapest on Cybercrime⁶⁸ with the Act No. 48, which modifies Articles 244 and 247 CPP in order to guarantee both the integrity and quality of the data to be used in criminal trials. Still, the new provisions do not clarify the distinction between "searches" and "wiretaps" as it occurs in the paradigmatic case of SMS/MMS and whether it should be applied Article 254 CPP on search or the more "liberal" Article 266 *bis* CPP on wiretaps.

On 21 June 2005, the Italian collective and Internet service provider (ISP) Austistici/Inventati discovered a major police backdoor in its server, which hosts a large number of websites, mailboxes, mailing lists, and Internet services for NGOs, grassroots activists, and public interest associations. The Italian *Polizia Postale* (Postal Police) installed the backdoor the year before, after the *Procura di Bologna* (Office of the Public Prosecutor of Bologna) ordered a seizure during an investigation of the anarchist collective Crocenera. The police gained access to the private SSL certificate stored on the server and installed several tools to monitor, intercept and decrypt all the traffic going through the server – that is, traffic that was not directly relevant to the investigations. This included the communications of more than 30,000 of the ISP's subscribers, whose basic rights to privacy and presumption of innocence, as granted under the Italian constitution, were violated.

In 2005 and 2006, the new internal security team of Telecom Italia, which reports directly to the CEO of the company, collected thousand of files regarding politicians, reporters, influential people in the financial sector, stars, and soccer players. This was done using both the internal wiretapping capabilities of Telecom Italy (which owns most of the physical phone and communication network in Italy) as well as covert (and illegal) decoding activities by the members of the Telecom Italia security team. This activity resulted in over 20 charges of having used the above information to gain unfair advantages against competitors and to blackmail individuals for politic and/or economic gain. The first hearing of such a complex case was held before the Tribunal of Milan on 23 March 2009. By May 2010, the 25th hearing had taken place and it seems there is still

⁶⁶ *Id.*

⁶⁷ Legge No. 547, 23 December 1993.

⁶⁸ Cfr. "International Obligations & International Cooperation," *infra* in this Report.

a long way to go. Meanwhile, the *Garante* issued a decision requiring Telecom Italia to "implement IT solutions that are suitable for ensuring supervision over the activities carried out by any and all persons in charge of any kind of processing with regard to the individual items of information included in the databases in use, regardless of the individual person's capacity, tasks, and scope of activity as authorised in respect to the data at issue," and fined the Telecom €500 (only!), to be paid to a complainant.⁶⁹

In August 2007, an Italian judge ruled that installing bugging devices in a car was "not a criminal offence" because the provisions forbidding bugging apply only to the inviolability of the home. The ruling arose in Brescia, northern Italy, where a private detective agency specialising in infidelity cases offered to plant hidden microphones and satellite tracking devices in the cars of suspected spouses, at a cost of up to €1,500. The judge suggested that Parliament should take another look at Italy's privacy laws. In the judgment No. 28251 of 9 July 2009, the Court of Cassation, IV Penal Section, established that the car is not comparable to a private house, and therefore installing in the car a device that would be able to record the sound of what happens inside it doesn't entail a privacy breach.⁷⁰

National security legislation

In July 2005, the Italian government passed Act No. 155/2005 as "urgent measures to enhance the prevention of and fight against international terrorism." The Act greatly expands law enforcement powers in anti-terrorism investigations. In 2007, the UN High Commissioner for Human Rights Subcommittee on Torture issued recommendations concerning Italian legislation. In the report, the Committee voiced concern that fundamental legal safeguards for persons detained by the police, including the right of access to a lawyer, are not being observed in all situations under Act No. 155/2005 (the "Pisanu Decree"). The Committee was concerned that the Act includes a provision that extends the permissible period of deprivation of liberty by the police for identification purposes from 12 to 24 hours. The Committee recommended immediate amendment of the Act.⁷¹

On 21 July 2007, Italian law enforcement made three arrests under Act No. 155/2005. The law empowers police to arrest individuals without any evidence of involvement with terrorist groups or in the planning of terrorist attacks. After two years of surveillance, police still lack concrete evidence against the trio. Under the new measures, training

⁶⁹ Garante per la Protezione dei Dati Personali, Decision on the Need for Enhanced Security Measures in Processing Telephone Traffic Data, 1 June 2006, available at http://ec.europa.eu/justice/policies/privacy/docs/policy_papers/italy/telecom_security_jun06.pdf.

⁷⁰ Corte di Cassazione, IV Sezione Penale, Judgment No. 28251/2009, 9 July 2009. See also Roberto Codini, "Spiare la ex in automobile non è interferenza illecita" ("Spying an Ex-girlfriend in the Car is not an Unlawful Interference with Private Life"), 15 July 2009, at http://www.cittadinolex.kataweb.it/article_view.jsp?idArt=88725&idCat=75.

⁷¹ UN Committee Against Torture, Consideration of Reports Submitted by States Parties under Article 19 of the Convention, 18 May 2007, available at <http://www2.ohchr.org/english/bodies/cat/cats38.htm>.

others to commit an attack and the possession of dangerous materials is enough for conviction.⁷²

Data retention

Legislative Decree No. 109/08 enforced EU Directive 2006/24/CE and amended (again) the Data Protection Code by setting a new legal framework for data retention concerning both the traffic data to be retained, and the period of retention (two years for telephone traffic and one year for Internet traffic). The companies had a further six months (until 31 October 2008) to comply with the requirements imposed by law and delete five years of data stored until then because of the "Decreto Pisanu" and subsequent numerous extensions.⁷³

However, the *Garante* on 17 January 2008 ruled that telephone operators had until 30 April 2009 to finally comply with the Internet and telephone data traffic retention requirements established by law.⁷⁴ In the IT community this is regarded as proof that ISP's and telephone companies only consider important the IT implementation of legal requirements regarding data retention, underestimating the ones regarding deletion; in other word implementing only mandated investigatory needs and not citizen privacy rights.

National databases for law enforcement and security purposes

In order to enforce the Treaty of Prüm⁷⁵ of 2005, as well as the EU Decision 2008/615/GAI,⁷⁶ the Parliament passed the Law No. 85 of 30 June 2009, on a national DNA database.⁷⁷ More particularly, the provisions distinguish between DNA profiles and biological samples of convicted persons, thereby establishing two different databases under the control of the Departments of Justice and Internal Affairs. Pursuant to Article 9 of the Law, the retention of both DNA profiles and biological samples concerns a specific

⁷² "Italy Arrests Terror Suspects," ISN ETH Zurich, 27 July 2007, available at <http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?id=53584&lng=en>.

⁷³ See Manlio Cammarata, *Dati del traffico: i nuovi tempi di conservazione* (Traffic Data: New New Time Limits for Storage), available at <http://www.interlex.it/675/datitraffico.htm>.

⁷⁴ *Garante per la Protezione dei Dati Personali*, "Dati traffico tlc e internet: proroga per i gestori." 1 September 2008, available in Italian at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1547213>.

⁷⁵ Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime, and illegal migration, Prüm, 27 May 2005, available at <http://www.libertysecurity.org/IMG/pdf/Prum-ConventionEn.pdf>.

⁷⁶ Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 23 June 2008, OJ L 210 6 August 2008, at 1–11, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:01:EN:HTML>.

⁷⁷ Legge No. 85, 30 June 2009, available in Italian at http://www.interno.it/mininterno/export/sites/default/it/sezioni/servizi/legislazione/accordi_internazionali/0996_2009_06_30_Legge_ratifica_Trattato_Prum.html.

set of convicted persons or people arrested while committing a crime. Notwithstanding the remarks of the *Garante* on 15 October 2007, national law-makers have established a huge period of data retention, that is, according to Article 13 of the Law, 40 years for DNA profiles and 20 years for biological samples. By considering the ruling of the European Court of Human Rights on 4 December 2008, in *S. and Marper vs. UK*, it is nonetheless likely that these provisions should be deemed disproportionate pursuant to Article 8 of the European Convention on Human Rights.⁷⁸

Cybercrime

The 1993 computer crime law prohibits unlawfully using a computer system and intercepting computer communications.⁷⁹

Since a decree-law issued in March 2004, the responsibilities of Internet service providers (ISPs) are increasing, even though it is still debatable whether they should report who among their users engages in peer-to-peer file sharing.⁸⁰ At the end of May 2004, Italy passed one of the world's toughest laws against piracy and file sharing.⁸¹ Penalties include a prison term of up to three years and fines that can exceed approximately €220,000. The Culture Ministry said that the law was necessary to protect the intellectual property rights of artists in light of the growing popularity of peer-to-peer networks. An early version draft of the Urbani Law (from the Minister's surname) included a special penalty for using encryption as tool to disguise illegal activities. This provision was not included in the final text.

In the light of this trend, it is thus likely that the Italian public will soon discuss the "three strikes" doctrine, already passed by some national Parliaments in Europe, so that Internet users should be logged off after three notices of copyright infringement.

On 14 July 2007, the Civil Court of Rome ruled in a peer-to-peer case where a music label asked the Court to force a telecommunications company to release the identity of customers suspected of copyright infringement using peer-to-peer software. A private company collected the IP number of 3,000 peer-to-peer users. The Court ruled that collection of an IP number for this purpose by a private entity is a violation of Articles 2 and 15 of the Italian Constitution as well as Articles 13, 23 and 37 of the Code, thus preventing this data from being used in Court.⁸²

⁷⁸ ECtHR (Gch), Applications Nos. 30562/04 and 30566/04, Case of *S. and Marper V. The United Kingdom*, Judgment of 4 December 2008, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbk&action=html&highlight=MARPER&sessionid=62835990&skin=hudoc-en>.

⁷⁹ Legge No. 547, *supra*.

⁸⁰ Decreto Legislativo No. 72 enforcing urgent actions to fight the illicit diffusion of audio-visual works and to sustain movie and entertainment activities, 22 March 2004.

⁸¹ Aidan Lewis, "Italy Passes Tough Internet Piracy Law," *USA Today*, 28 May 2004, available at http://www.usatoday.com/tech/news/techpolicy/2004-05-28-italy-piracy-law_x.htm?POE=TECISVA.

⁸² Court of Rome, Ordinanza 14 Luglio 2007, at <http://www.ictlex.net/?p=580>.

In July 2007, Italian law enforcement made 26 arrests from two separate groups of phishing fraudsters, in the culmination of an operation, dubbed "Phish and Chip", aimed at tracking down phishers defrauding banking clients of the national postal service *Poste Italiane*. The gangs were accused of sending out emails claiming to represent the *Poste Italiane*, and directing victims to faked websites to gather banking details, which were then used to strip accounts of funds. They are thought to have used casinos to enable larger withdrawals than offered by ATM cash machines. No details of the scale of the phishing activity have yet emerged. A judge involved in the case has called for improvements to the laws governing such fraud, including a specific crime of phishing, describing current legislation covering some of the crimes involved as "weak".⁸³ Accordingly, the Parliament strengthened the rules by modifying Articles 640 *ter* and 617 *quater-quinquies* of the Criminal Code via the Legislative Decree No. 231 from 2007.

INTERNET & CONSUMER PRIVACY

E-Commerce

The Italian Code considers the sending of unsolicited emails to be a very serious offence.⁸⁴ If an individual is found guilty of sending spam and trying to profit from such emails, he could face up to three years in prison. Since many companies are losing a large amount of bandwidth as a result of dealing with spam, the Italian government has now made spam an act of theft. Italy is one of the first countries to implement legislation that actively deals with combating spam. Critics remain skeptical of Italy's law, because many of the sources of spam are from outside the country and therefore outside the Italian court's jurisdiction.

The sending of spam, however, is an ever-recurring topic, not only as regards commercial messages, but also in connection with "political marketing". In 2004, the *Garante* issued two provisions. The *Garante* took part in meetings in which fixed and mobile telephony operators, consumer associations, and ISP associations participated. These meetings were focused on the drafting of a self-regulatory code.⁸⁵ In 2008-2009 the *Garante* received many requests for action against unsolicited messages (email, fax, phone calls, SMS). On several occasions, even after inspection findings, the Authority has prohibited the sending of promotional communications by mail to third parties without data subjects' prior, specific, and informed consent according to Article 130 of the Code.⁸⁶ In some case where unlawful processing was found, the *Garante* imposed administrative penalties according to Articles 161 and 162, paragraph 2-*Bis* of the Code) and informed the

⁸³ "26 Phishing Arrests in Italy," *Virus Bulletin*, 17 July 2007, at http://www.virusbtn.com/news/spam_news/2007/07_16.xml.

⁸⁴ Will Sturgeon, "Italy Plans to Jail Spammers," *Silicon.com*, 5 September 2003, available at <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,10005895,00.htm>.

⁸⁵ *Garante per la Protezione dei Dati Personali*, Annual Report for 2007, *supra*.

⁸⁶ See e.g. <http://www.garanteprivacy.it/garante/doc.jsp?ID=1520263>.

prosecution authority. With regard to "fax advertisements" to recipients who had received adequate information *ex* Article 13 of the Code, but who had never given their consent, the *Garante* adopted various restrictive measures and imposed administrative sanctions.⁸⁷ On 20 November 2009, the Act No. 166, Art. 20 *bis*, finally adopted an opt-out system for commercial information, thus reversing the opt-in mechanism introduced by the Code.

Online social networks and virtual communities

In the 2007 Annual Report, the *Garante* stressed the necessity to clearly determine whether the information contained in personal profiles on social networks is protected and used properly.⁸⁸ A Guide on Social Network Services and Privacy was finally adopted in March 2008. In the document, while mentioning the risks of the new digital environment, the *Garante* suggested a number of proactive measures like use of pseudonyms and the implementation of privacy by design. By stressing that data protection should be "embedded" in ICT through default settings, the idea is to prevent privacy infringement from the very beginning, through the incorporation of data protection safeguards in the use and employ of ICT.⁸⁹

Online youth safety

As previously mentioned,⁹⁰ during 2009, the *Garante* decided to launch an initiative targeted at students on the occasion of European Data Protection Day (28 January).⁹¹ The initiative was termed "Cinema & Privacy" and lasted four days; it was aimed at raising youths' awareness of the importance of protecting privacy in today's society and of the need for learning how to protect one's privacy. Movies chosen as particularly relevant in addressing privacy issues from different standpoints were shown at the Conference Room of the *Garante*. Each movie was introduced by one of the four members of the *Garante* as well as by a video created on purpose by the *Garante* to describe – again with the help of movies – minor and major "intrusions" into our private sphere. Students from high schools in Rome were invited to the shows and called upon to discuss and exchange views. Additionally, a booklet was produced by the *Garante* in 2009 to provide guidance (especially to youths) in dealing with social networks and making knowledgeable use of their potential. The booklet, called "Social Networks: Watch out for Side Effects" was

⁸⁷ See *e.g.* <http://www.garanteprivacy.it/garante/doc.jsp?ID=1667012>.

⁸⁸ *Garante per la Protezione dei Dati Personali*, Annual Report for 2007, full text in Italian available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1533131>. The English summary is available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1750234>.

⁸⁹ *Id.* See also the section "Online youth safety," *infra* in this report.

⁹⁰ See section "Data Protection Authority," *supra* in this report.

⁹¹ See <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FIniziativa%2FGiornata+europea+della+protezione+dei+dati+personali>.

made available for free in the main Italian post offices.⁹² This initiative was aimed at helping both experienced and inexperienced users to take full advantage of the potential inherent in these innovative communication tools without endangering their private and professional lives.

TERRITORIAL PRIVACY

Video surveillance

Along with a set of safeguards for storing and processing personal data, some recent provisions on video surveillance are nonetheless problematic. For example, Act No. 38 from 23 April 2009 allows municipalities to employ video surveillance in order to guarantee "urban security," although bypassing national provisions on data protection and, more particularly, Article 53 of the Code. It seems in fact clear that such provisions are not covered by the exceptions of "national security" or "public security" pursuant to Article 13 (let alone 3) of the EU Directive 1995/46/EC.

Since a decision adopted in April 2004, the *Garante* has referred to the basic principles on video surveillance and described the general requirements to be fulfilled by any video surveillance system. Guidance was also provided for specific data processing operations concerning the use of video surveillance in schools, hospitals, on board transportation means, and in the workplace. The *Garante* reserved the right to take *ad hoc* measures in particular situations on a case-by-case basis. It was determined that the basic criteria should be the respect for citizens' fundamental rights and freedoms as well as personal dignity, with particular regard to privacy, identity, and personal data protection.⁹³ Accordingly, the *Garante* stated that individuals may not be deprived of the right to move without interferences that are incompatible with a free democratic society,⁹⁴ such as those resulting from invasive and oppressive data acquisitions with respect to an individual's whereabouts and movements. The *Garante* also drew inspiration from the guidelines issued by several international and European fora such as, in particular, the Council of Europe's guidelines on video surveillance of 2003,⁹⁵ and the documents drafted by the European data protection authorities within the framework of the Article 29 Working Party.⁹⁶

⁹² Available in Italian and English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1614258>.

⁹³ See § 2(1) of the Data Protection Code.

⁹⁴ See Article 8 of the European Convention on Human Rights, as ratified in Italy by Legge No. 848/1955.

⁹⁵ Council of Europe, European Committee on Legal Co-operation (CDCJ), Report Containing Guiding Principles for the Protection of Individuals with regard to the Collection and Processing of Data by Means of Video Surveillance, 20-23 May 2003.

⁹⁶ Article 29 Data Protection Working Party, Opinion 4/2004 (WP 89) on the Processing of Personal Data by means of Video Surveillance, 11 February 2004, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2004_en.htm; Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance (WP 67), 25 November 2002, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2002_en.htm.

On 25 September 2008, the *Garante* announced that it would begin carrying out inspections of operators of video surveillance equipment to determine whether they comply with the Data Protection Code. The findings of the *Garante* also aimed to identify any issues not specifically covered by the legislation.⁹⁷ On 8 April 2010, the *Garante* finally set out the general principles of video surveillance and data protection, along with specific provisions for both the public and private sector, including security measures, data retention, and particular data subjects' rights like the partial ability to update their data in this field (pursuant to Article 3.5 of the *Garante's* decision).⁹⁸ According to the Decision the installation of cameras is permitted only if it is proportionate to the objectives it pursue; video surveillance systems should be activated only when other measures are inadequate or impracticable; any storage of images should be limited in time. Citizens should be informed if an area is subject to surveillance.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The Italian Ministry of Foreign Affairs issued a Decree on Electronic Passports in December 2005, according to which new passports should include an RFID proximity chip to store the image of the holder's face and both forefinger prints. The Decree states that the biometric information stored on the chip will not be stored in a central database, but will be used only for authentication purposes.⁹⁹ This decree was never applied and the Italian passports were modified only by inserting ordinary enhancements like printing computer-readable text and photo, because the negative privacy consequences of RFID features became an international affair. Further provisions were established by a new Decree of 23 June 2009, dealing with "the security of the ordinary e-passports."

The *Garante* considered the use and appropriateness of biometrics in relation to a project called *S-Travel*, which considered initial tests at the Athens and Milan Malpensa airports. Biometric authentication technologies, using fingerprints and/or iris scans, with particular regard to check-in and boarding operations, were the main issue. The *Garante* stated that it was necessary to comply with data minimisation and proportionality principles, as well as with data relevance and non-excessiveness requirements. In the case at issue, the technologies to be implemented were only partly suitable for achieving enhanced security of airport controls. Furthermore, the collection of biometric data related to both fingerprints and iris scans of both eyes was found to be excessive and disproportionate compared with the purposes of the processing. The *S-Travel* pilot projects have now concluded in Milan, but further implementation of the system is being considered.

⁹⁷ "Videosorveglianza: ispezioni del Garante privacy in tutta Italia" (Video Surveillance: Inspections of the Garante in the whole Country'), 25 settembre 2008, available at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1550089>.

⁹⁸ Decision on Video Surveillance, 8 April 2010, available in English at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653>.

⁹⁹ 9th Annual Report of the Article 29 Data Protection Working Party (2005), 14 June 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf.

NATIONAL ID & SMART CARDS

Starting in 2005 a fully electronic national identity document (*Carta di Identità Elettronica* or CIE)¹⁰⁰ conceived in 2000, was deployed in limited quantities. The original document design that wouldn't have stored the whole fingerprint but only its "features" and wouldn't have sent fingerprints to a central database was dropped in favour of a full fingerprint stored in both the smartcard and a central database. Also, the possibility for the CIE to refuse giving the fingerprint was dropped. The whole CIE initiative was silently dismantled in 2009.

On 31 March 2005, Law No. 43/2005 was adopted. The statute, which takes into account an Opinion on e-cards adopted by the *Garante*, consolidates various regulations regarding electronic ID cards, and indicates which data must be included on the card and which information may or not be included. DNA information can never be included on the card, even with the cardholder's consent. However, at the cardholder's express request, biometric data, blood group data, and organ donation information can be included. The move from paper cards to electronic cards is voluntary, and there will be no obligation to obtain an electronic card. The statute also includes security standards and encryption standards for storage of biometric data in the card's chip.¹⁰¹

Starting from 1 January 2010 all Italian ID, electronic or traditional, should have carried a printed fingerprint that would have been also centrally recorded in digital format.¹⁰² The Financial Law 2010 (*Legge Finanziaria* 2010) postponed the date to 1 January 2011.¹⁰³

RFID tags

The *Garante* has paid considerable attention to the development of radio frequency identification (RFID) technology.¹⁰⁴ An initial in-depth analysis of this issue was carried out by addressing the way in which the new technology might impact the conditions for the exercise of individuals' freedoms, as well as the issues that are bound to arise in a data protection perspective following implementation of the technology.¹⁰⁵

¹⁰⁰ Decreto Ministeriale 19 July 2000 "Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici," in *Gazzetta Ufficiale* 21 July 2000.

¹⁰¹ 9th Annual Report of the Article 29 Data Protection Working Party, *supra*.

¹⁰² "Dal 2010 impronte digitali per tutti sulle carte di identità" (Starting from 2010, all ID Cards will store fingerprints"), *IlSole24Ore.com*, at <http://www.ilsole24ore.com/art/SoleOnLine4/Norme%20e%20Tributi/2008/07/manovra-impronte-digitali.shtml?uuid=0413d2cc-5303-11dd-b353-a98d07585a6c>.

¹⁰³ Legge No. 191 del 23 December 2009, available at <http://www.parlamento.it/parlam/leggi/091911.htm>.

¹⁰⁴ Cfr. "Travel privacy(travel identification documents, biometrics, etc.) and border surveillance," *supra* in this report.

¹⁰⁵ *Garante per la Protezione dei Dati Personali*, Annual Report for 2007, *supra*.

The Winston Smith Project (Progetto Winston Smith),¹⁰⁶ an Italian NGO, has responded with a legal proposal to control the use of RFID tags. First, the organisation wants legal rules that oblige manufacturers to make RFID tags easily identifiable and removable. Second, the organisation says the presence, type, and position of RFID tags must be clearly advertised on the packaging of an article or the article itself. Third, the group requires permanent deactivation of RFID tags when buying the product or when usage of the tag has ended. Fourth, the group urges that all data collected by RFID readers be treated as personal data, to which all privacy principles apply. Fifth, the group says collection, storage, and further processing should only happen within the boundaries of a strict and publicly known goal. In case of additional processing or conservation for a longer time, companies should notify the *Garante*. Furthermore, the groups says these rules should not only apply to RFID-related data, but to all kinds of new electronic databases, such as GSM location data, web log files, and data generated by wireless networks.¹⁰⁷ The proposal 1728/2006 on Norms Regarding the Collection, Use, Storage, and Deletion of Geo-referenced or Chrono-referenced Data containing an Unique User Identifier Obtained through Automatic Data Collection was submitted to the Chamber of Deputies in 2006, dropped because of new elections in 2008, and resubmitted on 29 April 2008 as proposal 257/2008 and is currently "on hold" in the Justice Commission of the Italian Parliament.¹⁰⁸

BODILY PRIVACY

In 2008 the *Garante* addressed the case of a father who had performed a genetic test on his son without informing him, in connection with investigations he was carrying out to establish consanguinity.¹⁰⁹ A private investigation agency had collected two cigarette butts binned by the man's son, acting on instructions of the man's legal counsel. The biological samples had been tested, without informing the data subject, to establish genetic compatibility between father and son. The *Garante* ruled that a paternity/maternity test may not be performed without the child's consent if such test is not indispensable for judicial purposes. The Italian DPA recalled that genetic data may only be collected and processed with the data subject's "prior, written" and informed consent. This requirement may only be derogated from@@@ to establish or defend a judicial claim; however, this only applies if the test is absolutely "indispensable" and is carried out pursuant to the conditions set forth by the Italian DPA – which include, in particular, an

¹⁰⁶ Homepage <http://pws.winstonsmith.org/>.

¹⁰⁷ "Answer to RFID consultation Italian Privacy Authority," EDRI-gram newsletter Number 3.1, 12 January 2005, available at <http://www.edri.org/edriagram/number3.1/RFID>.

¹⁰⁸ Law proposal No. 1728 of 28th September 2006 "Norme in materia di raccolta, uso, conservazione e cancellazione di dati georeferenziati o cronoreferenziati, contenenti identificatori univoci di utente, effettuata mediante apparecchiature automatiche". See http://www.camera.it/_dati/lavori/schedela/trovaschedacamera_wai.asp?pd1=1728&ns=2.

¹⁰⁹ 12th Annual Report of Article 29 Data Protection Working Party (2008), 16 June 2009, at 58, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/12th_annual_report_en.pdf.

obligation to provide specific information to the data subject if the genetic test is aimed at establishing paternity/maternity. The *Garante* found that the son's data protection rights had been violated and prohibited both his father and the legal counsel from further processing the genetic information that had been unlawfully collected in the manner described above.

It seems likely that the *Garante* will soon address some further problems concerning the protection of people's privacy since, in January 2010, the Government introduced body scanner devices at airports, apparently violating Article 13 of the Constitution.

WORKPLACE PRIVACY

The Workers' Charter prohibits employers from investigating the political, religious, or trade union opinions of their workers, and in general, any matter that is irrelevant for the purposes of assessing their professional skills and aptitudes.¹¹⁰

On 2 February 2010, by sentence No. 4375/2010, the Court of Cassation, Job Section, stated that companies cannot spy on employees who surf the Web during office hours. The centralised computer monitoring of employees constitutes "a breach of their privacy and autonomy". In addition, if the navigation is done without encroaching on abuse the employee can not be fired.¹¹¹

HEALTH & GENETIC PRIVACY

Medical records

Legislative Decree No. 269 of 30 September 2003,¹¹² converted with amendments into Act No. 326 of 24 November 2003,¹¹³ set out the requirements to monitor health care expenditure. During the process leading to the conversion of the legislative decree, the *Garante* drew Parliament's attention to the sensitive issues raised by Section 50 in the decree, providing, *inter alia*, for the establishment of a database containing the fiscal identification codes of all health care beneficiaries in order to monitor health care expenditure. The *Garante* pointed out that the purpose the decree sought was undoubtedly in line with streamlining supervision over the state's expenditure; however, the tools envisaged to that end might jeopardise citizens' rights to the protection of their

¹¹⁰ Legge No. 300, 20 May 1970. § 8.

¹¹¹ Corte di Cassazione, Sezione Lavoro, Judgment No. 4375/2010, 2 February 2010. See also Roberto Cataldi, "Cassazione: non si spiano i dipendenti ed è illegittimo il licenziamento di chi naviga nel web" ("Court of Cassation: It Is Forbidden to Spy Employees and It Is unlawful to Fire who Is Surfing on Internet"), 25 February 2010, at http://www.studiocataldi.it/news_giuridiche_asp/news_giuridica_8080.asp.

¹¹² Decreto Legislativo No. 269, 30 September 2003.

¹¹³ Legge No. 326, 24 November 2003.

personal data – in particular the data concerning health, which are covered by special safeguards.¹¹⁴

On 1 January 2005, the Italian Electronic Health card was launched. Together with e-prescriptions, the e-Health card is a key element of the Italian national e-Health Programme, which aims at controlling public health expenses while improving communication between health professionals and delivering better services to patients. The card, which contains a magnetic stripe but no chip, also features the European e-health insurance card information on the back. They are used in conjunction with the National Healthcare Expenditure Monitoring System, commonly referred to as the "TS System." Designed to monitor and manage each phase of the public health expenditure cycle, from drug prescription to service delivery, the system will allow Italian authorities to enhance controls on the healthcare benefits of each citizen. The TS System is coordinated by the Italian Revenue Agency and implemented by Sogei¹¹⁵ in those regions where e-health cards are being issued. Distribution of the cards has already started in the Regions of Abruzzi, Umbria, Emilia Romagna, Veneto, and Lazio. The government will progressively introduce the e-health card in other regions, with the objective of issuing 15 million cards by April 2005.¹¹⁶ By June 2010, the goal of covering all of the regions of Italy was mostly achieved (with the safeguards we will illustrate in the section on major privacy case law).

The *Garante* has finally specified the conditions in which the right to privacy and the right of access to clinical records held by health care institutions could be balanced. This is an issue arising mostly in connection with the requests made by defence counsel carrying out their own investigations in order to access records containing data relating to health and/or sex life. In particular, the so-called "equal importance" principle holds that the processing of personal data in order to enable access is only allowed if the right to be defended through the request for accessing administrative records is at least as important as the data subject's rights, or else consists in a personal right or another fundamental, inviolable right or freedom. In other words, the defendant's rights must be equal to, or outweigh, the other individual's fundamental right to privacy.

¹¹⁴ Indeed, it would arguably always be possible to trace each data subject's medical history based on the information concerning prescriptions and specialists' advice. The *Garante* pointed out that the legislation in force already sets forth procedures to monitor health care expenditure without setting up centralised databases, and stressed that the need to increase the effectiveness of such procedures should not result in limiting the right to personal data protection. According to the *Garante*, in order to comply with personal data protection legislation, the monitoring system would have to prohibit the processing of identification data, and the setting up of a centralised database, if any, should be based exclusively on the use of anonymised data.

¹¹⁵ Homepage <http://www.sogei.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/1/>.

¹¹⁶ See "Italy eServices for Citizens," eGovernment News, 12 January 2005.

As reported above, on 16 July 2009, the *Garante* issued guidelines concerning the management of health dossiers and e-files, as well as online medical reports.¹¹⁷

FINANCIAL PRIVACY

In 2008, the *Garante* prohibited the Italian Revenue Office from posting the tax returns of all Italians on the Internet a few days after the data had been made public on the Revenue Office's website.¹¹⁸ Dissemination of the data was found to be in breach of the sector-specific legislation, which allowed for different, less privacy-intrusive mechanisms to obtain information on taxpayers' income. Posting the data on the Internet was also found to be disproportionate *vis-à-vis* the purpose of making available the information in question. The consequences of this blanket, unfiltered disclosure of the data concerning all Italian taxpayers were manifold. A considerable number of users in Italy as well as abroad were able to access a huge amount of data in the space of a few hours, since the data were available at a single source. They could copy the data, generate their own databases, modify and/or process the data, create profiling lists, and circulate the data further with all the attendant accuracy risks. In addition, it could be established that the Revenue Office had failed to request the Italian DPA's opinion – which is mandatory under the law – prior to adopting the decision to publish the data on the Internet.

A decision adopted in September 2008 took stock of the critical problems found by the *Garante* following several inspections that had been carried out with respect to the taxpayers' register – where millions of records on Italian taxpayers are kept and may be accessed, via different tools, by a considerable number of users including public and private bodies – and set forth the technological and organisational measures required to enhance security of access and bring the processing into line with data protection legislation.¹¹⁹ Given that the critical problems in question were related to the lack of information on the overall number of access-enabled users, poor monitoring of access and inappropriate use of passwords and user IDs, and the inadequate technological measures to ensure data security, the Italian DPA required regular monitoring of the access-enabled bodies and organisations; carrying out a survey of all data flows from and to the Register including the particulars of the entities able to access the Register, the applicable legal grounds, nature and type of the transferred data; partitioning the data that may be accessed to ensure that only such data may be viewed as the individual user is authorised to access; implementing alert systems to detect and prevent security breaches; implementing authentication/enhanced authentication mechanisms; logging access and restricting the maximum number of instances of access; implementing secure connection channels in case of web-based data flow management; timely disabling of users no longer entitled to access the relevant data.

¹¹⁷ See Section "Data Protection Authority," *supra* in this report.

¹¹⁸ Annual Report of Article 29 Data Protection Working Party (2008), *supra* at 55.

¹¹⁹ *Id.*

E-GOVERNMENT & PRIVACY

The e-government portal for citizens is currently being reengineered. A new portal will be realised, hardening the search function and implementing new features for rating the quality of on line services.¹²⁰

Adopted as a Legislative Decree on 7 March 2005 the e-Government Code (*Codice dell'Amministrazione Digitale*) entered into force on 1 January 2006.¹²¹ It aims to provide a clear legal framework for the development of e-Government and for the emergence of an efficient and user-friendly Public Administration.¹²² Among other things, the Code mandates Public Administrations to: share relevant information by electronic means in order to make life easier for citizens and businesses; make a minimum set of contents and services available on their websites, including a comprehensive organisation chart, an email directory, a list of e-Services, the possibility to download forms, and details on administrative procedures; communicate by email, namely for the exchange of documents and information; accept online payments from citizens and businesses; use the electronic ID card and the National Services Card, as a standard means of granting access to online services.¹²³

The provisions of this Code shall apply in respect of the regulations governing the processing of personal data and, in particular, the provisions of the Data Protection Code. Citizens and businesses are, however, entitled to require@@@ that data processing carried out by the Public Administration is consistent with the fundamental rights and freedoms, as well as dignity of the person concerned.¹²⁴

On 19 February 2010, the Italian Council of Ministers approved the new version of the e-Government Code proposed by the Ministry of Public Administration (PA) and Innovation. Once the approval procedure has been completed, the new Code will be published as a legislative decree.¹²⁵

The EU Directive 2003/98/EC on the access and re-use of public sector information (PSI) has been implemented with Legislative Decree No. 36 of 24 January 2006, and the Senate was emending it in Autumn 2010 so as to adequately respond to the European Commission's remarks on its infringement procedure from 19 March 2009. PSI can be re-used in many perspectives, i.e., not only to create added-value services but to improve public choices (e.g. e-governance) and to allow citizens to take part to public choices as

¹²⁰ See <http://www.italia.gov.it>.

¹²¹ The text of the Code is available in Italian at <http://www.altalex.com/index.php?idnot=9618>.

¹²² ePractice, eGovernment Factsheet – Italy – Legal Framework (May 2010), available at <http://www.epractice.eu/en/document/288279>.

¹²³ *Id.*

¹²⁴ eGovernment Code, *supra* at Art. 2 paragraph 5.

¹²⁵ ePractice, eGovernment Factsheet – Italy – Legal Framework, *supra*.

well (e.g. e-democracy). Although the EU Directive subordinates the processing and re-use of PSI to the provisions of Directive 1995/46/EC on the protection of personal data, most of the time access and re-use of PSI concerns information such as geographic and meteorological data, museums, and local archives metadata, land register data, and the like. Nevertheless, the *Garante* has recently addressed the re-use of PSI by private companies involving personal data on 26 March 2010.¹²⁶ On that occasion, the *Garante* has granted the right to collect and re-use (personal) information already available on public sector websites, excluding a duty to inform the individuals.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Electronic Frontiers Italy (ALCEI) has been active since 1994 in several fields.¹²⁷ A Founding Member of the Global Internet Liberty Campaign (GILC), ALCEI is also a member of the European Digital Rights Initiative (EDRI). ALCEI's recent activities include challenging in court the legal admissibility of non-computer forensics digital evidence; support media, journalists, and international civil rights NGOs with reliable information on civil rights issues.

The National Association for the Defence of Privacy (*Associazione Nazionale per la Difesa della Privacy* or ANDIP)¹²⁸ and the Italian Institute for Privacy¹²⁹ promote different activities aimed to develop a culture of privacy. They assist the *Garante* in its awareness-raising activities.

Italy's Big Brother Awards (organised by Privacy International and the Winston Smith Project, in association with 14 other organisations) announced the 2006 winners. The Trusted Computing Group won two awards "thanks" to the privacy implications associated with DRM technologies used to enforce intellectual property rights.¹³⁰

On 19 May 2007, the 2007 Italian Big Brother Awards were held.¹³¹ Telecom Italia received the "People's Complaint" award for its system of illegal eavesdropping of telephone conversations (especially for the aforementioned Tavaroli & Co case before the Tribunal of Milan). The Municipality of Milan won the award "The Worst Public

¹²⁶ Garante Italiano per la Protezione dei dati, "Esonero dall'informativa per un sito web che raccoglie e diffonde dati già disponibili online" ("Duty to Inform Exemption for a Website that Collects and Disseminates Data Already Available Online"), 26 March 2010, available in Italian at <http://www.garanteprivacy.it/garante/doc.jsp?ID=1721169>.

¹²⁷ Associazione per la Libertà nella Comunicazione Elettronica Interattiva, available at <http://www.alcei.it/>.

¹²⁸ At <http://www.difesaprivacy.it/>.

¹²⁹ At <http://www.istitutoitalianoprivacy.it/en/>.

¹³⁰ Big Brother Award Italia 2006 webpage, at <http://bba.winstonsmith.info/bbai2006.html>.

¹³¹ Big Brother Award Italia 2007 webpage, available at <http://bba.winstonsmith.info/bbai2007.html>.

Institution", receiving the prize for having installed several cameras in the city, starting with public parks, without giving any information on who would use the recorded data.¹³²

On 10 May 2008, the 2008 Italian Big Brother Awards were presented during an e-privacy convention in Florence.¹³³ The Ministry of Economics received the "Worst Public Institution" award. The Ministry had been empowered to create mass personal (bank, health, etc.) databases to fight against tax evasion. Yahoo! received the "Worst Private Company" award for providing the Italian Government with the personal data of its Internet users. The DNA Bank of the RIS (the Scientific Investigation Division of the "carabinieri") of Parma received the award for their most invasive technology, which was created "quietly" without any specific normative act. TV journalist Bruno Vespa was awarded the "Boot in the Mouth" prize for having dealt superficially with, and therefore misinforming people about, the Internet and new technologies. Franco Frattini, the Italian Minister of Foreign Affairs, received the lifetime award for having spread an idea of security that involves "monitoring and censoring dangerous words."¹³⁴

On 23 May 2009, the 2009 Italian Big Brother Awards went mostly to Facebook, which won three awards: "Worst private company", "Most invasive technology" and "People's Choice".

In 2010 Mr. Berlusconi received the "Neo-speech and Encore Thought" award, Facebook was awarded for "Lifetime Menace," "The Most Invasive Technology," "Worst Private Company," and, last but not least, "People's Complaint."¹³⁵ Facebook sets a new record in the annals of the Big Brother Awards, both Italian and International.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Italy has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol that establishes an individual complaint mechanism.¹³⁶

Italy is a member of several organisations that influence the country's treatment of privacy and personal data. Most notably, Italy is part of the Council of Europe (CoE) and has signed and ratified the European Convention for the Protection of Human Rights and

¹³² EDRI-gram, "The Italian Big Brother Awards for 2007," Number 5.10, 23 May 2007, available at <http://www.edri.org/edriagram/number5.10/Italy-BBA-2007>.

¹³³ Big Brother Award Italia 2008 webpage, at <http://bba.winstonsmith.info/bbai2008.html>.

¹³⁴ Digital Civil Rights in Europe, "BBA Awards Italy 2008", available at <http://www.edri.org/edriagram/number6.10/bba-italy-2008>.

¹³⁵ Big Brother Award Italia 2010 webpage, at <http://bba.winstonsmith.info/index.html>.

¹³⁶ Italy has signed the ICCPR on 18 January 1967 and ratified it on 15 September 1978; it has signed the First Optional Protocol to the ICCPR on 30 April 1976 and ratified it on 15 September 1978. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

Fundamental Freedoms (ETS No. 5).¹³⁷ It has signed and ratified the CoE's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).¹³⁸ In addition, Italy signed and ratified the CoE's Convention for Cybercrime.¹³⁹

Italy is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

However, as suggested by both the Italian *Garante* and the other European Data Protection Authorities over the last few years, further international and transnational provisions seem urgently necessary.¹⁴⁰

*Updates to the Italian Report published in the 2010 edition of EPHR have been provided by: Marco Calamari, Progetto Winston Smith, Italy; Michele Iaselli, Associazione Nazionale per la Difesa della Privacy, Italy; Ugo Pagallo, Università degli Studi di Torino, Italy; Guido Scorza, Istituto per le Politiche dell'Innovazione, Italy.

¹³⁷ Ratified on 26 October 1955. All CoE's conventions are available in English at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

¹³⁸ Ratified on 29 March 1997.

¹³⁹ Ratified on 5 June 2008.

¹⁴⁰ *Cfr.* i.e. Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection, 30th International Conference of Data Protection and Privacy Commissioners, Strasbourg, 17 October 2008, at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adaptados/common/proposal_international_standards_en.pdf.

REPUBLIC OF LATVIA

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 96 of the Latvian Constitution established a fundamental human right to privacy: "Everyone has the right to inviolability of their private life, home and correspondence."¹ All laws protecting privacy apply to citizens and non-citizens equally.²

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Personal Data Protection Law was adopted by the Parliament on 23 March 2000 and came into force in January 2001.³ The law is based on standard fair information practices and is fully compliant with the EU Data Protection Directive 1995/46/EC. The Personal Data Protection Law has been amended several times. In 2007 the Personal Data Protection Law was amended to determine exemptions from the notification obligations and to simplify notification procedures.⁴ In 2008 the law was amended to limit data subjects' right to be fully informed about what has been collected about them, if such rights have been limited by specialised laws intended to preserve the financial interests of the State in the tax field. Additionally, these amendments allowed the processing of sensitive personal data in cases of claimed insurance compensation.

In 2009 the Personal Data Protection Law was amended. It was strengthened by giving data subjects the right to submit requests and receive answers from the data controller, as well as to appeal against the data controller's actions (or inaction) to the Data State Inspectorate.⁵ Additionally, the requirement to register data processing with the Data State Inspectorate was abolished in the following cases: the data subject has given consent; the data processing derives from contractual obligations or, subject to a request by the data subject, is necessary in order to conclude a contract; the data subject's personal (identification) code is processed in accordance with the requirements set by the law; processing of personal data is carried out for scientific or statistical purposes or for the purposes of genealogical studies. On the other hand, these amendments established a

¹ Constitution of the Republic of Latvia, available in English at http://www.likumi.lv/doc.php?id=57980#saist_11.

² US State Department Human Rights Report 2002 – Latvia, available at <http://www.state.gov/g/drl/rls/hrrpt/2002/18375.htm>.

³ Personal Data Protection Law, available in English at <http://www.dvi.gov.lv/eng/legislation/pdp/>.

⁴ 11th Annual Report of the Article 29 Working Party on Data Protection, 24 June 2008, at 64, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

⁵ Amendments to the Personal Data Protection Law, 12 June 2009, available in Latvian at <http://www.likumi.lv/doc.php?id=193584>.

duty to register the processing of personal data with the Data State Inspectorate when personal data are transferred to a non-European Union or non-European Economic Association state; when processing of personal data is carried out for the purposes of providing financial services, carrying out market or sociological research, personnel selection or personnel evaluation (if this is done as a commercial activity or for the purposes of lotteries); when processing of personal data is related to health or crimes, criminal records, and administrative punishments. These amendments also abolished the requirement to register the data processor's internal and external auditors with the Data State Inspectorate, and delegated to the Cabinet of Ministers the responsibility to establish requirements for the auditor's report.

In 2010 the Personal Data Protection Law was further amended in order to widen the circumstances under which personal data may be processed to include purposes that were not initially envisaged (including in the sphere of criminal law), especially allowing processing of sensitive personal data in cases when patients data fixed in medical records are used for research purposes. The 2010 revision also eliminated the requirement to register with the Data State Inspectorate if the data processor has instead registered a personal data protection specialist.⁶

Personal data protection law does apply to the police sector.⁷ It also regulates the protection of personal data that is recognised as an official secret, with the exceptions set out in the Law on Official Secrets.⁸ This law applies specifically to personal data related to criminal offences, criminal records, court decisions, and other court files, which can only be processed by persons prescribed by law on the occasions provided for by law.

Sector-based laws

Some specific provisions regarding the processing of personal data are contained in sector-based legislation such as, for example, the Law on Electronic Communication or the Law on Establishment and Use of National Database of DNA.⁹

DATA PROTECTION AUTHORITY

Supervision of personal data protection shall be carried out by the Data State Inspectorate (*Datu valsts inspekcija*), an institution established in 2001 and currently under the jurisdiction of the Ministry of Justice.¹⁰ In 2005 "The Concept" for independent

⁶ Amendments to the Personal Data Protection Law, 6 May 2010, available at <http://www.likumi.lv/doc.php?id=210207>.

⁷ Latvia's Contribution to the Regular Report from the Commission on Latvia's Progress Towards Accession (National Progress Report), June 2002, at 99 available at http://www.mfa.gov.lv/data/file/e/national_progress_report_2002.pdf.

⁸ See *infra*.

⁹ See *infra* in the text and footnotes.

¹⁰ See <http://www.dvi.gov.lv/eng/about/>.

institutions was developed under the Prime Minister's Order No. 484.¹¹ The working group that developed the Concept recommended many amendments to the relevant legislation in order to ensure independent institutions could fulfil their functions efficiently. A second working group was created in January 2005 in order to implement requirements under Article 28 of Directive 1995/46/EC. This working group developed amendments to the Personal Data Protection Law, and agreed that eventually it will be necessary to develop a separate Law on Data State Inspectorate.¹² The draft law was ready in 2006¹³ but was substantially redrafted in 2008.¹⁴ For a number of years the work on this law and discussions were ongoing. Currently, adoption of a separate "Data State Inspectorate Law" has been postponed. The official reasons are that on 1 December 2009 the Lisbon Treaty came into force, and as a consequence changes in the context of the personal data protection laws are anticipated. Because the pillar system has been abolished and the European Union intends to develop a new framework for personal data protection in the police and judicial institutions. In addition, the Consultative Committee of the European Council is planning to develop recommendations on requirements for an independent personal data protection institution in the light of the judgment of the European Court of Justice in case No C-518/07 on the interpretation of the "independence" of the personal data protection supervisory authority as stated in the Directive 1995/46/EC.¹⁵

As of August 2007, the Data State Inspectorate had a staff of about 23 employees (rising to 25 employees in 2008), but the number of employees was reduced to approximately 19 in 2009. It is charged with the responsibility of: controlling compliance with the security requirements for information systems; reviewing complaints and issuing decisions and formal recommendations; maintaining the national registers of data processing systems (data processing systems were registered until 1 September 2007; since that date only data processing systems falling under one of a few exceptions provided by the law have to be registered), of data processing cases, and of personal data protections specialists; accrediting and controlling providers of certification services for digital signatures; controlling compliance with the prohibition against sending unsolicited commercial announcements; issuing permission for the transfer of personal data to third countries; carrying out inspections and controlling personal data protection during the provision of information society's services in the field of electronic communications. The Data State

¹¹ See Data State Inspectorate Annual Report 2005, at 7, available at <http://www.dvi.gov.lv/eng/about/reports/2005/2005-year.pdf>.

¹² *Id.* at 7-9.

¹³ See Data State Inspectorate Annual Report 2006, at 11, available in Latvian at http://www.dvi.gov.lv/par_mums/files/Gada_parskats_2006_DVI.pdf.

¹⁴ See Data State Inspectorate Annual Report 2008, at 9, available at http://www.dvi.gov.lv/eng/about/reports/2008/Annual%20Report_2008.PDF.

¹⁵ See Data State Inspectorate Annual Report 2009, available in Latvian at http://www.dvi.gov.lv/par_mums/dvi_parskats_2009.pdf.

Inspectorate is also authorised to impose administrative penalties for violations of personal data processing.¹⁶

In 2006, a draft amendment was submitted to the Cabinet of Ministers that stipulates criminal liability for illegal data processing if it is performed repeatedly within one year, or if it was performed by prior agreement by a group of persons.¹⁷ Draft amendments were again submitted to Parliament in 2007. These stipulated criminal liability for illegal data processing if significant harm resulted and specific intent could be shown.¹⁸ After completing the constitutional procedures the Criminal Law was amended in 2009 to create criminal penalties for publishing illegal personal data processing, if significant harm was done, or if performed by the data processor or operator for the purposes of revenge, obtaining material benefits, or blackmail, or with the hope of influencing the personal data processor or operator.¹⁹

In 2008 Latvia enacted substantial amendments to the Administrative Offences Code to impose more serious sanctions on certain offences, including violations of the Personal Data Protection Law.²⁰ The amendments stipulate administrative liability for the unlawful processing of an individual's personal data and increase sanctions for other data offences.²¹

By the end of 2005, the Inspectorate had registered 625 systems, bringing the total number of registered personal data processing systems to more than 12,000.²² In 2006 the Inspectorate registered another 731 systems and between then and 1 September 2007 it registered an additional 769 systems. After that date, amendments to the Personal Data Protection Law entered into force, and the registration requirements were changed. Currently the Inspectorate registers personal data processing cases (controllers). For example, in 2009 the Inspectorate registered 384 cases of personal data processing and 93 changes in the information concerning the personal data processing. Out of these cases, the Inspectorate carried out pre-registration verification in 157 cases. These pre-registration verifications revealed two main problems, namely, the holding of an

¹⁶ Latvia's Contribution to the Regular Report from the Commission on Latvia's Progress Towards Accession, *supra* at 99; as of July 2003, 35 complaints had been received.

¹⁷ 9th Annual Report of the Article 29 Working Party on Data Protection, 14 June 2006, at 72. Annual Reports of the Art. 29 Data Protection Working Party are available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

¹⁸ 11th Annual Report of the Article 29 Working Party on Data Protection, at 64.

¹⁹ Article 145 of the Criminal Law, available in Latvian at <http://www.likumi.lv/doc.php?id=88966>.

²⁰ Infolex Legal Portal, Latvia: Amendments to the Administrative Offences (February 2009), available at <http://www.infolex.lt/portal/ml/start.asp?act=legupd&lang=eng&biulid=183&srid=76&strid=1214>.

²¹ *Id.*

²² Data State Inspectorate Annual Report 2005, *supra* at 19.

excessive amount of personal data in relation to the purpose of the processing, and the transfer of personal data to third parties without an appropriate legal basis.²³

An alternative to registering as a personal data processor with the Data State Inspectorate is to employ a personal data protection specialist who is certified by the Data State Inspectorate. In 2009 the Inspectorate certified 17 such specialists.²⁴

In 2005, the Inspectorate considered 168 applications and provided 1,500 consultations to data controllers and citizens (via written answers as well as direct communication). The majority of the complaints received by the Inspectorate in 2005 involved illegal data processing in the process of collecting overdue loans and payments; lack of notification, particularly in medical services; and disproportionate data processing beyond the original purpose of the collection.²⁵ In 2006 the Data State Inspectorate received 133 complaints.²⁶ In 2007 it received 120 complaints, of which 30 were determined to be violations.²⁷ In both 2006 and 2007 the primary source of complaints was processing without a legal basis.²⁸ Since then, the Data State Inspectorate has been the supervisor of spam-related violations.²⁹

In 2009 the Inspectorate received 158 written complaints concerning personal data processing. By comparison, in 2008 the Inspectorate received approximately 140 written complaints, and provided more than 600 consultations.³⁰ Primary concerns with respect to personal data processing in 2009 were related to publishing personal data on the Internet, video surveillance, and the loss of documents containing personal data. Particular problems were discovered in relation to creditors' use of their debtors' personal data.

The Data State Inspectorate is also supervising personal data processing by Europol. Anyone has a right to access personal data stored by Europol, as well as to request corrections or deletions. Anyone also has the right to ask the Data State Inspectorate to verify the legitimacy of transferring the personal data to Europol.³¹

²³ Data State Inspectorate Annual Report 2009, *supra*.

²⁴ *Id.*

²⁵ Data State Inspectorate Annual Report 2005, *supra* at 19. See also 9th Annual Report of the Article 29 Working Party, *supra* at 74.

²⁶ 10th Annual Report of the Article 29 Working Party on Data Protection, 20 June 2007, at 72.

²⁷ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 65.

²⁸ 10th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 72; 11th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 65.

²⁹ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 65.

³⁰ Data State Inspectorate Annual Report 2008, *supra*.

³¹ See informative material available in Latvian at http://www.dvi.gov.lv/files/Europol_buklets.pdf.

In the framework of the Article 29 Working Party (established by Article 29 of Directive 1995/46/EC), the Inspectorate and other EU Data Protection authorities are working to implement common data protection policies and practices.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The *Mentzen* case concerned the law requiring personal names of foreign origin to be "Latvianised" in official documents. The Latvian Constitutional Court ruled that the law does impinge upon the constitutional right to privacy, but the restriction was declared constitutional because it protected "the right of other inhabitants of Latvia to use the Latvian language on all of Latvia's territory and to protect the democratic order."³² The European Court on Human Rights dismissed the application, stating that the alleged violation is one that could be necessary in a democratic society.³³

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Violating the confidentiality of correspondence, information in the form of transmissions over a telecommunications networks and other information is subject to criminal punishment.³⁴ On 28 October 2004, the Law on Electronic Communications was adopted,³⁵ replacing the Law on Telecommunications. It incorporates the provisions of the EU Directive on Privacy and Electronic Communications (2002/58/EC), and has a chapter regulating data protection in the electronic communications sector. Section 68 of the Law on Electronic Communications states that service providers are prohibited from disclosing information about users or subscribers and the electronic communications services or value-added services they receive. Under the Law only officials of bodies performing investigative operations in specific cases have the right to the interception or surveillance of communications. The Law on Electronic Communications regulates the processing of traffic and location data.³⁶

³² *Mentzen v. Latvia*, Judgment of the Latvian Constitutional Court No. 2001-04-0103, 2 December 2001, available in English at http://www.minelres.lv/NationalLegislation/Latvia/Latvia_ConstCourt2001_English.htm.

³³ See "The European Court of Human Rights Has Declared Inadmissible a Number of Complaints about the Possible Violations of Human Rights in the Republic of Latvia," available at <http://www.mkparstavis.am.gov.lv/en/@id=53>.

³⁴ The Criminal Code of the Republic of Latvia, Section 144, unofficial English translation available at <http://www.legislationline.org/documents/section/criminal-codes>.

³⁵ Law on Electronic Communications, available in Latvian at <http://www.likumi.lv/doc.php?id=96611>. The Law entered into force on 1 December 2004. See also ePractice, eGovernment Factsheet – Latvia – Legal Framework (April 2010), available at <http://www.epractice.eu/en/document/288289>.

³⁶ Law on Electronic Communications, *supra*.

The Criminal Procedure Law, which replaced the Soviet Time Criminal Procedure Code of 1961, was adopted in April 2005 and has been amended several times.³⁷ Among other things, the Law covers the role and process of acquiring electronic evidence. Under this regulation, investigative officers have the power to oblige information system managers to ensure that data necessary for the purposes of investigation is immediately preserved unchanged and will not be revealed to any third persons whatsoever. But the officer can only require a manager to reveal the stored data after receiving permission from the supervising authority (depending on the procedural status and the stage of the process the supervising authority may be a higher prosecutor or a judge).³⁸ New rules cover investigations conducted without the individual's consent or knowledge, such as wiretapping, control of data stored in an electronic storage system, control of transferred data, or video and audio control of a certain place or person. A person may be tracked only with judicial permission. The law outlines detailed guidelines for the implementation of discretionary powers of responsible officers and the court.

Section 143 of the Criminal Law prescribes liability for illegal entry into a residence unit against the will of the person residing there. Under Section 144 of the Criminal Law the intentional violation of the secrecy of personal correspondence or information transmitted over telecommunications networks, as well as the intentional violation of the secrecy of such information and software provided for use in connection with electronic data processing, is punishable by imprisonment for a term of up to three years' community service or a fine of up to fifty times the minimum monthly wage. The sanctions are graver if the crime is committed with intent to gain material benefit.³⁹

The Criminal Procedure Law provides an exhaustive list of situations in which public agencies have the right to interfere with the right of a person to the inviolability of privacy in family life, residence, and correspondence in compliance with the prescribed procedures. The Law lists the following procedural activities: search of the residence, search of the person, inspection, observation, seizure of property, seizure of post and telegraph correspondence, tapping of telephone conversations, and the acquisition of information by technical means, and the verification of testimonies on-site.⁴⁰

If there are sufficient grounds to believe that tapping conversations or acquiring information by technical means can provide information relevant to a case, investigators may tap conversations over the telephone and other means of communication of the suspect or the accused person if authorised to do so by a judge.. In urgent cases an officer

³⁷ Criminal Procedure Law, Latvijas Vestnesis, 11 May 2005, effective from October 2005, unofficial English translation available at <http://www.legislationline.org/documents/section/criminal-codes>.

³⁸ *Id.* at Sections 191 and 192.

³⁹ The Criminal Code of the Republic of Latvia, *supra*.

⁴⁰ Criminal Procedure Law, *supra*. See also Periodic Report of the Republic of Latvia on the Implementation of the 1966 International Covenant on Civil and Political Rights in the Republic of Latvia during the Period from 1995 till 2002, available at <http://www.mkparstavis.am.gov.lv/en/@id=58>.

may commence wiretapping with nothing more than a prosecutor's consent, but within one working day he must also receive judicial permission. Conversations of persons over the telephone or other means of communication may be tapped without a court order if they give written consent, if there is a possibility that a crime will be directed against them or if they are or may be involved in performance of a crime.⁴¹

The Law on "Operative Activity" includes standards that prohibit the arbitrary and unjustified interference with the right of a person to the inviolability of residence and correspondence.⁴² Under Article 8 of the law, operative control of correspondence, acquisition of information via technical means, tapping of non-public conversations (over the telephone, electronic, or other means of communication) and data entry may only be undertaken with the approval of the Chairman of the Supreme Court or his designated Supreme Court judge. Permission for these activities may be issued for a period of up to three months and may, in the event of justified necessity, be prolonged, but only as long as the relevant proceedings concerning the person are active. In exceptional cases, i.e., when there is a need to act without delay to prevent a threat to vital public interests, such as an act of terrorism or subversive activity, a murder or other serious crime, or if there is actual threat to the life, health, or property of a person, the above activities can be initiated without the judge's approval. The prosecutor must be notified within 24 hours and the judge's approval received within 72 hours. If the officers fail to do so, tapping must be terminated. In addition, Article 5 of the above law stipulates that if the person under observation believes that his or her lawful interests and freedoms have been violated, the person has the right to either submit a complaint to the prosecutor, who after a review issues a compliance statement or submit a claim in court.⁴³

However, in 2010 several provisions of the Law on "Operative Activity" were challenged in the *Satversmes tiesa* (the Constitutional Court).⁴⁴ These include the provision that in exceptional cases allows wiretapping without judicial approval. The case should be ready for judicial review by December 2010.

There is no separate binding regulation on the use of surveillance technologies; issues arising from such cases are dealt with in accordance with the principles and norms of data protection law. However, in 2004 the Inspectorate prepared a non-binding recommendation comprising basic principles that should be followed by those willing to use such technologies in accordance with the rule of law. Updated recommendations were

⁴¹ *Id.*

⁴² The Law on "Operative Activities" was adopted on 16 December 1993 and since then has been amended many times, most recently in December 2009. The consolidated text of the Law is available in Latvian at <http://www.likumi.lv/doc.php?id=57573>.

⁴³ *Id.*

⁴⁴ The decision to initiate proceedings, dated 16 July 2010, is available in Latvian at http://www.satv.tiesa.gov.lv/upload/lem_ierosin_2010_55.htm.

published in 2009.⁴⁵ The first legal act appeared in 2010 when, on 10 August, the Cabinet of Ministers issued its regulation No. 773 concerning obtaining, storing, and using data from the State Border guard's video information systems.⁴⁶

In 2007 a lower court ordered the Latvian financial police agency to pay LVL100,000 (approximately €420.300) to the high-profile TV news presenter Ilze Jaunalksne for illegally tapping her telephone and selling the transcripts to a newspaper.⁴⁷ In 2010 the Supreme Court finally ordered the State to pay to Jaunalksne LVL12.000 (€17,074). The court found that the Ministry of Finance and State Revenue Service had failed in its duties by breaching Jaunalksne's privacy. Four financial police officers were prosecuted for abuse of office in connection with the wiretapping case.⁴⁸

National security legislation

In 2004, the fight against terrorism inspired several amendments that loosened the rules guaranteeing the protection of personal data held by credit institutions.⁴⁹

In November 2004, the Cabinet of Ministers accepted the Concept on Establishment of Anti-Terrorism Centre, a document that establishes a new, specialised department within the institutional structure of the Security Police. The Anti-Terrorism Centre is now operational, conducting mainly analytical and planning activities. In order to ensure better consultation and co-ordination among the key institutions, in 2005 a consultative council of experts of the Anti-Terrorism Centre was established, which includes representatives from the key institutions.⁵⁰

Data retention

The Law on Electronic Communications requires the providers of electronic communications to retain the so-called "storable data" for a period of 18 months. Among other things, these "storable data" include data about callers and their telephone numbers, recipients and their telephone numbers, and mobile phone identifiers and location data. According to the law, providers of electronic communications shall provide these data to the pre-trial investigatory institutions, to the subjects carrying out investigative activities, to state security institutions, prosecutor's office, and court, if these institutions request

⁴⁵ Available in Latvian at http://www.dvi.gov.lv/files/Rekomendacija_videonoverosana.pdf.

⁴⁶ Available in Latvian at <http://www.likumi.lv/doc.php?id=215316&from=off>.

⁴⁷ "News Presenter Wins 10.000 Lats in Phone Tapping Case," *The Baltic Times*, 12 February 2007, available at <http://www.baltictimes.com/news/articles/17304/>.

⁴⁸ See Press release of the Supreme Court, "12 000 LVL Have Been Recovered from the Republic of Latvia for Ilze Jaunalksne," 18 February 2010, <http://www.at.gov.lv/en/information/about-trials/2010/201002/20100218/>.

⁴⁹ See *infra*.

⁵⁰ Terms of reference of the Consultative Council of experts of the Anti-Terrorism Centre are available in Latvian at <http://www.likumi.lv/doc.php?id=122154&from=off>.

it.⁵¹ In accordance with the Law on "Operative Activity," the "subjects carrying out operative activities" are state security and defence institutions, institutions in charge of maintaining public order and other state bodies authorised by law to perform investigative operations within the scope of their competence.⁵²

National databases for law enforcement and security purposes

The Law on Establishment and Use of National Data Base of DNA,⁵³ adopted on 17 June 2004, requires the establishment of a national DNA database. to be used in the investigation of crimes. The law provides for storing the following information: profiles and data about the suspect, accused person, defendant, or convict, and information concerning the DNA profiles and data of unidentified dead bodies, missing persons, and traces of biological origin. This information is classified as restricted access information.

In 2007, access to the Schengen Information System (SIS) was enabled in Latvia.⁵⁴ The SIS contains information about wanted or missing persons, persons being clandestinely followed, and vehicles and other objects that were stolen or otherwise separated from their owners.⁵⁵ A communal system allows access to this information by police and other authorities in all SIS Member States.⁵⁶ Anyone may request the review of personal data entered into SIS, request the correction of incorrect information, or request the deletion of illegally obtained information.⁵⁷

The Court Information System is a database of legal proceedings aimed at automating the administrative cycle – data registration, processing, storage, and availability. Recently, the Latvian Government has introduced new rules for the system's development, maintenance, and use, including the minimum amount of data that must be entered into the system and conditions for accessing the database.⁵⁸

⁵¹ Paragraph 11 of Section 19 and Section 71 primus of the Law on Electronic Communications, available at <http://www.likumi.lv/doc.php?id=96611>.

⁵² Law on "Operative Activity," supra. See Chapter 4 of the Law.

⁵³ Law on Establishment and Use of National Data Base of DNA, available in Latvian at http://www.ic.iem.gov.lv/files/likumi/DNS_datu_bazes_likums.pdf, and in English at http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Development_and_Use_of_the_National_DNA_Database.doc. The Law entered into force on 1 January 2005.

⁵⁴ *Id.*

⁵⁵ Data State Inspectorate, Personal Data in the Schengen Information System (SIS), available at <http://www.dvi.gov.lv/eng/pdp/schengen/>.

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ ePractice, eGovernment Factsheet – Latvia – Infrastructure (April 2010), available at <http://www.epractice.eu/en/document/288292>.

National and international data disclosure agreements

No specific information has been provided under this heading.

Cybercrime

No specific information has been provided under this heading.

Critical infrastructure

The notion of "critical infrastructure" is relatively new to Latvia. Before it was introduced in the first half of 2010 by amending the National Security Law,⁵⁹ there was a similar but not identical concept of "objects which are important for national security".⁶⁰ These amendments to the National Security Law establish the principle that the owner or user of a critical infrastructure is personally responsible for planning and carrying out the necessary steps to ensure its security. The State's role is mainly regulatory. If government institutions needed to monitor information systems, it would have to be on a different legal basis, for example, under the aforementioned Law on "Operative Activity". However, the system is very new and it is difficult to say how it will work.

INTERNET & CONSUMER PRIVACY

E-commerce

Sending commercial announcements via email or other means of electronic communications is regulated by the Law on Information Society Services.⁶¹ In principle, this law forbids sending commercial announcements to ordinary persons unless they have expressly consented to receiving them. Commercial enterprise that have obtained a person's email address, may use it for the purpose of sending other commercial announcements as long as the announcements concern similar goods or services and the person has not opted out of receiving them. Each message must include an option to block further use of the email address.

Cybersecurity

No specific information has been provided under this heading.

Online behavioural marketing and search engine privacy

No specific information has been provided under this heading.

Online social networks and virtual communities

No specific information has been provided under this heading.

⁵⁹ Amendments to the National Security Law, 24 April 2010, available in Latvian at <http://www.likumi.lv/doc.php?id=209821>.

⁶⁰ National Security Law, 2005 consolidated text available in English at <http://www.mfa.gov.lv/en/security/basic/4536/>.

⁶¹ Available in Latvian at <http://www.likumi.lv/doc.php?id=96619>.

Online youth safety

No specific information has been provided under this heading.

TERRITORIAL PRIVACY

Video surveillance

In principle, video surveillance is subject to the LPDP's general rules on personal data protection. For example, the recently adopted regulations of the Cabinet of Ministers No. 773, which concern the obtaining, storage, and use of data from the video information systems of the State Border guard, frequently refer to LPDP's requirements.⁶²

One of 2010's most reported news items was that the Data State Inspectorate has started to evaluate the compliance of Google's "Street View" service with the data protection principles and requirements. This evaluation started because Google, in compliance with the law, notified the Data State Inspectorate that it wished to introduce this service in Latvia and therefore to photograph the streets of various Latvian cities.⁶³

Location privacy (GPS, mobile phones, location based services etc.)

According to the Electronic Communications Law, location data may only be processed to enable the provision of electronic communications services. The processing of location data for other purposes without the consent of a user or subscriber is permitted only if the user or subscriber cannot be identified. Processing location data for other purposes with the written consent of a user or subscriber is permitted only when it is necessary to provide value added services. A user or subscriber has the right to revoke his or her consent for the processing of location data for any other purpose at any time by notifying the relevant electronic communications service provider.⁶⁴

Travel privacy (travel identification documents, biometrics etc.) and border surveillance

Starting in November 2007, the Latvian government began issuing e-passports to comply with European Union standards.⁶⁵ The new passports feature a chip that stores biometric data (the holder's digital photo and fingerprints).⁶⁶ All other (non-e) passports will be

⁶² Available in Latvian at <http://www.likumi.lv/doc.php?id=215316&from=off>.

⁶³ The relevant press release by the Data State Inspectorate is available in Latvian at <http://www.dvi.gov.lv/jaunumi/read.php?c=&id=1282646801.787.2.2>.

⁶⁴ Section 71 of the Electronic Communications Law, available in English at http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Electronic_Communications_Law.doc.

⁶⁵ Giesecke & Devrient, "Latvia Government Begins Issuing Electronic Biometric Passports Made by Giesecke & Devrient," available at http://www.gi-de.com/portal/page?_pageid=44,139709&_dad=portal&_schema=PORTAL.

⁶⁶ ePractice, eGovernment Factsheet – Latvia – Infrastructure, *supra*.

replaced as per their expiration dates.⁶⁷ In total, 1.1 million e-passports will be produced by 2012.⁶⁸

NATIONAL ID & SMART CARDS

In 2002, the Latvian Parliament passed a law introducing compulsory identity cards for all residents. It requires all citizens and non-citizens of Latvia over the age of 15 to be issued with machine-readable ID cards that will also be a means for creating personal e-signatures. The introduction of ID cards was set for 2005, but was originally postponed to 2007.⁶⁹ In 2007 the government issued a mandate establishing a working group, which agreed that identity cards would be in the form of both a card and travel document with e-signature support.⁷⁰ The draft of the eID card conception was unveiled on 10 December 2008.⁷¹ The government now expects the first eID cards to be rolled out in 2010, with a goal of producing 2 million cards by 2013.⁷²

E-signature cards were first issued by the Latvian government in September 2006; they are based on qualified certificates and authentication certificates⁷³ and used to sign electronic documents and access online services, including declarations and tax reports. A National Unified Library System is currently in process that will link all of Latvia's libraries through a single network and a unified catalogue.⁷⁴

The new Law on Civil Registration Records was adopted on 17 March 2005.⁷⁵ This law replaces the Law on Civil Registration and regulates the registration of marriage, birth, and death. The Law on Civil Registration Records states that cause of death will no longer be indicated on death certificates.⁷⁶

On 10 February 2010 the Cabinet of Ministers of Latvia approved the e-ID card concept, which provides an introduction to the national e-ID card; its implementation will take

⁶⁷ Office of Citizenship and Migration Affairs, Questions and Answers on E-Passports, available at <http://www.pmlp.gov.lv/en/pakalpojumi/passport/questions.html>.

⁶⁸ ePractice, eGovernment Factsheet – Latvia – Infrastructure, *supra*.

⁶⁹ Personal Identification Documents Law with amendments of 20 April 2004, available in Latvian at http://www.ic.iem.gov.lv/files/likumi/personu_apliecinosu_dokumentu_likums.pdf and in English at http://www.ic.iem.gov.lv/files/lrcm/Personal_Identification_Documents_Law.doc.

⁷⁰ EPractice, Egovernment Factsheet – Latvia – National Infrastructure, May 2009, available at <http://www.epractice.eu/en/document/288292>.

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ Law on Civil Registration Records, available in Latvian at <http://www.likumi.lv/doc.php?id=104832> "><http://www.likumi.lv/doc.php?id=104832> . The Law entered into force on 15 April 2005.

⁷⁶ *Id.*

place in the course of 2011.⁷⁷ The concept was drafted by the Ministry of Regional Development and Local Government (MRDLG). The e-ID cards will be used both to identify people travelling abroad or visiting public or municipal institutions and to provide authentication in the electronic environment. The Ministry perceives the future card as a key enabler of the development of national and local e-Government services and, as a result, Latvian e-Government generally. The Office of Citizenship and Migration Affairs (OCME) will be in charge of issuing the cards while a private partner selected following a tendering process will deliver the relevant certification services.⁷⁸

RFID tags

No specific information has been provided under this heading.

BODILY PRIVACY

No specific information has been provided under this heading.

WORKPLACE PRIVACY

In 2005, the Inspectorate prepared recommendations on personal data protection in the workplace in the form of a handbook for employers and employees which explains what personal data may be processed by employers and whether they must inform their employees about the data processing performed.⁷⁹

The Inspectorate also issued a decision on workplace email monitoring. The Inspectorate stated that where the employer provides the means for communications intended for use in carrying out the employees' duties, the employer has the right to monitor the communications. However, the employer must notify employees of the monitoring.⁸⁰

HEALTH & GENETIC PRIVACY

Medical records

Privacy of medical records is protected by the Law on the Rights of Patients.⁸¹ According to Section 10 of this law, information relating to an identifiable patient is protected in accordance with the regulations covering the protection of the data of natural persons. Such information shall not be disclosed even after the death of the patient. Information regarding a patient may only be disclosed with his or her written consent or in the cases prescribed by this law.

⁷⁷ ePractice, eGovernment Factsheet – Latvia – Infrastructure, *supra*.

⁷⁸ *Id.*

⁷⁹ 9th Annual Report of the Article 29 Working Party, *supra* at 73.

⁸⁰ See Data State Inspectorate Annual Report 2005, *supra* at 24.

⁸¹ Available in English at http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Law_On_the_Rights_of_Patients.doc.

The patient's data recorded in the medical documents may be used in research as long as the patient cannot be directly or indirectly identified by the information to be analysed, or if the patient has consented in writing to its use in specific research. The patient data recorded in medical documents may also be used in research without observing the conditions referred to in paragraph 7 of this Section if the following conditions exist concurrently: (1) the research is being performed in the public interest; (2) a competent State administrative institution has allowed the use of the patient data in specific research in accordance with the procedures specified by the Cabinet of Ministers; (3) the patient has not previously prohibited the transfer of his or her data to a researcher in writing; (4) it is not possible to acquire the consent of the patient with proportionate means; or (5) the benefit of the research for public health is commensurate with the restriction of the right to the inviolability of private life.

Genetic identification

The Law on Establishment and Use of National Database of DNA also regulates the exchange of results of genetic research with other countries and international organisations.⁸²

FINANCIAL PRIVACY

As mentioned above, starting in 2004, coordinated amendments were made to the laws governing credit institutions: the Prevention of the Laundering of the Proceeds from Crime and Law on Financial Instruments. In 2008 a new Law on the Prevention of the Laundering of the Proceeds from Crime and Financing of Terrorism was adopted.⁸³

Though the basic principle in the law on credit institutions classifies information about clients and their dealings as protected information, lawmakers have widened the scope of exceptions. The law now requires that information on clients (existing and prospective) and their dealings be revealed to specified institutions on any of 16 occasions, in some cases without needing the consent of a judge.⁸⁴

E-GOVERNMENT & PRIVACY

Launched in August 2006, the *Latvija.lv* portal provides individuals with Internet resources relating to state institutions⁸⁵ and centralised access to public e-services. From 2010 it will link together information about 1,333 e-government services for citizens and

⁸² Law on Establishment and Use of National Data Base of DNA, *supra*.

⁸³ Available in Latvian at <http://www.likumi.lv/doc.php?id=178987&from=off>.

⁸⁴ Law on Credit Institutions, Section 63, unofficial English translation available at <http://unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN018386.pdf>.

⁸⁵ See the English version of the portal at <https://www.latvija.lv/EN/WebLinks>.

businesses. More services are currently being added. All these services are intended to function automatically, ensuring data exchange between citizens and state institutions.⁸⁶

The first e-service on the portal was released in February 2008 and contains four state registers. Currently, the most commonly used e-services are electronic declaration and verification of a person's place of residence as well as verification of documents' validity. Authorised access is possible via an Internet bank or e-signature.⁸⁷

The Conception on the Points of Single Contact (PSC), which implements Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, was approved by the Cabinet of Ministers in 2009. The Ministry of Regional Development and Local Government, provides the technical support for the PSC; the back-office function is ensured by competent authorities. The Latvian Development and Investment agency acts as mediator (it solves non-standard requests by services providers and recipients and also consults them on usage of the portal). The front-office function is fulfilled by the State portal. The development of an e-infrastructure for the PSC is in progress. The public service catalogue has been developed and is already operational. Extra functionality will be added in 2010/2011.⁸⁸

OPEN GOVERNMENT

The Freedom of Information Law (FOIL) was adopted by the Latvian Parliament on 29 October 1998 and signed into law by the President in November 1998.⁸⁹ It guarantees public access to all information held by state administrative institutions and local government institutions in "any technically feasible form" not specifically restricted by law. Public bodies must respond to requests for information within 15 days. According to FOIL there are several exemptions from the basic principle: if the information is for internal use by an institution; it is a trade secret not relating to public procurements or information about the private life of an individual; or if it concerns certification, examination, project, tender, and similar evaluation procedures; and (a recent addition) information for the use of the service itself/ The latter mainly concerns information received from NATO and other international institutions relating to state security. Finally, the FOIL introduces a broad exception allowing legitimate grounds for restricting public access to be defined by other laws (e.g. criminal procedure, law on police, and other laws governing particular institutions).

⁸⁶ ePractice, eGovernment Factsheet – Latvia – Infrastructure, *supra*. See also eGovernment Factsheet – Latvia – eServices for Citizens, available at <http://www.epractice.eu/en/document/288293>.

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ Freedom of Information Law, available in Latvian at <http://www.likumi.lv/doc.php?id=50601> and in English at http://webcache.googleusercontent.com/search?q=cache:http://www.ttc.lv/export/sites/default/docs/LRTA/Likumi/Freedom_of_Information_Law.doc.

Appeals can be made internally to a higher body or directly to a court. The law was amended in 2003 to give the Data State Inspectorate oversight authority starting in January 2004.⁹⁰ In practice, however, the Inspectorate experienced considerable problems with implementing this task due to lack of resources and administrative capacity. In addition, in contrast to the oversight of data protection issues, the Inspectorate had no competence to punish any violations of FOIL. Therefore, in 2009 FOIL was amended and the Data State Inspectorate was relieved of its responsibility with respect to this law.

The Law on Official Secrets⁹¹ establishes that information on the economic situation of the country, the status of the budget, and rates of salaries, benefits, preferences, and guarantees granted to officials and employees of the state and local government institutions cannot be placed under restricted access.

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this heading.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

In 2009 a personal data protection association was founded with the aim of promoting education and the dissemination of information on privacy issues in Latvia and assisting governmental institutions in privacy-related legal developments.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Latvia acceded to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol that establishes an individual complaints mechanism.⁹²

Latvia joined the Council of Europe (CoE) in 1995 and held the six-month rotating presidency from November 2000 to May 2001. It has signed and ratified both the ECHR⁹³ and the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).⁹⁴ The European Convention on the Suppression of Terrorism was ratified on 20 April 1999. On 22

⁹⁰ David Banisar, Freedominfo.org Global Survey: Freedom of Information and Access to Government Records Around the World - Latvia, July 2006, available at <http://www.freedominfo.org/regions/europe/latvia/>.

⁹¹ Law on Official Secrets, 29 October 1996, Article 5, available at <http://www.likumi.lv/doc.php?id=41058,%20available%20in%20English%20at%20http://www.ttc.lv/New/lv/tulkojumi/E0612.doc>.

⁹² Latvia acceded to the ICCPR on 14 April 1992 and to its First Optional Protocol on 22 June 1994. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁹³ Signed 10 February 1995, ratified 26 July 1996, entered into force 26 July 1996. Text and relevant information on all the Conventions adopted within the Council of Europe are available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

⁹⁴ Signed 31 October 2000, ratified 30 May 2001, entered into force 1 September 2001.

December 2004, Latvia ratified the Protocol Amending the European Convention on the Suppression of Terrorism. Latvia has signed and ratified the European Convention on Cybercrime.⁹⁵

The European Court of Human Rights (ECHR) concluded that Latvia had violated applicants' right to respect for private and family life when the country failed to regularise the citizenship of stateless individuals within Latvian territory prior to the breakup of the Soviet Union and Latvian independence. Although the applicants failed to apply for permanent residency before the stated deadline, the Court concluded that the individuals had formed and developed personal, social, and economic relationships, which constituted the private life of any human being. It also found that the Latvian authorities' refusal to grant them the right to reside lawfully and permanently in Latvia represented an interference with their private lives that could not be considered "necessary in a democratic society".⁹⁶

In the case of *Igors Dmitrijevs v. Latvia* the ECHR ruled, among other things, that the opening and monitoring by the prison authorities of the letters ECHR had sent to the applicant had not been in "accordance with the law" within the meaning of Article 8 paragraph 2 of the European Convention on Human Rights.⁹⁷ In the case of *Cistiakov v. Latvia* the ECHR found that restrictions on correspondence with his relatives had not been in "accordance with the law" within the meaning of Article 8 paragraph 2 of the European Convention on Human Rights.⁹⁸ The case of *Pacula v. Latvia* also related to correspondence with the ECHR.⁹⁹

Latvia became a member of the European Union in 2004.

⁹⁵ Signed 5 May 2004, ratified 14 February 2007, entered into force 1 July 2007.

⁹⁶ European Court of Human Rights, Appl. No. 60654/00, *Sisojeva and Others v. Latvia*, 15 January 2007, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=SISOJEVA&sessionid=61538667&skin=hudoc-en>; *Kaftailova v. Latvia*, Appl. No. 59643/00, 7 December 2007, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=KAFTAILOVA&sessionid=61538966&skin=hudoc-en>; See also Amnesty International World Report 2007 - Latvia, available at <http://www.amnesty.org/en/region/latvia/report-2007>.

⁹⁷ See Press release issued by the Registrar, 30 November 2006, available in French at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=61638/00&sessionid=61539652&skin=hudoc-pr-en>.

⁹⁸ See Press release issued by the Registrar, 8 February 2007, available in English at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=67275/01&sessionid=61540315&skin=hudoc-pr-en>.

⁹⁹ The judgment is only available in French at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=PACULA%20%7C%2065014/01&sessionid=61540717&skin=hudoc-en>.

* Updates to the Latvian Report published in the 2010 edition of EPHR have been provided by: Raivo Raudzeps, Attorney-at-Law at Sorainen, Latvia; Prof. Arturs Kucs, Head of Department of International and European Law at University of Latvia, Latvia.

REPUBLIC OF LITHUANIA

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 22 of the Constitution states, "The private life of an individual shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and any other communication shall be inviolable. Information concerning the private life of an individual may be collected only upon a justified court order and in accordance with the law. The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honour and dignity."¹ Article 24 of the Constitution states, "The home of a human being shall be inviolable. Without the consent of the resident, entrance into his home shall not be permitted otherwise than by a court decision or the procedure established by law when this is necessary to guarantee public order, apprehend a criminal, save the life, health, or property of a human being."²

The case law in the privacy and data protection fields is not very extensive, as there still is no strong history of data protection in Lithuania. It is, however, constantly developing: the Supreme Court of Lithuania has on multiple occasions reaffirmed the right to private life to be one of the most fundamental human rights.³

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The main rules regarding privacy and data protection are defined in the Civil Code of Lithuania, which was enacted in 2000 (the privacy protection provisions have not been amended since) as well as in the Law on Legal Protection of Personal Data (LLPPD).⁴

Article 2.22 of the Civil Code protects the right to an image. It states "Photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his consent. Such consent after natural person's death may be given by his spouse, parents or children." Consent will not be required where such acts are related to a person's public activities, his/her official post, request of law enforcement agencies, or where a person is photographed in public places.

¹ Constitution of the Republic of Lithuania (Approved by the Citizens of the Republic of Lithuania in the Referendum on 25 October 1992 as last amended on 13 July 2004, No. IX-2343, No. IX-2344), available at <http://www3.lrs.lt/home/Konstitucija/Constitution.htm>.

² *Id.*

³ *Ž.Ž. v Ltd Ekstra Žinios*, 14 August 2008, No. 3K-3-393/2008, the Supreme Court of Lithuania; *S.Š. and V.Š. v Ltd Lietuvos rytas*, 2 January 2008, No. 3K-7-2/2008, the Supreme Court of Lithuania. See also *infra*.

⁴ The Law on Legal Protection of Personal Data, No. I-1374 (2009), available in English at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=315633 (Official Translation).

A person's photograph (or its part) produced under the said circumstances, however, may not be demonstrated, reproduced, or sold if those acts were to abase person's honour, dignity or damage his professional reputation. The Civil Code provides that a natural person whose right to an image has been infringed has the right to request the court to oblige the discontinuance of the said acts and redressing of the property and non-pecuniary damage. After a person's death, such a claim may be presented by his spouse, children, and parents.

Article 2.23 of the Civil Code elaborates the ways of protection of the right to privacy embedded in Articles 22 and 24 of the Constitution. It states, "Privacy of a natural person shall be inviolable. Information on person's private life may be made public only with his consent. After person's death the said consent may be given by person's spouse, children and parents. "Public announcement of facts of private life, however truthful they may be, as well as making private correspondence public in violation of law as well as invasion of person's dwelling without his/her consent except as otherwise provided by the law, keeping his/her private life under observation or gathering of information about him/her in violation of law as well as other unlawful acts, infringing the right to privacy shall form the basis for bringing an action for non-pecuniary damage incurred by the said acts.

According to Article 2.24(6) of the Civil Code, the author's liability is waived when the data falls short of reality, if publicised data is about a public person, or his or her state or social activities, and the author publicised the data in good faith in order to acquaint society with that person.⁵ The Supreme Court interpreted Article 2.24(6) of the Civil Code noting that the author of misleading, incomplete, or incorrect information about a public person is released from liability for the act of publishing the material, but the author is not released from a duty to correct the information, should it degrade the honour and dignity of the public person.⁶

Lithuania's predominant data protection regulation, the Law on Legal Protection of Personal Data,⁷ was passed in 1996 and has since been amended multiple times, most recently on 1 January 2009. Its passage was mainly fostered by Lithuania's political aim to become a member of the European Union; legislative amendments to the LLPPD ensured its compliance with the EU Directive 1995/46/EC on data protection.⁸ Lithuania has been a full member of the EU since 2004.⁹

⁵ *J. Kaliacius v. I. Starosaitė-Zvagulienė*, 27 October 2004, No. 3K-3-579/2004, Supreme Court of the Republic of Lithuania, Overview of the Supreme Court Cassation Practice for the year 2004, at 14.

⁶ *Id.*

⁷ Law on Legal Protection of Personal Data, *supra*.

⁸ Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, available both in English and in Lithuanian at <http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation..>

⁹ European Union Member States Index, available at http://europa.eu/abc/european_countries/eu_members/lithuania/index_en.htm.

The 2003 amendment radically changed the aim of the LLPPD. The current law seeks "protection of an inviolability of an individual's right to private life with regard to the processing of personal data"¹⁰ in comparison with previous wording of the LLPPD, which aimed at balancing individuals' and controllers' interests. The stated purpose of the LLPPD is to protect the private lives of people by establishing the rights of individuals and regulations for data controllers. It extends to personal information held by both public and private entities. In addition to baseline protections, the LLPPD also includes specific provisions for the processing of personal data in various sectors and for various purposes, including social security, social care, health care, scientific research, direct marketing, statistics, elections, video surveillance, referenda, and citizens' legislative initiatives and telecommunications.

Individuals are entitled to know about the processing of their personal data, have access to that data, familiarise themselves with the processing method, demand rectification or destruction of their personal data and object to the processing of their personal data. These rights are, however, contingent upon several enumerated exceptions, such as national security, law enforcement and important economic or financial interests of the state. In addition to these rights, the data subject who has sustained damage as a result of unlawful processing of personal data, or any other acts or omissions by the data controller, the data processor or any other persons, in violation of the provisions of the LLPPD, shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused to him/her. The extent of pecuniary and non-pecuniary damage is determined by the courts.

The latest amendments of 1 January 2009 introduced some novelties into the Lithuanian personal data protection rules. The main amendments are the following. A new chapter on video surveillance was introduced, including a definition of the concept of video surveillance, and requirements for the installation of video surveillance devices, notification to data subjects, and processing of collected video data.¹¹ The use of personal identification codes was restricted: the amendments prohibit making personal identification numbers public and prohibit the collection and processing of personal identification numbers for direct marketing purposes. The scope of application of the LLPPD was broadened: the amendments provide that Lithuanian branch offices and representative offices of a data controller of EU Member State or another state of the European Economic Area shall be bound by the provisions of the LLPPD applicable to the data controllers. It must be noted that before this amendment, Lithuanian branch offices and representative offices of EU-based companies did not fall within the scope of the LLPPD. More stringent requirements were placed on data controllers regarding health-related personal data for scientific or medical research: The amendments provide

¹⁰ Law on Legal Protection of Personal Data, *supra*.

¹¹ State Data Protection Inspectorate, Newsletter on Personal Data Protection No. 1 (16), January 2009, available at [http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/2009%20January,%201\(16\).pdf](http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/2009%20January,%201(16).pdf). On video surveillance, see also *infra*.

that the State Data Protection Inspectorate must be notified and must carry out prior checking when personal data on a person's health is processed by automatic means, and also when this data is processed for scientific medical research purposes.¹² More specific rules were established regarding the processing of personal data by credit institutions for the purposes of evaluating creditworthiness of their clients. Finally, the independence of the State Data Protection Inspectorate was strengthened; the amendments provide for the rights of the data controller to designate a person or unit to be responsible for data protection, which shall notify the State Data Protection Inspectorate about the violations of the LLPPD.¹³

Personal data can only lawfully be processed if used for predefined purposes such as compliance with a legal obligation or as a necessary adjunct to a commercial transaction. The use must be accurate, fair, lawful, and not excessive in relation to the predefined purpose. Finally, personal data can only be further disclosed under a personal data disclosure contract, specifying the purposes for which the data will be used and the conditions and procedures of its use.

Article 25 of the LLPPD determines that personal data may be processed by automated means subject to notification by the data controller or his representative of the State Data Protection Inspectorate in accordance with the procedure established by the Government of the Republic of Lithuania, except the case where the personal data is possessed for the purposes of internal administration and other cases prescribed by the LLPPD. LLPPD establishes a definition of the internal administration and defines it as an activity which ensures an independent functioning of the data controller (structure administration, personnel management, management and use of materials and finances, and clerical work).

Furthermore, the processing of sensitive personal data requires a special notification form for prior checking. Sensitive personal data are data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life, and criminal convictions. Article 33 of the LLPPD specifies the circumstances under which prior checking by the State Data Protection Inspectorate of information processing activities is necessary. Prior checking must be carried out where the data controller intends to process sensitive personal data or process public data files by automatic means, where the data controller of state or institutional registers or information systems of state and municipal institutions intends to authorise the data controllers to process personal data and in other cases established by the LLPPD. In addition, the Law on State Registers¹⁴ provides for further controls on the use and legitimacy of state data registers that contain personal

¹² State Data Protection Inspectorate, Newsletter on Personal Data Protection No. 5 (20) 1 May 2009, available at [http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/2009%20May,%205\(20\).pdf](http://www.ada.lt/images/cms/File/naujienu/Biuleteniai/2009%20May,%205(20).pdf).

¹³ *Id.*

¹⁴ The Law on State Registers, No. I-1490 (1996), State News, 1996, No.86-2043.

information, and mandates that data registers may only be erased or destroyed in cooperation with the State Data Protection Inspectorate.

As a complement to the protections described above, in 1998 the Code of Administrative Offences was supplemented with monetary penalties for unlawful personal data processing and unlawful state information systems processing. The violation of personal data protection entails administrative liability.

Article 214(14) of the Code of Administrative Offences provides sanctions for the processing of personal data in violation of the provisions of the LLPPD. The unlawful processing of personal data *per se* (for instance, the unlawful use of person's email address or any other personal data, irrespective of the purpose of use) is subject to a fine from LTL500 (approximately. €145) to LTL1,000 (€290). If the violation is repeated the fines range from LTL1,000 (€290) to LTL2,000 (€579).

A 2006 amendment to the Code of Administrative Offences provides that any organisation that fails to indicate mandatory information (name, registered office, legal form, code, register where registration data is stored and kept, or other mandatory data, as established by the laws) on its corporate Internet site shall be subject to a fine.

Sector-based laws

In addition to the above-mentioned laws, several other Lithuanian laws additionally regulate certain specific aspects of data processing activities. These laws are: the Law on Electronic Communications,¹⁵ adopted in 2004 and amended most recently on 15 March 2009, which contains rules on processing of personal data and the protection of privacy in the sphere of electronic communications; the Code of Administrative Offences,¹⁶ which establishes administrative sanctions for violation of the national legal rules on data processing; the Law on the Ratification of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as amended by the Committee of Ministers of the Council of Europe;¹⁷ and the Law on the Rights of Patients and Compensation of the Damage to their Health, adopted in 1996 and amended several times, most recently on 1 March 2010, which provides for the rules concerning the inviolability of the patient's private life.¹⁸

¹⁵ In Lithuanian: Elektroninių ryšių įstatymas, No. IX-2135, adopted on 15 April 2004, last amendments adopted on 14 November 2008, in force as from 15 March 2009.

¹⁶ In Lithuanian: Administracinių teisės pažeidimų kodeksas, last amendments adopted on 10 June 2010, in force as from 22 June 2010.

¹⁷ In Lithuanian: Įstatymas dėl Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis ratifikavimo, No. IX-189, adopted on 20 February 2001.

¹⁸ In Lithuanian: Pacientų teisių ir žalos sveikatai atlyginimo įstatymas, No. I-1562, adopted on 3 October 1996, last amendments adopted on 10 November 2009, in force as from 1 March 2010, available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=360565.

DATA PROTECTION AUTHORITY

The State Data Protection Inspectorate (the Inspectorate) is responsible for supervising and monitoring the processing of personal data, and enforcing the provisions of the LLPPD and the Law on State Registers.¹⁹ Before data processing takes place, the data controller must inform the Inspectorate, which registers the processor and has the power to carry out prior checking.²⁰ After processing is carried out, the Inspectorate checks its lawfulness, handles appeals for denial of access to records, and grants authorisations to data controllers to disclose personal data to data recipients in third countries. Other functions of the Inspectorate include examination of personal requests and complaints, assistance to data controllers and data subjects, and composition of methodological recommendations on the protection of personal data.

The Inspectorate is a government institution financed from the state budget. The Inspectorate is accountable to, and its regulations are approved by, the government. The status of the Inspectorate is a specific one because, while under the executive power, it is competent to inspect and control the processing of personal data by legislative bodies. The lack of full independence of the Inspectorate as a national supervisory authority was noted in 2006 in evaluation by experts of the European Commission relating to Lithuania's preparedness for implementation of its membership in the Schengen agreement, specifically the country's adequacy in the data protection field.²¹ The EU's report states that data protection in Lithuania is appropriate and entirely conforms to Schengen, except the fact that the Inspectorate is not fully independent. The Inspectorate's administrative integration within the government structures could represent a risk for its functional independence.²²

On 15 April 2009, the government planned to change the status of the Inspectorate from an institution accountable to the government to an institution accountable to the Ministry of Justice.²³ Since the Ministry of Justice supervises the state register system and individual registers, the functional independence of the Inspectorate would have remained imperilled. The project, however, was not implemented and the Inspectorate still functions under the government.

¹⁹ Government of Republic of Lithuania Resolution No. 1185 Concerning the Setting up of the State Data Protection Inspectorate, 10 October 1996, State news, 1996, No. 100-2293.

²⁰ Recommended form approved by Order No. 1T-28 of 29 January 2004 of the Director of the State Data Protection Inspectorate, "Notification of automated processing," 29 January 2004. See State Data Protection Inspectorate, Registration of Data Controllers, available at <http://www.ada.lt/index.php?lng=en&action=page&id=10107>.

²¹ Annual Activity Report 2006 of the State Data Protection Inspectorate, at 3, available at http://www.ada.lt/images/cms/File/ataskaitos/Galutinis_EN.pdf.

²² *Id.* at 3.

²³ Annual Activity Reports 2009 of the State Data Protection Inspectorate, at 5, available in Lithuanian at http://www.ada.lt/images/cms/File/ataskaitos/Microsoft%20Word%20-%202009%20ataskaita%20_pateikta%20vyriausybei_.pdf.

In 2004, the Inspectorate gained full membership status in the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of the Directive 95/46/EC of the European Parliament and of the Council. After the ratification of the Europol Convention²⁴ on 22 April 2004 and its entering into force on 1 September 2004, as well as the ratification of the Convention on the Use of Information Technology for Customs Purposes²⁵ on 1 May 2004 and its entering into force on 1 August 2004, the Inspectorate became a full member of the Joint Supervisory Authorities of Europol, Schengen, and Customs.

In a 2005 case, *O. Jakstaite v. Prime Minister*,²⁶ the petitioner, former Inspectorate Director Ms. Jakstaite, appealed the judgment of the Vilnius Circuit Administrative Court to the Supreme Administrative Court of Lithuania for annulment of a Prime Minister's decree. The decree imposed on the Inspectorate Director an official sanction, namely, a severe reprimand for breach of principles and rules of ethics of state servants' activities, as well as, infringement of principles of objectivity and proportionality. Vilnius Circuit Administrative Court indicated that the Inspectorate selected an authoritarian management style, and that the Director often adopted all decisions *ex parte* and employees had no actual influence on decision-making. The representative of the Prime Minister in the case stated that the internal rules of the Inspectorate are too strict. Furthermore, it was determined that Ms. Jakstaite was often behaving in an unprofessional manner, and thus raised the mistrust of the society and commercial entities, whose activities in the data protection field are controlled by the Inspectorate. It was also established that the Inspectorate had often been expressing different opinions on the same issues. The Supreme Administrative Court concluded that the Director of the Inspectorate, Ms. Jakstaite, breached principles and rules of ethics of state servants' activities and violated the objectivity and proportionality principles embedded in Article 4 of the Law on Public Administration.

During 2006 the Inspectorate reviewed 161 complaints and requests from individuals, investigated 729 notifications on data processing, answered 84 requests from Convention ETS No. 108 Member States, prepared 310 conclusions on prior checkings and conducted 92 preventative inspections. In total, the Inspectorate provided 2,484 consultations. The Inspectorate provided information to the public through mass media, conferences, seminars, and other means 141 times in 2006; this is a significant improvement in outreach efforts as compared to 2005. In 2006, the Inspectorate performed inspections on

²⁴ Europol Convention, State News, 2004, No. 113-4202 (in Lithuanian), available at <http://www3.lrs.lt/cgi-bin/preps2?Condition1=238239&Condition2=>. On 1 January 2010, the Europol Convention was replaced by the Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL), Official Journal of the European Union L 121, 15 May 2009, at 37.

²⁵ Convention on the Use of Information Technology for Customs Purposes, State News, 2004, No. 36-1188 (in Lithuanian), available at <http://www3.lrs.lt/cgi-bin/preps2?Condition1=228195&Condition2=>.

²⁶ *O. Jakstaite v. Prime Minister*, 22 April 2005, No. A10 – 459 – 05, Supreme Administrative Court.

how personal data are being processed in selected sections: in banks established and operating in Lithuania and also in public utilities service providers.²⁷

In 2007, the Inspectorate celebrated its tenth anniversary.²⁸ In this year the Inspectorate received 154 complaints and handled 129 of them.²⁹ It carried out 318 inspections. The Inspectorate also analysed 790 notifications on data processing.³⁰ The Inspectorate drafted 53 replies to enquiries from countries to Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108).³¹ Among the inspections, six were conducted on financial institutions to check the scope and lawfulness of personal data processing of individuals referring to the financial institutions for the speedy credit services by Internet or mobile text messages.³² The Inspectorate also found that police officers checking the identity of traffic violators were also checking personal data including their genealogical tree. This data was also printed and attached as evidence. After a series of reversals on appeals, the Supreme Administrative Court acknowledged that the Inspectorate's instruction to disable the software's access to the Residents' Register was valid as the rule was overbroad and did not have basic privacy protections.³³ In the same year, in a joint initiative with the data controllers, the Inspectorate organised seminars, meetings and workshops, which resulted in an increased level of public awareness and dissemination of information.³⁴ The Inspectorate planned to intensify the activities performed to increase information dissemination on data protection matters and carry out preventive activities by performing sectoral inspections. In addition, the Inspectorate issued sample Rules for Personal Data Processing at Schools, which were subsequently approved by the Inspectorate Director. The rules aim to ensure compliance with the LLPPD.³⁵

²⁷ Annual Activity Report 2006 of the State Data Protection Inspectorate, *supra*.

²⁸ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 69.

²⁹ Annual Activities Report 2007 of the State Data Protection Directorate, at 11, available at http://www.ada.lt/images/cms/File/ataskaitos/2007_ANNUAL_REPORT.pdf.

³⁰ *Id.* at 13.

³¹ *Id.* at 16.

³² Country Report of State Data Protection Inspectorate to International Working Group on Data Protection in Telecommunications, 13 August 2008.

³³ IWG Country Report – Lithuania, 43rd Meeting of the Working Group, March 2008.

³⁴ Annual Activities Report 2007 of the State Data Protection Directorate, *supra* at 5.

³⁵ 11th Annual Report of the Article 29 Working Party on Data Protection 66 (June 2008) available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

In 2008, the Inspectorate investigated 115 complaints out of the 153 received.³⁶ In addition, the Inspectorate performed 126 preventive inspections and prepared 114 conclusions on prior checking.³⁷

In 2009, the Inspectorate investigated 166 complaints out of 201 received.³⁸ This is the largest number of complaints received in the last three years. In 2009 persons most actively complained about the processing of personal data for direct marketing purposes: these complaints increased three times in comparison to 2008.³⁹ In addition, in 2009 the Inspectorate performed 165 preventive inspections and prepared 114 conclusions on prior checking.⁴⁰ The Inspectorate also started preparation on draft laws regarding the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.⁴¹ The European Council requires relevant provisions to be transposed into national legislation by November 2010.⁴²

In 2008 and 2009 the number of legal consultations provided by the Inspectorate to data subjects and data controllers has increased: 3,179 consultations in 2008 and 3,696 consultations in 2009.⁴³

The available results show that contrary to previous years, the number of administrative law offence protocols drawn up in 2009 has increased significantly. Fourteen protocols out of 27 drawn up by the Inspectorate were found by the court of first instance to be well grounded, thus the number of the protocols rejected by the court is decreasing.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The case law in the privacy and data protection fields is not very extensive. One of the reasons for this *status quo* is that the right to privacy is still a novelty in the laws of Lithuania and in the courts' practice. Lithuanians rarely refer to the courts or other institutions due to violations of their private life.⁴⁴ The more rural settlements especially

³⁶ Annual Activities Report 2008 of the State Data Protection Directorate, at 10, available at <http://www.ada.lt/images/cms/File/ataskaitos/Report%202008%2020090528.pdf>.

³⁷ *Id.* at 14.

³⁸ Annual Activity Report 2009 of the State Data Protection Inspectorate, *supra* at 12.

³⁹ *Id.* at 13.

⁴⁰ *Id.* at 14.

⁴¹ *Id.* at 20.

⁴² *Id.* at 23.

⁴³ *Id.* at 9.

⁴⁴ Activity Report of the Inspector of Journalistic Ethics, *supra*.

perceive the boundaries of private life in a very liberal way.⁴⁵ However, the case law regarding the right to privacy is gradually developing.

The majority of cases regarding privacy protection dealt with by the Supreme Court of Lithuania relate to conflicts between two constitutional rights, i.e., right to private life and right to freedom of expression. In the majority of the cases violations of the right to privacy or the right to an image were found.

In the case of 17 February 2004, the Supreme Court explained that a public person is not under the same defence of honour and dignity as the private one because higher behaviour requirements are set for the public person than for the private one. Therefore, the public person has to tolerate the publicised information (even though it is not precise in full) or opinion about him.⁴⁶

In another case, the Supreme Court indicated that person's right to privacy is not absolute.⁴⁷ Immunity of private life can be restricted if the person abuses his/her right (for example, by acting dishonestly, then seeking to defend himself or herself with a claim to privacy). The right to claim a right of privacy might be reasonably denied on a case-by-case basis. The plaintiff worked as a sales clerk. From the point of view of the territory the sphere of the private life consists of a person's living accommodations, as well as premises which the person uses for his housekeeping or professional activities or similar.⁴⁸ The public workplace is not a person's private sphere. Salesmen cannot require that their privacy be guaranteed at their workplace, i.e., in the salesroom; therefore, surveillance of the salesroom and the salesmen's work is not secret surveillance of person's private life. The defendant, the owner of the store, installed video cameras in public locations, i.e., in the salesroom above the working place of the saleswomen (cash register) in order to prevent law infringements and crimes. The work of the saleswoman was public character activity; therefore she could not require privacy at her workplace. The plaintiff made an administrative law infringement; her behaviour was dishonest in the workplace, even unlawful; therefore, the plaintiff cannot use violation of her right to privacy in her defence.

In the case of 2 November 2004, the Supreme Court, interpreting Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and the person's right to private life, entrenched in national law, indicated that a violation of the right to private life can be understood as the filming of a private person in his/her private tenure without his/her consent, and/or distribution or publicising of the video record in

⁴⁵ *Id.*

⁴⁶ *V. Vizbaras v. I. Dzedulioniene*, 17 February 2004, No. 3K-3-56/2004, Supreme Court of the Republic of Lithuania, Overview of the Supreme Court Cassation Practice for the year 2004, at 14.

⁴⁷ *J. Bartasiuniene v. Public Institution "Humana people to people Baltic"*, 3 May 2004, No. 3K-3-289/2004, Supreme Court of the Republic of Lithuania, Overview of the Supreme Court Cassation Practice for the Year 2004, at 67 – 68.

⁴⁸ *Id.*

which the private person is recorded without his/her consent.⁴⁹ Substantiation measures, or admissible evidence, may consist of photos, audio, and video records, made without infringing the law. Admissibility of the substantiation measure is understood as receiving of information, constituting the content of the proof, without violating procedures set by the laws. Upon assessing the admissibility of the video record as the substantiation measure, it should be decided whether this proof was received without violation of the rights and interests of the data subjects who are recorded in the video record, in particular their right to privacy. The Supreme Court indicated that since in the present case the filming was conducted in the shop premises belonging to the defendant, the salesroom, i.e., the public place, the filmed persons were in labour relations with the defendant and materially liable for carried work. Such filming cannot be regarded as violation of the private person's rights; therefore, information in the video record has to be recognised as a proper proof when considering the labour duties violation.⁵⁰ This proof shall be assessed and analysed together with other evidence in the case. On the basis of these arguments the Supreme Court repealed the decision of the appellate instance court, where it was decided that the discussed video records violated the person's right to his private life and, thus, could not be regarded as admissible measure of substantiation.

On 29 November 2004, the Supreme Court indicated that the right to the private life and privacy is not violated if the elements of a publication's content do not create a possibility to identify the person about whom the information in the publication is provided.⁵¹ In this decision, the Supreme Court concluded that the first instance court reasonably rejected the claim and the court of appeals left the decision without changes after the courts were not able to determine that the publicised information in the article was in particular about the plaintiff's private life.

In the case of 2 January 2008, the Supreme Court found a violation of the constitutional right to privacy and confirmed that any information related to person's health would be deemed to be private.⁵² The Supreme Court rejected the argument of the Court of Appeal of Lithuania that it was necessary to publish the information in question regarding the person's health in order to inform the society about the effects of drug use. The Court found that the information was published merely to draw readers' attention and no real social interest to know the facts of a certain person's private life existed. As emphasised by the Court "lawful and well-grounded public interest to know certain information about other person cannot be equated to society's interest to satisfy its curiosity".

⁴⁹ *P. Lasas v. JSC "VP Market"*, 2 November 2004, No. 3K-3-643/2004, Supreme Court of the Republic of Lithuania, Overview of the Supreme Court Cassation Practice for the Year 2004, at 67.

⁵⁰ *Id.* at 67.

⁵¹ *J. Varapnickiene-Mazyliene v. Vilnius City Children Rights Defence Service*, 29 November 2004, No. 3K-3-600/2004, Supreme Court of the Republic of Lithuania, Overview of the Supreme Court Cassation Practice for the year 2004, at 13 - 14.

⁵² *S.Š. and V.Š. v Ltd Lietuvos rytas*, 2 January 2008, No. 3K-7-2/2008, the Supreme Court of the Republic of Lithuania.

In another case of August 2008, the Supreme Court of Lithuania has also explained that the fact that a person had not previously avoided talking to the media and had revealed information which is considered to be intimate (e.g., the conception, etc.), shall not be considered to be a consent to publish information about his/her private life.⁵³

In the case of 23 September 2008, the Supreme Court found a violation of person's right to an image. The case concerned a video shown on a local channel about the alleged violation of the traffic rules by the plaintiff, without her consent.⁵⁴ Since the Civil Code does not provide for the ways in which the consent must be expressed, the Supreme Court affirmed that upon the well-established case law it may be given verbally, in writing, or may be implied from the actions, e.g. the person talks publicly about the details of his/her private life, gives an interview for a journalist, etc. Nevertheless, consent to be photographed does not *ex officio* provide for consent to reproduce, sell, demonstrate, or publish the photograph.⁵⁵ The same rules apply for broadcasting the video record: if the person has not given consent to be recorded, be it explicitly or implicitly, it shall be deemed that he/she has not given consent to broadcast the video via media tools.

In the case of 13 February 2009, the Supreme Court again found a violation of the right to private life: the applicants' complaint concerned the publishing of pictures of them taken at the nudist beach, and thus interfering with their right to private life. The Court found that "no public interest" existed to justify this kind of interference. The Supreme Court, however, reduced the amount to be paid for the plaintiffs as non-pecuniary damage, from LTL75,000 (approximately €21,740) to LTL15,000 (€4,350).⁵⁶ One must note that the European Court of Human Rights (ECHR) has criticised the case law of Lithuanian courts regarding the reward of non-pecuniary damage.⁵⁷

In 2007 the Supreme Administrative Court heard an appeal from the Vilnius District Administrative Court concerning the practice of checking personal data and using software to compose the complete genealogical tree of anyone detained for a traffic violation.⁵⁸ The District Court had concluded that the practice was needed for the pursuit of legitimate police interests.⁵⁹ The Supreme Court reversed this finding, stating that the

⁵³ *Ž.Ž. v Ltd Ekstra Žinios*, 14 August 2008, No. 3K-3-393/2008, the Supreme Court of the Republic of Lithuania.

⁵⁴ *L.L. and A.L. v Ltd Roventa*, 23 September 2008, No. 3K-3-394/2008, the Supreme Court of the Republic of Lithuania.

⁵⁵ See also *T.G. v R.Š., Ltd Brolių Tomkų leidykla*, 24 February 2003, No. 3K-3-294/2003, the Supreme Court of the Republic of Lithuania.

⁵⁶ *D.M. and L.M. v Ltd Ekstra Žinios*, 13 February 2009, No. 3K-3-26/2009, the Supreme Court of the Republic of Lithuania.

⁵⁷ *Biriuk v. Lithuania*, Application No. 23373/03, Judgment of 25 November 2008, paragraph 44 – 47.

⁵⁸ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra* at 66-67.

⁵⁹ *Id.* at 67.

data could be processed for a person under operational investigation, but not for an individual who contravened road traffic regulations.⁶⁰

In 2008 the Supreme Administrative Court resolved a dispute in which the police published on a Web site for a month personal data related to drivers who were caught driving under the influence as an informational, educational, and preventive measure. The Court concluded that in this situation an offender's right to privacy does not counterweigh the interest of prevention of grave infringements, so such data processing was lawful.⁶¹

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The Constitution and the law limit government observation of and intrusion into individuals' privacy. Under a Criminal Procedure Law, as well as a Law on Operational Activities,⁶² wiretapping requires a warrant issued by a judge upon the request of a prosecutor. In urgent cases it may be issued by the prosecutor, but it has to be affirmed by the judge within the next three days.⁶³ Police and security services may, with this warrant, engage in surveillance and monitoring activities on the grounds of national security, law enforcement, and important financial or economic interests of the state. In practice, the boundaries of lawful surveillance are still being determined, with the emergence of new national and international case law. The list of potential surveillance targets, covered by the Law on Operational Activities, is not exhaustive, and includes "other persons and events related to the state security."⁶⁴ In addition, the law does not include a principle of proportionality – it does not contain a requirement to assess the reasonable relationship between the means employed and the aim sought to be achieved.

Courts tend to issue warrants for surveillance without strict scrutiny. In 2006 the Commission for Parliamentary Scrutiny of Intelligence Operations stated that courts had

⁶⁰ *Id.* at 67.

⁶¹ *Vilnius County Police Headquarters v. State Data Protection Inspectorate*, 24 April 2008, No. A-525-689-08, Supreme Administrative Court.

⁶² Law on Operational Activities, No. IX-965 (2002), (last amended November 2009), available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=359437.

⁶³ In Lithuanian: Baudžiamojo proceso kodeksas, article 154(1), last amendments adopted on 15 April 2008, in force as from 30 April 2008, available at http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=319053.

⁶⁴ Law on Operational Activities, *supra* Art. 3(2).

sanctioned surveillance too informally and without careful consideration.⁶⁵ This statement was based on the data received from different state institutions; for example, the Lithuanian Customs office stated that in 2004-2006, courts issued two warrants for secret checks of mail and posted documents, 604 for use of special technical equipment, and 217 for taped telephone conversations. Only once during the period of 2004-2006 did a court refuse an application for surveillance activities.

The Chairman of the Human Rights Monitoring Institute (HRMI) Steering Committee has stated that there is no clear procedure for when calls may be intercepted and when not.⁶⁶ There is no need to have very serious proof that a crime was committed.⁶⁷ The mere assumption that such a crime could be committed is sufficient for starting the wiretapping. After this happens, it is not necessary to submit the case to the court. In addition, no one explains what happens with the records. The records may be stored in the archives, copied, and later on distributed for various purposes. Moreover, there is a huge potential to intercept all phone calls of important people.⁶⁸

In 2004, the press announced that the State Security Department has the ability to tap mobile phones without any restrictions.⁶⁹ Representatives of the major telecommunication companies admitted that, taking into account current technical possibilities for the operational activity services to intercept mobile phone calls, the companies couldn't control whether the officers are tapping only those subscribers indicated in the court order. There is a lack of the detailed procedure guaranteeing that the officers would control only those subscribers indicated in the court order and only during the foreseen period of time. The institution nominated for the control of electronic communications, i.e., the State Security Department, is the same institution that conducts operational activities and pre-trial investigations.⁷⁰ The Report of the HRMI states that this is a malpractice and suggests the control of electronic communications should be allocated to another institution than the State Security Department.

The excessive use of wiretapping is particularly troubling given published leaks of collected information. In 2004, phone conversations between Parliament members who were suspected of being corrupted and private persons were publicised. These conversations were broadcast on TV and radio and publicly discussed. The heads of the

⁶⁵ "Specialiosios tarnybos seka tūkstančius, bet įtariamųjų randa tik dešimtis" ("Special Services Spy on Thousands, but Trace Only Tens of Suspects"), BNS, 23 June 2006, available at <http://www.bernardinai.lt/index.php?url=articles/49997>.

⁶⁶ Dalia Gudavičiute, "The Words Hunters Bluster without Limitations," (interview with the Chairman of the Human Rights Monitoring Institute Steering Committee), Respublika, 1 March 2005, at 4.

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ Human Rights in Lithuania 2004: Overview, 2nd Periodic Report of Human Rights Monitoring Institute, available at http://www.hrmi.lt/uploaded/HR_Overview_2004_EN_full.pdf.

⁷⁰ *Id.* at 3.

law enforcement institutions, the Deputy General Prosecutor and the Head of Vilnius Board of the Special Investigation Service, called for publicising the private conversations between the Parliament members and private persons.⁷¹

A 2005 survey on "How the Society Evaluates the Human Rights Situation in Lithuania" assessed the level of tolerance for interference with the private life of the respondent and of the public person.⁷² Respondents totalling 1,005,⁷³ from 19 cities and 59 villages, participated in the survey. Almost 80 percent of the respondents negatively evaluated the possibility to publicise their telephone conversations, but only about one-fifth of the respondents thought that publicising the conversations of a well-known politician would violate his or her right to private life.⁷⁴ For most of the people, the decisive criterion on admissibility to limit private life is the person's status in the society.⁷⁵ The threshold for the privacy protection of well-known politicians, i.e., public persons, is rather low.⁷⁶

One particular case may be noted where the Special Investigation Service tapped the phone of the mayor of Vilnius city; later, a special agent of this service handed the telephone records over to journalists.⁷⁷ The agent received only a strict warning from the Head of the Special Investigation Service, who admitted that the agent caused a lot of trouble for the Special Investigation Service. However, the agent's actions were evaluated in a liberal manner. The Head of the Special Investigation Service also denied that the agent acted with the knowledge of the superior officers.⁷⁸

On 26 June 2003, the Parliament (*Seimas*) of the Republic of Lithuania passed a resolution to ensure the protection of personal information managed by government agencies.⁷⁹ There are specific privacy protections in laws relating to

⁷¹ *Id.* at 5.

⁷² Survey "How the Society Evaluates the Human Rights Situation in Lithuania," results presented by the Human Rights Monitoring Institute in the BNS press conference, Vilnius, 17 January 2005, available in Lithuanian at http://www.hrmi.lt/uploaded/TYRIMAI/Vilmorus_2004_grafinis_pristatymas.pdf.

⁷³ See http://www.hrmi.lt/uploaded/TYRIMAI/Vilmorus_2004_grafinis_pristatymas.pdf.

⁷⁴ *Id.*

⁷⁵ Survey "How the Society Evaluates the Human Rights Situation in Lithuania," *supra*.

⁷⁶ *Id.*

⁷⁷ Liuminata Mockute, "The Man of the Week, Invisible and Inaudible Agent of the Special Investigation Service, Takes Over the Mission of the Judge," *Republika*, 19 February 2005, at 4.

⁷⁸ *Id.*

⁷⁹ Resolution of the Seimas of the Republic of Lithuania on the Guaranteeing of Personal Data Protection in State Institutions, 26 June 2003, available in Lithuanian at <http://www3.lrs.lt/cgi-bin/preps2?Condition1=214375&Condition2=>.

telecommunications,⁸⁰ statistics,⁸¹ the population register,⁸² and health information.⁸³ The Criminal Code provides for criminal responsibility for violations of the inviolability of a residence, infringement on secrecy of correspondence and telegram contents, on privacy of telephone conversations, persecution for criticism, secrecy of adoption, slander, desecration of graves, and impact on computer information.⁸⁴ The new Criminal Process Code requires a judge's authorisation for the search of premises of an individual. The seizure, monitoring, and recording of information transmitted through telecommunications networks or surveillance must also be court-ordered.⁸⁵ Civil laws provide for compensation for moral damage because of dissemination of unlawful or false information demeaning the honour and dignity of a person in the mass media.⁸⁶

The safety of classified information remains problematic. There were instances in 2006 when classified information was leaked and publicised. For example, the State Security Department (SSD) detained an editor of a newspaper for attempting to publish an article based on classified information. Although there had been an intelligence information leak, the negative consequences were borne only by the editor – he was arrested and the newspaper edition was confiscated. The SSD director publicly stated that an intensive investigation would be carried out for identification of responsible persons;⁸⁷ however, in May 2006, they were not identified. To secure better protection of classified information, HRMI supports a more effective application of the existing legal norms, which enable initiation of pre-trial investigations and punishment of guilty persons. In addition, the law should define clear and precise safety rules and foresee deterrent sanctions.

The Inspector of Journalistic Ethics noted that the data protected by the LLPPD, such as personal identification number, family status, incapacities for work, health, are too often publicised without the public interest. In particular, he drew attention to publicised information about debtors (those indebted to the mobile communication companies,

⁸⁰ Law on Electronic Communications, No. IX-2135 (2004), *supra* replacing the Law on Telecommunications No. I-1109, (1995).

⁸¹ Law on Statistics, No. I-270 (1993), available at <http://www.stat.gov.lt/en/pages/view/?id=1851>.

⁸² Law on the Population Register, No. I-2237 (1992), available at <http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/44.HTM>.

⁸³ Law on the Health System, No. I-552 (1994), available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=23358.

⁸⁴ Criminal Code of the Republic of Lithuania, adopted by the Law No VIII-1968 on 26 September 2000.

⁸⁵ United States Department of State, Country Reports on Human Rights Practices, Lithuania, 2003, *supra*.

⁸⁶ United Nations Human Rights Committee, Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Initial reports of States parties due in 1993, Addendum, Lithuania, 1996.

⁸⁷ "Seimą jau pasiekė slapta VSD pažyma, sukėlusi skandalą" ("Parliament Received a Secret SIS Document that Caused a Scandal"), BNS, 19 September 2006, available at <http://www.delfi.lt/news/daily/lithuania/article.php?id=10730616>.

municipality companies).⁸⁸ The Inspector of Journalistic Ethics said in his report that a public announcement of debtors in the newspapers and other mass media initiated by the creditors is not lawful and violates the rights of these persons. Creditors do not have a right to disseminate information about debtors' solvency.⁸⁹ Some of the companies consider this an effective measure in the fight against the debtors' insolvency.⁹⁰ However, publicising such information should not become a precedent in the democratic society.⁹¹ Currently, the amendments to the LLPPD concerning rules for personal data processing for the purposes of solvency evaluation and debt management are pending in the Parliament.⁹²

In 2009 the press again announced that the tendencies of wiretapping in 2008 and 2009 remained the same: the number of requests for wiretapping provided by the SSD to the judges was so high that the judges issued warrants without sufficient time to dwell on them more carefully.⁹³

In October 2009 information spread around in public discourse about the wiretapping of journalists performed by the SSD.⁹⁴ As it turned out later, the Šiauliai District Court issued a warrant to wiretap Vilnius journalists upon the request of the SSD.

The Commission for Parliamentary Scrutiny of Intelligence Operations, which investigated the wiretapping of the journalists, stated that subjects of operational activities could in fact wiretap any person and sometimes this is being carried out in violation of the law.⁹⁵ It also found that the requests for wiretapping were not always submitted by the prosecutors, as sometimes entities of operational activities applied straight to the judges themselves, thus acting in violation of the law. The Commission

⁸⁸ Activity Report of the Inspector of Journalistic Ethics for the Year 2003-2004, 13 April 2004, available in Lithuanian at http://www3.lrs.lt/pls/inter/w5_show?p_r=2564&p_d=41808&p_k=1.

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² Draft Amendments to the Law on Legal Protection of Personal Data, 29 March 2010, No. XIP-760(2), Section 4, available in Lithuanian at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=368050&p_query=&p_tr2=.

⁹³ Liepa Pečeliūnaitė, "Malakauskas telefoninių pokalbių klausosi tiek pat, kiek klausėsi Pocius" ("Malakauskas Wiretaps as much as Pocius Did"), *alfa.lt*, 13 May 2009, available at <http://www.alfa.lt/straipsnis/10272735>.

⁹⁴ Eglė Digrytė, "D. Kuolys: sankcijos klausyti žurnalistų pokalbių VSD gaudavo Šiauliuose" ("D.Kuolys: SSD Acquired Warrants for Journalists' Wiretapping in Šiauliai"), *Delfi.lt*, 22 October 2009, available at <http://www.delfi.lt/news/daily/lithuania/dkuolys-sankcijos-klausyti-zurnalistu-pokalbiu-vsd-gaudavo-siauliuose.d?id=24971853>.

⁹⁵ "Seimo komisija: Lietuvoje galima pasiklausyti bet kurio žmogaus pokalbio" ("Parliament Commission: Any Conversation Might be Wiretapped in Lithuania"), *Vakaru Ekspresas*, 15 January 2010, available at <http://www.ve.lt/naujienos/lietuva/lietuvos-naujienos/seimo-komisija-lietuvoje-galima-pasiklausyti-bet-kurio-zmogaus-pokalbio/>.

also criticised the lack of an integrated information system in Lithuania where information regarding the warrant issue would be available for all the courts in Lithuania. The present situation allows someone to reapply to a different court in a different city requesting a warrant for wiretapping if the first request is not granted.

National security legislation

No specific information has been provided under this heading.

Data retention

The government adopted a resolution that affects Internet privacy.⁹⁶ The Resolution introduces data retention requirements for hosting service providers. They are required to log operations with data and content hosted on their servers and to provide them free of charge, along with the personal data of the individual and entities using the hosting services, to criminal investigators and other law enforcement authorities. However, the obligation to provide such data is limited to data necessary for normal business operations, following the September 2002 Constitutional Court decision.⁹⁷

On 15 April 2004, the Parliament adopted Law No. IX-2135 on Electronic Communications,⁹⁸ which replaced the former Law on Telecommunications. The law implements all of the EU directives of 2002 on electronic communications, including the EU Directive on Privacy and Electronic Communications (2002/58/EC), and is aimed at regulating the operation of electronic communications in Lithuania.⁹⁹

In March 2006, the European Union amended the EU Directive on Privacy and Electronic Communications by enacting the Directive 2006/24/EC (Data Retention Directive), which requires Member States to require communications providers to retain communications data for a period of between six months and two years.¹⁰⁰ Though Lithuania was among the 16 Member States that have declared that they would delay the implementation of data retention of Internet traffic data for the additional period, the

⁹⁶ The Resolution No. 290 of 5 March 2003 on Procedures for Control of Harmful Information and Distribution of Restricted Information in Publicly Accessible Computer Networks.

⁹⁷ Constitutional Court of the Republic of Lithuania, Ruling on compliance of Paragraph 2 of Article 27 of the Republic of Lithuania Law on Telecommunications (...), 19 September 2002, available at <http://www.lrkt.lt/dokumentai/2002/r020919.htm>.

⁹⁸ Law on Electronic Communications, No.IX-2135 (2004), *supra*.

⁹⁹ See Petrauskas Lideika, Update June 2004, Infolex.lt, June 2004, available at <http://www.infolex.lt/portal/ml/start.asp?act=legupd&lang=eng&biulid=87>.

¹⁰⁰ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT>.

relevant amendments were made to the Law on Electronic Communication and came into force on 15 March 2009.¹⁰¹

Annex No. 1 to the Law on Electronic Communication lists the categories of data to be retained, which is identical to Article 5(1) of Directive 2006/24/EC. According to the Law on Electronic Communication Data, retention period for traffic data in Lithuania is six months and an additional six months if this data is necessary for operational investigation services, pre-trial investigation institutions, prosecutors, courts, or judges to prevent, investigate and detect criminal acts.¹⁰²

National databases for law enforcement and security purposes

Lithuania joined Schengen Information System in September 2007. The System contains data on certain wanted/controlled persons and objects that can be accessed by relevant Lithuanian law enforcement agencies.¹⁰³

National and international data disclosure agreements

In 5 June 2008, Lithuania ratified an Agreement between the European Union and the United States of America on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the US Department of Homeland Security (DHS).¹⁰⁴ On 21 May 2009, Lithuania ratified a similar agreement concerning the processing and transfer of European Union-sourced PNR data by air carriers to the Australian Customs Service.¹⁰⁵

The EU Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters has not been transferred into Lithuanian national laws yet.¹⁰⁶ The draft version of the Law on legal protection of personal data processed in the framework of police and judicial cooperation in criminal matters, however, has already been prepared

¹⁰¹ Law on Electronic Communications, No. IX-2135 (2004), *supra*.

¹⁰² *Id.* Art.66 (6).

¹⁰³ More information on the SIS are available at http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133020_en.htm.

¹⁰⁴ In Lithuanian: Įstatymas dėl Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimo dėl oro vežėjų atliekamo keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Jungtinių Valstijų Vidaus Saugumo Departamentui (DHS) (2007PNR susitarimo) ratifikavimo, No. X-1577, adopted on 5 June 2008, in force as from 14 June 2008, available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=322127&p_query=&p_tr2=.

¹⁰⁵ In Lithuanian: Įstatymas dėl Europos Sąjungos ir Australijos susitarimo dėl oro vežėjų atliekamo Europos Sąjungos pateiktų keleivio duomenų įrašo (PNR) duomenų tvarkymo ir perdavimo Australijos Muitinės Tarnybai ratifikavimo, No. XI-267, adopted on 21 May 2009, in force as from 6 June 2009, available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=345290&p_query=&p_tr2=.

¹⁰⁶ OJ L 350, 30 December 2008, at 60-71, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML>.

by the State Data Protection Inspectorate and presented for coordination in February 2010.¹⁰⁷

Cybercrime

The Criminal Code of Lithuania provides for criminal liability for crimes against security of electronic data and information systems.¹⁰⁸ Article 196 states, "A person who unlawfully destroys, damages, removes, or modifies electronic data or technical equipment or software or otherwise restricts the use of such data thereby incurring major damage shall be punished by community service, by a fine, or by imprisonment for a term of up to four years." A person who unlawfully disturbs or terminates the operation of an information system thereby incurring major damage, or a person who unlawfully observes, records, intercepts, acquires, stores, appropriates, distributes, or otherwise uses the electronic data which may not be made public is subject to a fine or imprisonment. A legal entity shall also be held liable for these acts. A person who unlawfully connects to an information system by damaging the protection means of the information system shall be punished by community service, by a fine, or by imprisonment for a term of up to one year. A person who unlawfully produces, transports, sells or otherwise distributes the installations of software, also passwords, login codes, or other similar data directly intended for the commission of criminal acts or acquires or stores them for the same purpose shall be punished by community service, by a fine, or by imprisonment for a term of up to three years. A legal entity shall also be held liable for these acts.

Critical infrastructure

No specific information has been provided under this heading.

INTERNET & CONSUMER PRIVACY

E-commerce

Law on Electronic Communications provides that any electronic communication services, including e-mail messages, for direct marketing purposes may be used only upon a prior consent of subscriber or registered user of electronic communication services. The number of personal complaints submitted to the Inspectorate in 2009 concerning the processing of personal data for the direct marketing purposes was the highest. In comparison to 2008, the number of these complaints has increased three times.¹⁰⁹

In February 2009 the Inspectorate received a complaint regarding unwanted email messages. The Inspectorate found violations of the LLPPD and of the Law on Electronic Communications: an illegal processing of personal data and illegal use of personal email

¹⁰⁷ In Lithuanian: Asmens duomenų, tvarkomų vykdančios policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, teisinės apsaugos įstatymas, No. 10-508-01, available at http://www.lrs.lt/pls/proj/dokpaieska.showdoc_l?p_id=20814&p_org=&p_fix=y&p_gov=n.

¹⁰⁸ Criminal Code of the Republic of Lithuania, *supra*.

¹⁰⁹ Annual Activity Report 2009 of the State Data Protection Inspectorate, *supra* at 13.

address for direct marketing purposes. A person was collecting, accumulating and storing email addresses and using them for direct marketing purposes, i.e., sending unwanted email messages, and he did not follow the criteria for lawful processing of personal data. He got a fine of LTL100 (approx. €30).¹¹⁰

Cybersecurity

No specific information has been provided under this heading.

Online behavioural marketing and search engine privacy

No specific information has been provided under this heading.

Online social networks and virtual communities

No specific information has been provided under this heading.

Online youth safety

No specific information has been provided under this heading.

TERRITORIAL PRIVACY

Video surveillance

As previously reported, the latest amendments of the LLPPD of 1 January 2009 introduced a new chapter on video surveillance, which includes a definition of the concept of video surveillance, rules for installation of video surveillance devices, and notification to data subjects and processing of collected video data. These amendments to the LLPPD addressed the issue of video surveillance and created procedures that must be followed.¹¹¹ Among other things, the amendments require notification of public surveillance and prohibit surveillance in the workplace, except in cases to ensure safety.¹¹²

More and more companies and organisations have established video surveillance systems in public places. As of 2004, the Inspectorate had not yet made a systemic legal analysis on the use of video surveillance measures and had limited itself to the review of single complaints.¹¹³ In the absence of proper legal safeguards, in 2006 the HRMI observed a noticeable increase in establishment of video surveillance systems. In Vilnius, streets are

¹¹⁰ "Po Valstybinės duomenų apsaugos inspekcijos išnagrinėto skundo teismas pripažino pažeidimus dėl nepageidaujamų elektroninio pašto pranešimų siuntimo" ("Court Finds Violations Regarding Unwanted Email Messages, After Judging on Complaint of the State Data Protection Inspectorate"), Teises Forumas, available at <http://www.teisesforumas.lt/index.php/idomybes-ir-naudinga-informacija/732-vdai-isnagrinetas-skundas.html>.

¹¹¹ The Law on Legal Protection of Personal Data, *supra* at Art. 3.

¹¹² *Id.*

¹¹³ Human Rights in Lithuania 2004, *supra*.

monitored now by over 200 cameras.¹¹⁴ A growing number of video cameras had been installed in Kaunas, Klaipėda, Panevėžys, Šiauliai. and Kėdainiai.¹¹⁵ Vilnius municipality planned to allocate LTL2 million (approx. €580,000) each year for the maintenance of the system.¹¹⁶ Kaunas spends nearly LTL50,000 (approx. €14,500) each month for maintenance of its systems.¹¹⁷ The claims about the usefulness and effectiveness of video surveillance systems without a cost-benefit analysis remain questionable. In addition, public notice regarding video surveillance systems is lacking, and no signage regarding cameras in public places has been installed. On 20 March 2006, groups in Vilnius celebrated the "International Day Against Video Surveillance".

In March 2010, press announced that a secret video and audio surveillance system was installed in a night club "Paradoksas" in Klaipėda. Supposedly, the surveillance system was installed in 2008 and was used to collect private information about the visitors to the club.¹¹⁸ Klaipėda County Police Headquarters and Klaipėda Regional Prosecutor's Office have started a pre-trial investigation on the issue.¹¹⁹ Another article reported a detention of suspects in Vilnius as a result of a video surveillance: a girl was noticed on surveillance cameras consuming alcoholic drinks in a public place and consequently was detained; and two men were noticed stealing a mobile phone and also were detained.¹²⁰

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this heading.

¹¹⁴ "A Big Brother Will Openly Watch in Vilnius," *Omni*, 21 November 2006.

¹¹⁵ "Video Surveillance System Is Installed in Kaunas," *Irytas.lt*, 18 October 2006; Gina Kubiliūtė, "Klaipėdos parką nuo vandalų saugos kameros" ("Secret Cameras Will Protect Klaipėda Park from Vandals"), *Klaipėda*, 12 April 2006, available at <http://www.delfi.lt/archive/article.php?id=9292911&categoryID=5995&ndate=1144789200> ; "Panevėžiečiai parinko vaizdo kamerų vietas" ("People in Panevėžys Have Selected Places for the Installation of Video Cameras"), *Delfi*, 11 April 2006, available at <http://www.delfi.lt/archive/article.php?id=9280896> ; "Šiomet Panevėžyje bus įrengta 11 vaizdo kamerų" ("This Year 11 Video Cameras Will Be Installed in Panevėžys"), *vtv.lt*, 13 February 2006, available at <http://www.vtv.lt/content/view/15105/345>.

¹¹⁶ "Network of Video Surveillance System Will be Extended in Vilnius," *Delfi*, 6 December 2006.

¹¹⁷ "In Kaunas is Installed the Video Surveillance System," *Irytas.lt*, 7 February 2006.

¹¹⁸ Stasys Vaitonis and Bronius Beinoravičius, "Klaipėdos naktiniame klube slapta buvo klausomasi lankytojų pokalbių" ("Secret Surveillance System Installed in Klaipėda's Night Club"), *Irytas.lt*, 9 March 2010, available at <http://www.iryta.lt/-12681488611267151908-klaipėdos-naktiniame-klube-slapta-buvo-klausomasi-lankytojų-pokalbių-video.htm>.

¹¹⁹ "Buvo šnipinėjami naktinio klubo lankytojai" ("Night Club Visitors Were Being Spied On"), *Delfi*, 9 March 2010, available at <http://www.delfi.lt/news/daily/crime/buvo-snipinejami-naktinio-klubo-lankytojai.d?id=29841405> .

¹²⁰ "Pasitelkus vaizdo kameras Vilniuje sulaikyti įtariamieji" ("Suspects Detained After Being Caught on Surveillance Cameras in Vilnius"), *Klaipėda*, 4 June 2010, available at <http://klaipeda.diena.lt/naujienos/kriminalai/vaizdo-kameru-pagalba-vilniuje-sulaikyti-itariamieji-282276>.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Pursuant to EU Council Regulation No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by the member states,¹²¹ on 8 August 2008, Lithuania started issuing passports containing biometric data (facial image) and secured by basic access control. Moreover, the roll-out of new Lithuanian Passports following the "EU model" was to commence on 2 January 2008.¹²²

NATIONAL ID & SMART CARDS

Recently, Lithuania started to issue passports with biometric data to Lithuanian diplomats. In 2006, the Parliament amended Laws on Regular Passport,¹²³ Official Passport,¹²⁴ and State Registry¹²⁵ to introduce the use of biometric data (digital images of the face and fingerprints) in all passports and information storage in the state register. The European Union Regulation regulating personal biometric data and its storage provided Member States with discretion in deciding whether to store data only in the personal document or in the state registry as well. The HRMI urged members of Parliament while voting for amendments of law to take into consideration that biometric data storage in one centralised state database may put at risk the safety of stored information and leave possibilities for its leak.¹²⁶ The HRMI publicly opposed information storage in a centralised state registry; however, the law amendments were adopted and parliamentarians' discussion was limited only to the costs incurred in application of the new technology. Information provided to the public took the form of a public relations campaign and advertising portraying the adoption of biometric passports as an attractive innovation which increases the security of society,¹²⁷ without discussing the privacy implications. Passports that follow the EU Model for access to biometric data started to be issued in January 2008.¹²⁸

Another important issue concerning passports relates to writing of non-Lithuanian characters in the passports of Lithuanian citizens. On 6 November 2009, the

¹²¹ OJ L 385, 29 December 2004, at 1-6, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:HTML>.

¹²² ePractice, eGovernment Factsheet – Lithuania – Infrastructure (February 2010), available at <http://www.epractice.eu/en/document/288300>.

¹²³ Available in Lithuanian at http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=279763.

¹²⁴ Available in Lithuanian at http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=279764.

¹²⁵ Available in Lithuanian at http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=277499.

¹²⁶ Henrikas Mickevičius, "In Depth Discussion on the Planned Usage of Biometrical Data is Necessary," HRMI, 26 January 2006, available at <http://www.hrmi.lt/en/new/464/>.

¹²⁷ "Išduodami pasai su skaitmeniniu savininko atvaizdu" ("Passports Are Issued With the Digital Pictures of the Owner"), *Delfi*, 28 August 2006, available at <http://www.delfi.lt/archive/article.php?id=10507177>.

¹²⁸ ePractice, eGovernment Factsheet – Lithuania – Infrastructure, *supra*.

Constitutional Court of Lithuania submitted clarification regarding the writing of name and surname in the passport of a citizen of Lithuania. Though in general it is prohibited to write a person's name and surname in any other characters but Lithuanian in the passport, the Constitutional Court submitted that a legislature had a discretionary power to allow inclusion in some section of the same passport of a name and surname in non-Lithuanian characters and in non-grammatical form, if the person so wishes.¹²⁹

RFID tags

No specific information has been provided under this heading.

BODILY PRIVACY

A big issue of concern is a report, published in media several times, of surveillance cameras hidden in solariums, beauty salons, or cosmetology rooms. Last year the State Data Protection Inspectorate, upon an anonymous complaint, investigated the "Bovary" beauty saloon in Vilnius, and found eight cameras installed in almost every room, including the dressing-rooms of the employees and the cosmetology rooms. Upon the administrative law offence protocol submitted by the Inspectorate, Vilnius First Circuit Court fined the company LTL600 (approx €175) in April 2010.¹³⁰

WORKPLACE PRIVACY

The HRMI reported that in 2004 there was an active trade in computer software that allowed control of an employee's computer. Such control creates unlimited possibilities to observe the work of the employee. A special software installation enables employers to gain access to employees' electronic correspondence and see which Web sites are visited on the Internet. Although such software usage is becoming increasingly popular among private business enterprises, there is no legal framework regulating electronic surveillance at the workplace.¹³¹ Trade unions do not express concern for the matter. The HRMI suggests that to prevent individuals from losing their entitlement to respect for private life in the workplace, employers should always inform employees about the use of electronic surveillance in advance, explain its purpose, and obtain the employee's agreement. A law should further specify situations and conditions for electronic surveillance and provide deterrent sanctions. Considering the urgency of the issue, the proper legal regulation should be adopted as soon as possible. Currently, workplace privacy in Lithuania is regulated only by general provisions of the LLPPD and other privacy laws. However, the Inspectorate in its practice follows the recommendations of

¹²⁹ Constitutional Court of the Republic of Lithuania, Decision on Clarification of 21 October 1999 Constitutional Court Ruling's points 4 and 7 of the reasoning part, 6 November 2009, available at <http://www.lrkt.lt/dokumentai/2009/s091106.htm>.

¹³⁰ "Už slaptas kameras Vilniaus grožio salone – 600 litų bauda" ("600 Litas Fine for Hidden Surveillance Cameras in Vilnius Beauty Salon"), *Irytas.lt*, 25 May 2010, available at <http://www.irytas.lt/-12747706451273054336-uz-slaptas-kameras-vilniaus-grozio-salone-600-litu-bauda.htm>.

¹³¹ Valerija Lebedeva, "Electronic Working Place Control Is Not Legally Regulated," *Vakary ekspresas*, 13 November 2006.

Article 29 Data Protection Working Party.¹³² Overall, court practice is leaning towards allowing the employer's control over employee communication, as long as it is transparent and the employees are properly informed.

HEALTH & GENETIC PRIVACY

Medical records

The Law on the Rights of Patients and Compensation of the Damage to Their Health, adopted in 1996 and amended several times, most recently on 1 March 2010, provides rules concerning the inviolability of the patient's private life.¹³³

The Law requires that information on the facts of a patient's life can be collected only upon his/her consent and only if it is necessary to detect or treat a disease or to nurse a patient. All the medical information related to a patient's visits or stays in a health care institution, his/her health, means of detection or treatment of disease, or his/her nursing must be contained in patient's medical documents of a set form and kind. This information shall be deemed to be private after the patient's death as well. Successor by the will, heir by operation of law, spouse (partner), parents and children have a right to obtain this information after the patient's death.

Confidential information can be provided to other persons only upon the written consent of the patient, which also has to indicate grounds for such consent and a purpose except where the patient had indicated a concrete person who can be provided with the information in the medical documents. Confidential information about the patient's health can be provided without the patient's consent to the State institutions entitled by Lithuanian laws to acquire such information. Confidential information shall be provided only upon a written request by the relevant persons, indicating the basis of the request, purpose of the use of the information and the extent of information requested.

The Law on the Rights of Patients and Compensation of the Damage to Their Health submits that any person shall be accountable by law for any illegal collection and use of confidential information about a patient. In order to safeguard the patient's right to private life, the interests and welfare of a patient shall prevail over the interests of society. The application of this rule could only be limited if it is necessary for the protection of public safety, crime prevention, public health, or other human rights and freedoms. The Law also foresees a possibility to receive medical treatment without revealing a person's identity, provided the patient is older than 16 years, and he/she is sick with a certain disease defined by the Government. That being the case, the patient shall cover the expenses of healthcare services on his/her own.

¹³² Working document on the surveillance of electronic communications in the workplace, 29 May 2002, WP 55, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf.

¹³³ Law on the Rights of Patients and Compensation of the Damage to their Health In Lithuanian, *supra*.

In 2005 the Ministry of Health of Lithuania commenced the implementation of a health services system called "eHealth services".¹³⁴ On 18 June 2010, the Minister of Health adopted an eHealth system development programme project for the years 2009-2015. The main objectives of the programme are to develop a customer-oriented eHealth system, which would provide him/her with direct and indirect services, and to develop an effective infrastructure of eHealth services and cooperation.¹³⁵

Genetic identification

No specific information has been provided under this heading.

FINANCIAL PRIVACY

No specific information has been provided under this heading.

E-GOVERNMENT & PRIVACY

In Lithuania the Central Government is responsible for providing citizens with a different kind of e-services. Launched in January 2004, the Lithuanian eGovernment portal (reachable via "www.evaldzia.lt" and "www.epaslaugos.lt") is intended to offer access to public information and services for citizens and businesses. It offers links to the public information and public services by redirecting citizens and businesses to the appropriate Web sites of public authorities. The Gates of the eGovernment portal is currently being updated with tools for electronic personal identification, centralised access to electronic public services, online payment for the requested services, and online tracking of the service provision process. The person's identification in the Portal is available through eBanking systems, using a national identity card, eSignature certificates or the mobile signatures of certain operators. Currently, the portal offers 18 public eServices.¹³⁶

For example, an electronic declaration system has been available in Lithuania since 2004. This fully transactional system enables electronic filing of all tax returns: income tax returns, corporate tax returns, VAT returns, etc. Its key features include: multiple ways to fill in and submit declarations, notification on the status of declarations, multiple authentication methods, centralised archive, data exchange with other systems, new designs of return forms, and declaration process monitoring and management. Now, the service provider offers pre-filled declaration forms with some relevant data.¹³⁷

¹³⁴ ePractice, eGovernment Factsheet – Lithuania – Infrastructure, *supra*.

¹³⁵ In Lithuanian: Lietuvos Respublikos sveikatos apsaugos ministro įsakymas dėl E. Sveikatos sistemos 2009 – 2015 metų plėtros programos įgyvendinimo priemonių plano patvirtinimo, 18 June 2010, No V-570.

¹³⁶ For more information see ePractice, eGovernment Factsheet – Lithuania – Infrastructure, *supra*.

¹³⁷ See eGovernment Factsheet - Lithuania - eServices for Citizens (February 2010), available at <http://www.epractice.eu/en/document/288301>.

In 2008, Lithuania launched two projects relating to e-identification.¹³⁸ Under the "Project of the Civil Service Department", new public servants' identification cards were released, starting in September 2008, with chips containing both an identification and an e-signature certificate.¹³⁹ The "Creation of the Infrastructure for the Establishment of the National Certification Centre and Personal Identification in the Electronic Space" created the means to issue personal e-identification cards and insure interoperability.¹⁴⁰ In January 2009, electronic identity cards were first offered, containing a chip that provides identification and e-signature certificates as well as a chip with biometric data, including a facial image and fingerprints.¹⁴¹ Lithuania hopes to have all public institutions using electronic document exchange by the end of 2010, primarily through the use of qualified certificates that would allow for e-signatures. Since 2007 Lithuania has allowed e-signatures through the use of a SIM card in a mobile phone.¹⁴²

OPEN GOVERNMENT

The 1996 Law on the Provision of Information to the Public provides for a limited right of access to official documents and to documents held by political parties, political and public organisations, trade unions, and other entities.¹⁴³

There were subsequent developments with regard to various registers. At the beginning of 2004, the Information Systems on the Administration of the Debtors, which included both natural and legal persons, started to operate.¹⁴⁴ On average, there were more than 340,000 records and 100,000 requests made each month. In December 2004, the requests increased to 200,000 per month.¹⁴⁵ In 2005, the Electronic Internal Waters Vessels Register was created.¹⁴⁶ The register interacts with other state registers and information systems and will guarantee the effective distribution of information to the data subjects, such as marshalls, judicial institutions, and Tax Inspectorate.¹⁴⁷

¹³⁸ ePractice, eGovernment Factsheet – Lithuania – Infrastructure, *supra*.

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ Law on the Provision of Information to the Public, 2 July 1996 No.I-1418 (as amended on 11 July 2006 – No.X-752), art. 6.

¹⁴⁴ "News flow. Debts," *Lietuvos Rytas*, 4 March 2005, at 11.

¹⁴⁵ *Id.*

¹⁴⁶ "The Electronic Internal Waters Vessels Register Created," *Respublika*, 23 February 2005, at 28.

¹⁴⁷ *Id.*

The Lithuanian Social Insurance Fund now provides data by electronic means to private companies, such as banks and leasing companies.¹⁴⁸ The banks only have partial access to the data stored in the Social Insurance Fund's database. They are allowed to access the data concerning their client's solvency and data about a client's employment or work history and salary as well as any received pensions or one-time payments.¹⁴⁹ The banks are able to access the database only after receiving written consent of the client. Access to the database is provided for a certain fee at the bank's request. In 2005, an investigation was started concerning a copy of the Social Insurance Fund's database, allegedly sold for LTL10,000 (approx. €2,900) to special investigation officers who pretended to be potential purchasers.¹⁵⁰ The copy contained 20GB of data on the income of 1.5 million workers and 100,000 companies, names, surnames, workplaces, and home addresses.¹⁵¹

The Law on the Right to Acquire Information from the State and Municipality Institutions and Agencies requires that all information regarding the activities of institutions while performing their legal functions shall be accessible to everyone and provided free of charge.¹⁵² The amendments made to the Law on 31 July 2008 equated information on the salary of an employee of an institution to information on the activities of institutions. Therefore, information on the salary is not considered to be private information any more. HRMI submits that applicability of a principle of publicly declared salary to all the employees of institutions may not always be justifiable by the public interest. Through the perspective of human rights, only salaries of persons performing public administration powers, administering a provision of public services, or whose activities influence public matters, should undoubtedly be public.

The amendments to the Law on the Right to Acquire Information from the State and Municipality Institutions and Agencies, that came into force on 1 July 2010, detailed certain information that must be published on the official Web sites of State or Municipality institutions. The publication of the information must comply with the provisions of the LLPPD and other laws.¹⁵³

¹⁴⁸ See Mantas Dubauskas, "The Country Banks will not Require Any More Piles of Notes," *Lietuvos Rytas*, 10 February 2005, at 10, and Martynas Zilionis, "Data about Salary – Directly from the Social Insurance Fund," *Respublika*, 12 March 2005, at 17.

¹⁴⁹ *Id.*

¹⁵⁰ Justinas Vanagas, "Trade in Social Insurance Fund's Data," *Lietuvos Zinios*, 30 April 2005.

¹⁵¹ *Id.*

¹⁵² In Lithuanian: Teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymas, No. VIII-1524, adopted on 11 January 2000, amended on 13 May 2010, in force as from 31 May 2010, article 6(3), available at http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=373811.

¹⁵³ *Id.* article 6(2).

OTHER RECENT FACTUAL DEVELOPMENTS

In the past few years, data protection issues in courts' practice started to emerge. The HRMI reports that the use of technical measures during the court hearings is not properly regulated.¹⁵⁴ The Law foresees wide possibilities for the use of video recording and other technical measures during court hearings; however, there are no comprehensive rules for the storage and destruction of the collected data.¹⁵⁵ The courts in their decisions still frequently use full names and last names of the parties in publicised court decisions and include excessive personal data of the parties to the case. Examples include addresses and sometimes even personal identification numbers, which jeopardise the interests of the parties.

Article 123(3) of the Civil Procedure Code provides that if a person who is delivering a procedural document does not find the addressee at home or at his/her workplace, one of the options to deliver the document is to hand it over to the administration of the addressee's workplace. However, it should be noted that such a document contains not only the plaintiff's, but also the defendant's personal data, which should not be accessible to the employer, unless the employer is a party to the case.¹⁵⁶

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Since 2004 the HRMI publishes Human Rights Overviews with a focus on the privacy issue. A team of human rights experts, with a reference to data collected during media monitoring, reports, analysis of legislation, and personal insights, and other documents from national and international institutions, produces an extensive evaluation of the human rights situation according to set criteria. Privacy has also been addressed in the last Human Rights Overview of 2007-2008,¹⁵⁷ which was widely disseminated among legal practitioners, public institutions, law enforcement officers and other NGOs, and was followed by a number of round-table discussions and briefings with stakeholders. In 2007, the HRMI also organised a two-day international workshop on the Right to Freedom of Expression and the Rights to Respect for Private Life, which analysed the interrelation of two fundamental human rights. In 2010, the HRMI addressed the Ministry of Transport and Communications with regard to its recently adopted order. The legal act provides for video and audio recordings to be made in the motor vehicle during the final driving test, with the data to be kept for a period of a year after finishing the driving

¹⁵⁴ Human Rights in Lithuania 2004, *supra*.

¹⁵⁵ *Id.*

¹⁵⁶ Seminar "Data Processing in the Courts," by Dr. Krause, Vilnius, 21 April 2005.

¹⁵⁷ Human Rights in Lithuania 2007-2008: Overview, 5th Periodic Report of Human Rights Monitoring Institute, available at http://www.hrmi.lt/uploaded/PDF%20DOKAI/Human_Rights_Overview_2007_2008.pdf.

course.¹⁵⁸ The HRMI advocated for an amendment of the order as it does not respect the right to private life and is contrary to the data protection standards.¹⁵⁹

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Lithuania acceded to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol that establishes an individual complaint mechanism.¹⁶⁰

Lithuania is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁶¹ In June 2001 it ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹⁶² In 2004 Lithuania has ratified the Council of Europe Convention on Cybercrime.¹⁶³ On 1 February 2007, Lithuania signed the Additional Protocol to the Convention on Cybercrime.¹⁶⁴

In February 2001, the European Court of Human Rights accepted two cases against Lithuania filed by a former prosecutor and a former tax inspector who alleged that their privacy was violated when they were fired from their positions and prohibited from taking certain posts in the private sector because of their previous collaboration with the KGB.¹⁶⁵ On 27 July 2004, ECtHR concluded that the ban on the applicants seeking employment in various private-sector spheres, in application of Article 2 of the KGB Act, constituted a disproportionate measure, even having regard to the legitimacy of the aims pursued by that ban and, thus, found a violation of Article 14 of the Convention taken in conjunction with Article 8.¹⁶⁶ In another case, the applicants, also former KGB agents,

¹⁵⁸ In Lithuanian: Lietuvos Respublikos susisiekimo ministro įsakymas "Dėl vairuotojų pirminio mokymo tvarkos aprašo patvirtinimo", 12 August 2010, No 3-493, available here.

¹⁵⁹ In Lithuanian: HRMI, Raštas dėl LR Susisiekimo ministro įsakymo "Dėl vairuotojų pirminio mokymo tvarkos aprašo patvirtinimo", 5 October 2010, available at @@.

¹⁶⁰ Lithuania accessed the ICCPR and its First Optional Protocol on 20 November 1991. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁶¹ Signed on 14 May 1993; ratified on 20 June 1995; entered into force as from 20 June 1995, available at <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>.

¹⁶² Signed on 11 February 2000; ratified on 1 June 2001; entered into force as from 1 October 2001, available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm>.

¹⁶³ Signed 23 June 2004; ratified 18 March 2004; entered into force 1 July 2004, available at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

¹⁶⁴ Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=3&DF=7/1/2009&CL=ENG>.

¹⁶⁵ "Strasbourg Probing 2 Cases Of Ex-KGB Agents Vs. Lithuania," Baltic News Service, 8 February 2001.

¹⁶⁶ *Sidabras and Dziautas v. Lithuania*, ECtHR, Applications Nos. 55480/00 and 59330/00, 27 July 2004.

complained that the loss of their jobs, respectively, as a private-company lawyer and barrister, and the ban on their employment in various private-sector spheres until 2009, breached their privacy. The Court recalled the case of *Sidabras and Džiautas* explaining that the applicants' complaints were very similar, albeit wider: they related not only to their hypothetical inability to apply for various private-sector jobs until 2009 (as in *Sidabras and Džiautas*), but they also concerned their actual dismissal from existing employment in that sector. Consequently, the ECtHR found a violation of Article 14 of the Convention, taken in conjunction with Article 8.¹⁶⁷

In 2005, the European Court of Human Rights found that Lithuania violated the right to respect for private and family life¹⁶⁸ embedded in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁶⁹ The applicant's complaint concerned the opening up and reading by the prison administration of all his letters to and from the State authorities, NGOs, and private persons such as his family, relatives, friends, and legal counsel. The Court noted that interference with the applicant's right to respect for his correspondence could only be justified if such interference would be "in accordance with the law", pursued a legitimate aim and was necessary in a democratic society in order to achieve that aim.¹⁷⁰ The interference had a legal basis, namely the provisions of the Detention on Remand Act and Remand Prisons Internal Rules, and the Court was satisfied that it pursued the legitimate aim of "the prevention of disorder or crime". However, as regards the necessity of the interference, the government had not explained why the control of all of the applicant's letters addressed to him and coming from the outside world was indispensable. The Court explained that the government's reason, namely the fear of the applicant's absconding or influencing his trial, may have been a basis for a certain form of interference with part of his correspondence, such as, for example, checking of some correspondence of non-legal nature or his correspondence with certain persons of dangerous provenance. However, the Court said that this fear alone could not be sufficient to grant the remand prison administration an open licence for indiscriminate, routine checking of all of the applicant's correspondence, in particular the applicant's letters from his legal counsel.¹⁷¹ The Court also did not find any reason to justify the censorship by the prison administration of the applicant's letters to State authorities. Overall, the government has not presented sufficient reasons to show that such a total control of the applicant's correspondence with the outside world was "necessary in a democratic society." Consequently, the Court found a violation of Article 8 of the Convention. The ECtHR affirmed this position in its 16 November 2006

¹⁶⁷ *Rainys and Gasparavicius v. Lithuania*, Applications Nos. 70665/01 and 74345/01, 7 April 2005.

¹⁶⁸ *Jankauskas v. Lithuania*, ECtHR, Application No. 59304/00, 24 February 2005.

¹⁶⁹ Convention for the Protection of Human Rights and Fundamental Freedoms, available at <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf>.

¹⁷⁰ *Jankauskas v. Lithuania*, *supra*.

¹⁷¹ *Id.*

decision, *Ciapas v. Lithuania*, where prison administration opened and read all of the applicant's correspondence from his wife, his co-suspects, and his acquaintances.¹⁷² As of 31 December 2007, Lithuania had 420 cases pending before the European Court of Human Rights and 35 cases adjudicated before it.¹⁷³ In 2008 the number of cases pending increased to 448.¹⁷⁴ Two decisions were rendered regarding an insufficient redress in breach of privacy.¹⁷⁵

In 2009, 17 new cases were initiated against Lithuania. As of 31 December 2009, Lithuania had 362 cases pending before the European Court of Human Rights and nine cases adjudicated before it.¹⁷⁶

As already noted, on 1 May 2004, Lithuania joined the European Union.

* Updates to the Lithuanian Report published in the 2010 edition of EPHR have been provided by: Henrikas Mickevičius, Human Rights Monitoring Institute, Lithuania; Mindaugas Kiskis, Mykolas Romeris University, Lithuania; Paulius Galubickas, Sorainen, Lithuania.

¹⁷² *Ciapas v. Lithuania*, ECtHR, Application No. 4902/02, Judgment of 16 November 2006.

¹⁷³ Annual Report 2007, European Court of Human Rights, at 135 and 141, available at http://www.echr.coe.int/NR/ronlyres/59F27500-FD1B-4FC5-8F3F-F289B4A03008/0/Annual_Report_2007.pdf.

¹⁷⁴ Annual Report 2008, European Court of Human Rights, at 128, available at http://www.echr.coe.int/NR/ronlyres/D5B2847D-640D-4A09-A70A-7A1BE66563BB/0/ANNUAL_REPORT_2008.pdf.

¹⁷⁵ *Armoniene v. Lithuania*, Application No. 36919/02; *Biriuk v. Lithuania*, Application No. 23373/03. Annual Report 2008, European Court of Human Rights, *supra* at 96.

¹⁷⁶ Annual Report 2009, European Court of Human Rights, at 140, available at http://www.echr.coe.int/NR/ronlyres/C25277F5-BCAE-4401-BC9B-F58D015E4D54/0/Annual_Report_2009_versionProv.pdf.

GRAND DUCHY OF LUXEMBOURG¹

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Constitution of the Grand Duchy of Luxembourg guarantees a general right to privacy as well as the secrecy of correspondence. Article 11 of the Constitution provides that the State guarantees the protection of one's private life, except if the law provides otherwise. Article 28 states, "(1) The secrecy of correspondence is inviolable. The law determines the agents responsible for the violation of the secrecy of correspondence entrusted to the postal services. (2) The law determines the guarantee to be afforded to the secrecy of telegrams."²

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The processing and use of personal data in Luxembourg is regulated by the Data Protection Act of 2002 and secondary legislation. Specific matters that affect privacy are governed by sectoral regulations.

Luxembourg's first act concerning the use of nominal data in computer processing was adopted in 1979.³ The law regulated individually identifiable automated personal records in both public and private computer files. All databanks including personal data had to be registered, and data subjects had the right to access their personal data and correct it if inaccurate. The law also required licensing of systems used for the processing of personal data. The law has been widely ignored as it was not in line with modern technology and compliance was very low.⁴

It has been replaced by the Act of 2 August 2002 relating to the protection of persons with respect to the processing of personal data (*Loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel*), as amended by the Laws of

¹ The EPHR 2010 "Luxembourg" report has been updated in August 2010 by Olivier Reisch, Linklaters (Brussels, Belgium), and in October 2010 by Jan Dhont and Thomas Daenens, Lorenz (Brussels, Belgium).

² Constitution of the Grand Duchy of Luxembourg, available in French at http://www.legilux.public.lu/leg/textescoordonnes/recueils/constitution_droits_de_lhomme/CONST1.pdf.

³ Act on the Use of Nominal Data in Computer Processing, 31 March 1979; see Charles E.H. Franklin, *Business Guide to Privacy and Data Protection Legislation* 306 (1996).

⁴ Comments to the draft Data Protection Act of 2002, Parliament document n° 4735-00, available in French at http://www.chd.lu/wps/PA_1_084AIVIMRA06I432DO10000000/FTSShowAttachment?mime=application%2fpdf&id=675297&fn=675297.pdf.

31 July 2006, 22 December 2006, and 27 July 2007 (the "Data Protection Act").⁵ The Data Protection Act has implemented⁶ EU Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.⁷ The Act entered into force on 1 December 2002.

The Data Protection Act of 2002 governs the processing and use of personal data. The law⁸ went beyond the framework of the EU Directive by covering not only natural, but also moral, persons. It contains specific provisions on the processing of medical data by health services,⁹ the processing of personal data for surveillance purposes,¹⁰ and in the workplace.¹¹

An amendment to the Data Protection Act was voted in July 2007 and took effect on 1 September 2007. It modified some of the Act's provisions in order to simplify them. The amendment also extended several exceptions relating to certain situations and professions, as well as modified certain terms and definitions, such as the concepts of consent, personal data, and surveillance.¹²

The Data Protection Act applies to "data controllers" ("a natural or legal person, public authority, agency, or any other body which solely or jointly with others determines the purposes and methods of processing personal data") and "data processors" ("any natural or legal person, public authority, administrative body or other entity that processes

⁵ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Data Protection Act of 2002), Mémorial, A-91, 13 August 2002, at 1836-1854, available in French at <http://www.legilux.public.lu/leg/a/archives/2002/0911308/0911308.pdf#page=2>. Available in English at http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf.

⁶ Luxembourg should have amended this law by 1st October 1998. In January 2000, the European Commission initiated a case before the European Court of Justice against Luxembourg and other countries for failure to implement the directive on time. A new bill was eventually drafted and submitted to Parliament in October 2000, and enacted in August 2002.

⁷ OJ L 281, 23 November 1995, at 31–50.

⁸ For more information on the law, see the exhaustive analysis made by Steve Jacoby & Catherine Dauger de Caulaincourt, AGEFI Luxembourg, December 2002 and February 2003; see also Dossier de presse quant à la présentation de la Commission nationale pour la protection des données http://www.gouvernement.lu/salle_presse/actualite/2002/12/12biltgen/dossierpresse.pdf (in French).

⁹ Data Protection Act of 2002, *supra* at Article 7.

¹⁰ *Id.* at Article 10.

¹¹ *Id.* at Article 11; on the particular issue of the processing of personal data by employers in the workplace, see Guy Castagnero, L'actualité du droit du travail: la protection des données personnelles des travailleurs, AGEFI Luxembourg, April 2003, available at <http://www.agefi.lu/mensuel/Article.asp?NumArticle=5364>.

¹² Eleventh Annual Report of the Article 29 Working Party on Data Protection, at 70, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf.

personal data on behalf of the controller" excluding any of the data controller's employees).¹³

In December 2004, a Grand-Ducal Decree¹⁴ established the conditions pursuant to which some data controllers have the option of designating a data protection officer (DPO): an independent person in charge of data processing and compliance with the data protection law. In doing this, they could avoid having to comply with the notification requirements to the Data Protection Commission (*Commission nationale pour la protection des données*, or CNPD). The CNPD is notified of the appointment of the DPO, who should refer to it any problems that he may encounter in the performance of his duties.

The Data Protection Act follows the framework of EU Directive 95/46/EC,¹⁵ including its provisions related to security requirements.¹⁶ To assist data controllers in determining the required levels of security, the CNPD has issued standard measures for the security of personal data processing.¹⁷

Sector-based laws

Luxembourg has a sectoral law and a regulation on privacy relating to telecommunications.¹⁸ In April 2004, however, the European Commission threatened legal action against the country and seven other countries for failing to implement on

¹³ For instance, in cases where a company has outsourced a particular function to a third party, such as payroll, this third party is likely to qualify as a data processor.

¹⁴ Règlement grand-ducal relatif à la désignation des chargés de la protection des données. Mémorial A-200, 20 December 2004.

¹⁵ The Data Protection Act applies to data controllers in respect of any processing of personal data if either: the data controller has a permanent establishment in Luxembourg and the personal data are processed in the context of that establishment; or the data controller is established neither in Luxembourg nor in any other EU member state, but uses equipment in Luxembourg for processing the data otherwise than just in transit. In such case, it must nominate a representative in Luxembourg. The Data Protection Act applies to the automated processing of personal data – whether fully or partially automated – and the non-automated processing of personal data entered in a file or intended to be entered in a file. A "file" is defined as "any structured set of personal data that are accessible according to specific criteria, whether centralized or dispersed on a functional or geographical basis." An unstructured manual file in which the data is not interrelated and that is not accessible in a systematic way is therefore not covered by the Act.

¹⁶ Data controllers need to ensure that appropriate technical and organisational security measures are taken to protect personal data against accidental or unauthorised destruction, loss, or disclosure, as well as against alteration, access, and any other unlawful processing. These measures should ensure an appropriate level of security, taking into account the state of the art in this field and the cost of implementing such measures on the one hand, and the nature of the data to be protected and the potential risks on the other hand.

¹⁷ Commission nationale pour la protection des données, "Mesures de sécurité à mettre en oeuvre", available in French at <http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/securite-informatique/mesures-requises/index.html>.

¹⁸ Law of March 21, 1997 on Telecommunications (Loi du 21 mars 1997 sur les télécommunications), available at <http://www.ilr.etat.lu/tele/legal/loi-t.htm>; Grand Duchy Ruling of 22 December 1997 (Règlement grand-ducal du 22 décembre 1997, modifié le 18 avril 2001, fixant les conditions du cahier des charges pour l'établissement et l'exploitation de réseaux fixes de telecommunications), available at <http://www.legilux.public.lu/leg/a/archives/2001/0540305/0540305.pdf#page=2>.

time the EU Directive on Privacy and Electronic Communications (2002/58/EC).¹⁹ In May 2005, a new law²⁰ (the "2005 law") eventually implemented the provisions of the EU Directive.²¹

The 2005 law states that any service provider must retain traffic and location data for a period of 12 months for the purposes of prevention, investigation, detection, and prosecution of criminal offences. The 2005 law adopted an "opt-in" system for unsolicited electronic communications, and the use of automated calling systems. It also prohibited the use of fax machines or email for the purposes of direct marketing without obtaining the subscriber's prior consent, unless the service provider can make use of the specific exceptions mentioned in the EU directive. Furthermore, the law provides for criminal sanctions (imprisonment and fines) for breach of the provisions related to spam and unsolicited communications, and a court may ban any illegal processing, together with a penalty payment. Following a recommendation of the CNPD, a new law, introduced on 27 July 2007, reduced the retention period of data traffic from 12 months to six months.²² The 27 July 2007 law clarified some of the provisions of the 2005 law in order to provide a more accurate interpretation of provisions of Directive 2002/58/EC. The CNPD was consulted during the drafting of the bill.

DATA PROTECTION AUTHORITY

The Data Protection Act of 2002 created a new data protection authority, the *Commission nationale pour la protection des données* (CNPD).²³ Created on 12 December 2002,²⁴ the CNPD is an independent agency whose task is to regulate the processing of personal data in Luxembourg and ensure compliance with data protection regulations.²⁵ The Data

¹⁹ Associated Press, "EU Issues Order on Internet Privacy," *Toronto Star*, 2 April 2004, at E05.

²⁰ Law "Privacy in Electronic Communications" of 30 May 2005 (Loi du 30 mai 2005 (1) relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et (2) portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle), Mémorial, A-073, 7 June 2005, at 1168-1173, available at <http://www.legilux.public.lu/leg/a/archives/2005/0730706/0730706.pdf#page=2>. Law of 30 May 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector; and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure (Loi du 30 mai 2005 (1) relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et (2) portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle), Mémorial, A-073, 7 June 2005, at 1168-1173, available in French at <http://www.legilux.public.lu/leg/a/archives/2005/0730706/0730706.pdf>.

²¹ OJ L 201, 31 July 2002, at 37-47.

²² *Supra*.

²³ Commission Nationale pour la Protection des Données, homepage <http://www.cnpd.lu/>.

²⁴ See Le Gouvernement du Grand-Duché de Luxembourg, Actualité gouvernementale: Présentation de la Commission Nationale pour la Protection des Données, available at http://www.gouvernement.lu/salle_presse/actualite/2002/12/12biltgen/index.html.

²⁵ See Article 32, Data Protection Act, for the details of its competences.

Protection Act has provided for a public data processing register online, which makes it possible to check if an authority, company, association, professional, or self-employed worker is likely to hold information about an individual and if it has declared such processing to the CNPD.

The CNPD has three permanent members and three substitute members, and is assisted by a team of IT and legal specialists.

The main tasks of the Data Protection Commission include:

- the control and verification of the legitimacy and lawfulness of data controllers' collection and use of personal data;
- to ensure implementation of the provisions of the Data Protection Act and its executive regulations;
- to ensure the respect of the freedom and fundamental rights of individuals, and to inform them about their rights; to receive and verify complaints from the public;
- to keep a register of processing operations;
- to render opinions on legislation relating to the processing of personal data;
- to approve codes of conduct submitted by professional associations which represent the controllers;
- to promote the dissemination of information relating to data subjects' rights and controllers' obligations, particularly as regards the transfer of data to third countries;
- to engage in legal proceedings and notify legal authorities of any offences of which it is aware;
- to cooperate with other data protection authorities set up in other member states of the European Union, notably by exchanging information; and
- to represent Luxembourg at the meetings of the Article 29 Working Party on Data Protection.

The CNPD also has extensive control powers and may request access to the personal data processed by data controllers. It may also do *in situ* verifications at a data controller's premises. It also investigates complaints and usually attempts to mediate between the parties involved. If no amicable settlement is reached, the CNPD provides an opinion on the merits of the complaint with recommendations to the data controller. In case the latter refuses to comply, or whenever any dispute occurs that relates to the application of the Data Protection Act and its implementing measures, the CNPD may forward the case to criminal prosecution authorities or submit it directly to the Criminal Section of the Court of First Instance.

The CNPD can, either at its own initiative or upon request, initiate an investigation to verify whether the processing of personal data is in accordance with the law. In the course of such investigation, the data controller is obliged to provide all necessary information

and cooperation. Furthermore, the CNPD is obliged, in principle, to notify criminal prosecution authorities of any criminal offence of which it becomes aware.

Violation of the Data Protection Law is criminally sanctioned with fines between €251 and €125,000) or imprisonment, or both, which can only be imposed by a court. Affected parties may also claim damages for infringement. Moreover, the CNPD may order (i) the seizure of the personal data systems to which the offence relates, such as manual filing systems, magnetic discs, or tapes, except for the computers or any other equipment; (ii) the erasure and destruction of personal data; or (iii) a prohibition to process personal data, directly or through an agent, for a period of up to two years. In addition, a court may order (i) the temporary closure of the business of the data controller or processor if its sole activity is to process data, for a period of up to two years; and (ii) the discontinuance of processing that is contrary to the provisions of the Data Protection Act and the temporary suspension of the activity of the controller or processor, for a period of up to two years.

The Data Protection Act of 2002 also created a specific regulatory authority for any data processing carried out by police forces, customs, the military, and the intelligence agency. The authority is composed of the state prosecutor and two members of the CNPD, and has the authority to access and verify, including by *in situ* controls, any personal data contained in the databases of the above public entities. Whenever an individual requests access to the personal data held in those databases, he has to address it to that regulatory authority, as there is no direct access right to those public entities.

The CNPD pursued an information and awareness-raising campaign, partaking in Data Protection Day in 2007 and 2008, as well as promoting awareness through its website and interviews with Luxembourg's media.²⁶

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The first conviction under the 2002 laws occurred in October 2007. A journalist divulged a list of persons who were members of the freemasons in France. The CNPD filed a complaint with the public prosecutor alleging a breach of the 2002 laws. The District Court found that an infringement had occurred as it constituted a communication of special categories of data to third parties without any legitimate condition warranting such a disclosure.

The Court of Appeals ruled in July 2007 that evidence obtained in violation of the Data Protection Act would be inadmissible. The Supreme Court however rescinded this decision, ruling that the judge has the right to determine the admissibility of such unlawfully obtained evidence.

In February 2008, the Court of Appeals ruled that the production of proof obtained illicitly, without the CNPD's prior authorisation, and proceedings that were not in

²⁶ *Supra*.

accordance with the governing provisions relating to criminal prosecution and judicial investigation, amounted to a violation of the right to a fair trial.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Articles 88-1 and 88-2 of the Criminal Investigation Code regulate telephone tapping.²⁷ Judicial wiretaps are authorised if it can be shown that: (i) a serious crime or infringement, punishable by two or more years imprisonment, is involved; (ii) there is sufficient evidence to suspect that the subject of the interception order committed or participated in the crime; or received or transmitted information to, from, or concerning the accused; and (iii) ordinary investigative techniques would be inadequate under the circumstances.

Orders are granted for one-month periods and may be extended repeatedly as long as the cumulative period does not exceed one year. Administrative wiretaps may also be authorised for national security reasons by a special tribunal appointed by the head of government. These interceptions are granted for three months at a time and must stop once the requested information is received. In case of emergency, the head of government may authorise such wiretaps without obtaining the CNPD's prior approval, but in such cases, the CNPD will decide whether the wiretap measures may be maintained.

The communications of persons bound by professional secrecy rules cannot be intercepted and any recordings of such must be destroyed immediately. Information gathered during judicial and administrative interceptions, but not subsequently used, must be destroyed. In the case of judicial warrants, persons who were the subject of the warrant will sometimes be informed of the action taken.

This law was highly criticised by human rights activists and the Socialist Workers Party when it was first introduced. The law was challenged on numerous occasions before the European Court of Human Rights. That court, however, ruled that the law violated neither Article 8 (concerning the right to private and family life) nor Article 13 (concerning the right to due process) of the European Convention on Human Rights.²⁸

An authorisation from the CNPD is required before using technical means for monitoring people, particularly by video camera or electronic tracing.²⁹ Even if authorisation for the

²⁷ Articles 88-1 - 88-4 of the Criminal Investigation Code (Code d'instruction criminelle), Law of 26 November 1982, modified by the laws of 7 July 1989 and 30 May 2005.

²⁸ Commission nationale de contrôle des interceptions de sécurité (France), 8e Rapport d'activité 1999, at 66-67, available at <http://www.ladocumentationfrancaise.fr/catalogue/9782110045867/>.

²⁹ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Data Protection Act of 2002), *supra* at Articles 10, 17.

use of video surveillance has been granted, the entity still must register the database concerning the video surveillance. Personal data gathered that way can only be processed under very specific circumstances set forth by law. This includes surveillance on public premises, in public transportation, in shopping malls, and in the workplace. Workplace monitoring may only be undertaken if the staff representative, joint committee, or the Labour and Mine Inspection Office (*Inspection du travail et des mines*) and the person being monitored have previously been informed.

A law dated 5 June 2009 grants police forces direct access to a number of state-held databases, such as the databases of the central population register, the tax registers, drivers' licences, social security records, asylum candidates, visas, and passports, etc.³⁰ Police forces and magistrates may access these databases without the need for a warrant or other prior control. However, each access to them is carefully logged and all logs are kept for three years. The CNPD is in charge of verifying these logs *ex post facto* and has to indicate any results in a yearly report to the State Ministry.

The Act of 22 July 2008 provides specific rules regarding the access by magistrates and judicial police officers to certain public bodies' personal data processing operations.³¹

National security legislation

No update to report under this section.

Data retention

As a general rule personal data which allows for the identification of a data subject, must not be kept longer than necessary for the purpose for which it was collected or will be processed, unless it is kept solely for historical, statistical or scientific purposes.

In March 2006, the European Union enacted the Directive on Data Retention.³² The Directive aims at harmonising the rules on retention of traffic data throughout the EU in order to facilitate judicial cooperation in criminal matters. All traffic data generated in publicly available electronic communications, such as telephony or the Internet, would have to be retained by service providers for law enforcement purposes. The data would have to be kept for a minimum period of six months and a maximum period of two

³⁰ Loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en oeuvre par des personnes morales de droit public. Mémorial A-135, 16 June 2009.

³¹ Loi du 22 juillet 2008 relative à l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel mis en oeuvre par des personnes morales de droit public et portant modification: du Code d'instruction criminelle, de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, et de la loi modifiée du 27 juillet 1997 portant réorganisation de l'administration pénitentiaire, available in French at <http://www.legilux.public.lu/leg/a/archives/2008/0126/a126.pdf>.

³² EU Directive 2006/24/EC (15 March 2006), O. J. L 105, 13 April 2006, at 54-63, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT>.

years.³³ Member states had until 15 September 2007 to transpose the requirements of the Directive into national laws; however, a delay of 18 additional months, until March of 2009, was available for retention of communications and Luxembourg postponed application of this Directive.³⁴ The final implementation only came through a law and a Grand-Ducal Decree, both dated 24 July 2010³⁵ (the "2010 law"), amending the 2005 law. As the 2005 law already had introduced the principle of traffic data retention (for a period of six months), the amendments undertaken were mostly of a technical nature.

The main change of the 2010 law is a clear definition of the crimes that authorise authorities to access traffic data for investigation purposes. Access is possible for any traffic data that may relate to crimes that are punishable with a prison sentence of more than one year. There has been a lot of discussion³⁶ about this condition of access to the data, as many felt that the condition was too broad. The counter-argument was that many of the primary crimes that relate to money laundering are not necessarily punishable by more than a one-year prison sentence, therefore undermining the main rationale for which data retention was justified in the first place. Furthermore, the original text of the 2005 law allowed access to the retained data for the investigation of any crimes.

Another important point of discussion³⁷ during the drafting process of the law was whether service providers subject to the data retention obligations were entitled to sub-contract the data retention function to a third party. While initial drafts permitted such sub-contracting, the final law no longer includes this possibility, further to a formal opposition of the State Council and the CNPD. Both feared that sub-contracting might lead to centralised storage of millions of communications at a single sub-contractor and thus pose a significant threat to citizens' privacy.

National databases for law enforcement and security purposes

No update to report under this section.

National and international data disclosure agreements

No update to report under this section.

³³ *Id.*

³⁴ *Id.*

³⁵ Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle and Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. Mémorial A-122, 29 July 2010, available in French at <http://www.legilux.public.lu/leg/a/archives/2010/0122/a122.pdf>.

³⁶ Comments to the draft law, Parliament document n° 6113-10, available in French at http://www.chd.lu/wps/PA_1_084AIVIMRA06I432DO10000000/FTSShowAttachment?mime=application%2fpdf&id=1048140&fn=1048140.pdf.

³⁷ *Id.*

Cybercrime

No update to report under this section.

Critical infrastructure

No update to report under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

A law on electronic commerce that implements three European Union directives (Directive 1999/93 on Electronic Signatures, Directive 2000/31/EC on Electronic Commerce, and Directive 1997/7 on Distance-Selling) was adopted in August 2000.³⁸ This law contains provisions on the privacy rules certification authorities have to comply with, spamming, and the liability of online service providers. A Grand-Ducal regulation on electronic signatures, electronic payments and the creation of the Electronic Commerce Committee was adopted on 1 June 2001.

On 5 July 2004, the legislator amended the Law on Electronic Commerce to establish the "opt-in" regime for unsolicited commercial communications and add various provisions on consumer protection.³⁹ The same opt-in regime is set forth in Article 11 of the Act of 30 May 2005 on Networks and Electronic Communications Services.⁴⁰ The Act transposes part of the EU "telecommunications regulatory package" by establishing new rights for consumers and telecommunications users, and corresponding obligations for network and publicly available electronic communications service providers.

This Act also lays down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector, and amends Articles 88-2 and 88-4 of the Code of Criminal Procedure. As a general rule, sending unsolicited commercial communications to prospects or clients is only allowed with the latter's prior and unambiguous consent. No prior consent is required, however, if the

³⁸ Loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la Directive 99/93 relative à un cadre communautaire pour les signatures électroniques, la Directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la Directive 97/7 concernant la vente à distance des biens et des services autres que les services financiers, Mémorial, 8 September 2000, at 2176, available in French at http://www.eco.public.lu/documentation/legislation/lois/2000/08/14_commerce_electronique/index.html.

³⁹ Law of 5 July 2004 modifying the Law of August 14, 2000 on Electronic Commerce (Loi du 5 juillet 2004, modifiant la loi du 14 août 2000 relative au commerce électronique), Mémorial, A-125, 16 July 2004, at 1848, available in French at <http://www.legilux.public.lu/leg/a/archives/2004/1251607/2004A18481.html>; see, for more details, Sandrine Munoz, "Le Luxembourg modifie sa loi relative au commerce électronique – Analyse," available in French at http://www.droit-technologie.org/1_2.asp?actu_id=1047.

⁴⁰ Law on Networks and Electronic Communications Services (Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques), Mémorial, A-073, 7 June 2005, at 1144-1159, available in French at <http://www.legilux.public.lu/leg/a/archives/2005/0730706/0730706.pdf>.

recipient's electronic contact details (such as email address or mobile phone number) were obtained by the sender in the context of the sale of products or services. The sender may then use these electronic contact details for sending direct marketing communications provided that the message relates to the sender's own similar products or services. In addition, at the moment of obtaining the electronic contact details, the recipient should be offered the opportunity to object (opt-out) to the use of his electronic contact details in a free-of-charge and easy manner. If the recipient does not make use of the initial possibility to opt-out at the time of sale, the recipient should in each subsequent transmitted communication be offered the option to register an objection under the same conditions.

Cybersecurity

There is nothing to report under this section.

Online behavioural marketing and search engine privacy

With respect to behavioural marketing, the Data Protection Commission (CNPd) follows the recommendations of the Article 29 Data Protection Working Party (WP29). In its Opinion 2/2010⁴¹ of 24 June 2010, the WP29 clarified how EU rules apply to online behavioural advertising. Although the scope of the opinion is limited to online profiling, its interpretation (of Article 5(3) in particular) of the amended Directive 2002/58/EC provides useful clarifications and guidance regarding the legal framework applicable to online behavioural advertising and the use of cookies.

Online social networks and virtual communities

In an online notice published on 31 July 2007,⁴² the CNPD adhered to the principles relating to online social networks as set forth in the WP29's Opinion 5/2009 on online social networking⁴³ of 12 June 2005.⁴⁴

⁴¹ Available in English at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf.

⁴² Available in French at <http://www.cnpd.public.lu/fr/actualites/international/2009/07/facebook/index.html>.

⁴³ Available in English at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

⁴⁴ According to the WP29, providers of online social networking services are subject to the following obligations: (a) they should inform users of their identity, and provide comprehensive and clear information about the purposes and different ways in which they intend to process personal data; (b) they should offer privacy-friendly default settings; (c) they should provide information and adequate warning to users about privacy risks when they upload data onto the social network; (d) users should be advised by social networking service providers that pictures or information about other individuals should only be uploaded with the individual's consent; (e) at a minimum, the homepage of the social network should contain a link to a complaint facility, covering data protection issues, for both members and non-members; (f) marketing activity must comply with the rules laid down in the Data Protection and ePrivacy Directives; (g) providers of online social networking services must set maximum periods to retain data on inactive users. Abandoned accounts must be deleted; and (h) with regard to minors, providers should take appropriate action to limit the risks.

Online youth safety

In July 2007, the CNPD adhered to the principles relating to online social networks as they were set forth by the WP29 in a 2005 opinion on online social networking.

(See more details under the "Online social networks and virtual communities" section.)

TERRITORIAL PRIVACY

Video surveillance

An authorisation from the CNPD is required before using video surveillance for monitoring people.⁴⁵ Even if authorisation for its use has been granted, the entity still must register the database concerning the video surveillance. Personal data gathered in this way can only be processed under certain very specific circumstances enumerated by law. This includes surveillance on public premises, in public transportation, in shopping centres, and in the workplace.⁴⁶ Data controllers must also inform the data subjects about such processing by posting signs or sending circulars or letters by registered mail or electronic means.⁴⁷

Workplace monitoring may only be undertaken if the staff representative, joint committee or the *Inspection du travail et des mines* and the person being monitored have previously been informed. Notice of surveillance may be communicated through the CNPD's newly created online system.⁴⁸ The Fair Labour Standards Act also governs workplace monitoring.⁴⁹

⁴⁵ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Data Protection Act of 2002), *supra* at Articles 10, 17.

⁴⁶ Pursuant to the Data Protection Act, data collected through video surveillance may only be processed for supervision purposes: (i) if the data subject has given his consent, or (ii) in surroundings or in any place accessible or inaccessible to the public other than residential premises, particularly indoor car parks, stations, airports and on public transport, provided the place in question due to its nature, position, configuration or frequentation presents a risk that makes the processing necessary for the safety of users and for the prevention of accidents, for the protection of property, if there is a characteristic risk of theft or vandalism, or (iii) in private places where the resident natural or legal person is the controller, or if the processing is necessary to protect the vital interests of the data subject or of another where the data subject is physically or legally incapable of giving his consent.

⁴⁷ The data collected for supervision purposes may be communicated to third parties only: (i) if the data subject has given his or her consent, except where forbidden by law or if data is communicated to the public authorities; or (ii) to the competent legal authorities to record a criminal offence or take legal action in respect of it and to the legal authorities before which a legal right is being exercised or defended (Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Data Protection Act of 2002), *supra* at Article 10).

⁴⁸ Commission Nationale pour la Protection des Données, "Simplification de certaines demandes d'autorisation," 26 June 2007, available at http://www.cnpd.lu/fr/actualites/activite_nationale/2007/06/22_06_2007/index.html.

⁴⁹ Code du Travail, 29 December 2006, available in French at http://www.legilux.public.lu/leg/textescoordonnes/codes/code_travail/Code_du_Travail.pdf.

The Grand-Ducal Decree of 1 August 2007 regulates the use of security cameras by police forces in "security areas". Any data recorded can only be retained for a period of two months.⁵⁰

The Administrative Court and subsequently the Administrative Court of Appeals have confirmed that supermarkets are not allowed to have video surveillance of interview rooms in which suspected shoplifters are questioned, as it constitutes a violation of the 2002 laws. Supermarkets are allowed to have surveillance cameras within the actual shopping mall.⁵¹

The CNPD in 2007 used its powers under the 2002 laws to verify compliance with its refusal to allow video surveillance in certain shops. It discovered that the stores had been compliant.⁵²

Location privacy (GPS, mobile phones, location based services, etc.)

In April 2010, Google announced that it had captured and stored data from users connected to WiFi networks when it collected photos for its Street View service. Google said Street View cars had been collecting WiFi data in several countries around the world, including Luxembourg.⁵³ In September 2010, the CNPD granted Google the permission to pursue its data collection, provided that it adhered to specific criteria, including the blurring out of faces to make it impossible to identify individuals and car number plates.⁵⁴

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

There is nothing to report under this section.

⁵⁰ *Supra.*

⁵¹ *Supra.*

⁵² *Supra.*

⁵³ "Google: We Have Collected Information Sent over the WiFi via StreetView", 19 May 2010, EDRi-gram, No. 8.10, 19 May 2010 <http://www.edri.org/edriagram/number8.10/street-view-wifi-data-google>.

⁵⁴ "You've Been Googled! Street View Approved for Luxembourg", *352LuxMag*, 30 September 2010 <http://www.352luxmag.lu/edito-14275-you-ve-been-googled-street-view-approved-for-luxembourg.html?p=edito&id=12935>.

NATIONAL ID & SMART CARDS

The Act of 30 March 1979 on Numerical Identification of Natural and Legal Persons⁵⁵ provides for the introduction of an identity number, consisting of 11 digits (including digits to represent date of birth and sex, nationality, marital status, and spouse's name) for every resident in the country, and a numbering system for companies. The law contains specifications for use of this number: the identification number and other related information can only be used by the public services that are authorised to have access to the index, and is restricted to an internal use. These specifications are loosely drafted, however, and allow the number to be widely circulated. The data protection authority is said to be monitoring the adoption of this number closely.⁵⁶

In April 2005, the government requested an opinion of the Data Protection Commission on a draft law regulating access by judicial and police authorities to personal data processed by the State administration and public authorities. The Commission advised the government to adopt a more restrictive approach and a better implementation of the rights of concerned citizens.⁵⁷

Luxembourg started issuing RFID-enabled passports in August 2006.⁵⁸ The chip contains the passport holder's name, date of birth, gender, nationality, place of residence, and biometric data consisting of the owner's photograph and fingerprint.⁵⁹ The data is encoded and managed by the Office of the Passports of the Ministry for Foreign Affairs. The data is given an electronic signature, which allows the passport holder to check if any modifications to their data have taken place. In an effort to keep passports up to date, in terms of both technology and changing the basic access code to decrease the risk of deciphering the passport data, passports are valid for five years. The Office of the Passports will remove biometric data from its files one month after the passport is issued.

⁵⁵ Loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales, available at <http://www.legilux.public.lu/leg/a/archives/1979/0460706/0460706.pdf>; Règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales, available in French at <http://www.legilux.public.lu/leg/a/archives/1979/0460706/0460706.pdf?SID=bae197f880b764969bea1d73e51d3c0c#page=8>. Règlement grand-ducal modifié du 21 décembre 1987 fixant les modalités d'application de la loi du 30 mars 1979, available in French at <http://www.legilux.public.lu/leg/a/archives/1987/1092912/1092912.pdf?SID=04ffd4a6c80ed2f62918d2c3f3d7d3c9#page=6>.

⁵⁶ The Council of Europe, The introduction and use of personal identification numbers: the data protection issues, 1991, available at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Pins_1991_en.pdf.

⁵⁷ Commission Nationale pour la Protection des Données, Rapport relatif aux années 2004 à 2006, at 1/21.

⁵⁸ Commission Nationale pour La Protection Des Données, "Le passport électronique et biométrique", 6 June 2007 http://www.cnpd.lu/fr/dossiers/passeport_electronique/index.html.

⁵⁹ Mémorial A n° 134 de 2006, "Passeports biométriques et titres de voyages pour étrangers", Règlement grand-ducal du 31 juillet 2006 portant règlement d'exécution de la loi du 14 avril 1934, concernant les passeports biométriques, les titres de voyage pour étrangers, apatrides et réfugiés et l'établissement d'un droit de chancellerie pour légalisations d'actes, 10 August 2006, available in French at <http://www.legilux.public.lu/leg/a/archives/2006/1341008/1341008.pdf>.

RFID tags

There is nothing to report under this section.

BODILY PRIVACY

There is nothing to report under this section.

WORKPLACE PRIVACY

An authorisation from the CNPD is required before using technical means for monitoring people in the workplace, particularly by video camera or electronic tracing.⁶⁰ Personal data gathered in this way can only be processed under certain very specific circumstances enumerated by law. Workplace monitoring may only be undertaken if the staff representative, joint committee, or the *Inspection du travail et des mines* and the person being monitored have previously been informed. Notice of surveillance may be communicated through the CNPD's newly created online system.⁶¹ The Labour Act also governs workplace monitoring.⁶² When the employer intends to use video surveillance in the workplace, he cannot rely on his employees' consent, e.g., obtained through their employment contract, as a sufficient legal basis.

HEALTH & GENETIC PRIVACY

The Data Protection Act contains specific provisions on the processing of health-related data by health services and genetic data.

Health privacy

Without prejudice to the rules relating to the processing of genetic data, the Data Protection Act allows the processing of health-related data in the following situations:⁶³

⁶⁰ Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (Data Protection Act of 2002), *supra* at Articles 10, 17.

⁶¹ Commission Nationale pour la Protection des Données, "Simplification de certaines demandes d'autorisation", 26 June 2007, available in French at http://www.cnpd.lu/fr/actualites/activite_nationale/2007/06/22_06_2007/index.html.

⁶² Code du Travail (Labour Code), 29 December 2006, available in French at http://www.legilux.public.lu/leg/textescoordonnes/codes/code_travail/Code_du_Travail.pdf. Article L.261-1 sets forth the conditions for video surveillance in the workplace: video surveillance by the employer, acting as data controller, is only allowed if it is necessary: (i) for employees' security and health; (ii) to protect the company's assets; (iii) to monitor the production process (provided such monitoring only relates to the machinery); (iv) to monitor the number of hours performed by employees, provided such video monitoring is the only measure allowing to determine the exact remuneration; (v) in the context of the organisation of work with flexible working schedules, in accordance with the provisions of the Labour Code. In cases (i), (iv) and (v), the employer must have obtained the prior approval of the Labour Council. The employer should also provide prior information about the installation of surveillance videos to the same Labour Council, or in absence thereof, the employees' representatives, or in absence thereof, to the Labour and Mining Inspection.

⁶³ Article 7, Data protection Act.

- Medical authorities may process personal data on health and sex life that are necessary for the purpose of preventative medicine, medical diagnosis or the provision of care or treatment;
- Medical authorities may also process personal data on health and sex life that are necessary for the purpose of healthcare or scientific research, as well as research bodies or the natural or legal persons whose research project has been approved under the legislation applicable to biomedical research. If the controller is a legal entity, it must appoint a delegated controller, who will be subject to professional secrecy;
- Medical authorities may process personal data on health and sex life where necessary for the management of healthcare services, and also, provided that, as data controllers, they are subject to professional secrecy, social security bodies, and authorities that manage that type of data in performance of their legal and regulatory tasks, insurance companies, pension fund management companies, the *Caisse Médico-Chirurgicale Mutualiste* and those natural or legal persons authorised to do so for socio-medical or therapeutic reasons.⁶⁴

The processing may be sub-contracted, but subject to certain conditions imposed by the Data Protection Act.

Genetic privacy

The Data Protection Act defines genetic data as any data concerning the hereditary characteristics of an individual or group of related individuals.

Genetic data falls into the category of sensitive data, the processing of which is generally prohibited. This type of data may, however, be processed if one of the following conditions is met:

- 1) its processing is required to verify the existence of a genetic link for the purpose of legal proof, for compensation of the data subject, or the prevention or punishment of a specific criminal offence in the cases covered by the Data Protection Act;
- 2) its processing is required to protect the vital interests of the data subject;
- 3) its processing is necessary in the public interest for historical, statistical or scientific reasons;
- 4) if the data subject has given his consent and if the processing is carried out only in the area of healthcare or scientific research, subject to the inalienability of the human body, and except where the law provides that the prohibition cannot be lifted by the data subject's consent;

⁶⁴ Pursuant to the Act of September 8, 1998 governing relations between the State and the bodies working in the areas of social security, family, and therapeutic matters where their activity falls within the areas to be listed in a Luxembourg regulation.

- 5) if the processing of genetic data is necessary for the purpose of preventive medicine, medical diagnosis or the provision of care or treatment. (In this case, the processing of this data may only be carried out by medical authorities); or
- 6) in cases where the law allows the processing of genetic data with the data subject's consent, but for which, for practical reasons, it either proves to be impossible to obtain, or if obtaining such consent would require a disproportionate effort in relation to the objective sought – without prejudice to the data subject's right of opposition. In either case, it is not necessary to get the data subject's prior consent, but it is subject to conditions to be laid down in a Luxembourg regulation.

FINANCIAL PRIVACY

There are also sectoral laws on privacy relating to banking secrecy. Luxembourg's status as a financial haven ensures that unwarranted surveillance of individuals is forbidden. This may change as Luxembourg comes under increasing pressure to amend its financial confidentiality laws to permit greater access to personal financial records by European and American investigators.

In December 2001, the Commission of Surveillance of the Financial Sector (*Commission de Surveillance du Secteur Financier*) released practical and technical guidelines to financial services companies that intend to promote the protection of customers' privacy and the confidentiality of their financial information when launching new online financial services.⁶⁵

E-GOVERNMENT & PRIVACY

There is nothing to report under this section.

OPEN GOVERNMENT

On 8 June 2004, Luxembourg adopted new legislation on the press, repealing the Acts from 1869 and 1979.⁶⁶ Journalists have an obligation to ensure their work does not infringe any individual's presumption of innocence or the entitlement to personal privacy, honour, or reputation.⁶⁷ In addition, a person who has been cited either by name or implicitly, or who has been accused wrongfully to have the inclusion, free of charge, or a reply, or information correcting the false information originally given. However, there is no general freedom of information law in Luxembourg. The new legislation only states

⁶⁵ Commission de Surveillance du Secteur Financier, Services financiers par Internet (Résultats du recensement Internet au 31 décembre 2000 et recommandations portant sur les aspects prudentiels), December 2001, available in French at http://www.droit-technologie.org/redirect.asp?type=legislation&legis_id=95&url=legislations/CSSF_services_financiers_sur_internet_decembre2001.pdf.

⁶⁶ Loi du 8 juin 2004 sur la liberté d'expression dans les medias, available in French at <http://www.legilux.public.lu/leg/a/archives/2004/0850806/0850806.pdf#page=2>.

⁶⁷ *Id.* at Art. 10-20.

that freedom of expression includes the right to receive and seek information.⁶⁸ Under the 1960 Decree on State Archives, the archives are open to the public, but citizens must make a written request explaining why they want access and ministers have broad discretion to deny requests.⁶⁹

OTHER RECENT FACTUAL DEVELOPMENTS

The Court of appeals ruled in July 2007 that evidence obtained in violation of the law of 2002 on data protection would be inadmissible. The Supreme Court however rescinded this decision ruling that the judge has the right to determine the admissibility of such unlawfully obtained evidence.⁷⁰

In February 2008 the Court of appeals ruled that the production of proof obtained illicitly without the CNPD's prior authorisation, and proceedings that were not in accordance with the governing provisions relating to criminal prosecution and judicial investigation amounted to a violation of the right to a fair trial.⁷¹

The Grand-Ducal Decree of 12 June 2007 set out the data that may be recorded on the register of legal persons, which is maintained by the Luxembourg Chamber of Commerce.⁷²

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

There is nothing to report under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Luxembourg is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).⁷³ It signed the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETC No. 181).⁷⁴ It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁷⁵ In January 2003, Luxembourg signed the

⁶⁸ *Id.* at Art. 6.

⁶⁹ Arrêté grand-ducal fixant l'organisation et les conditions de fonctionnement des Archives de l'Etat.

⁷⁰ *Supra.*

⁷¹ *Supra.*

⁷² *Supra.*

⁷³ Signed 28 January 1981; ratified 10 February 1988; entered into force 1 June 1988.

⁷⁴ Signed 24 February 2004; ratified 23 January 2007; entered into force 1 May 2007.

⁷⁵ Signed 11 November 1950; ratified 3 September 1953; entered into force 3 September 1953.

CoE Convention on Cybercrime, but has not ratified it.⁷⁶ It is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

In December 2006, Luxembourg approved the Treaty of Prüm, signed by Austria, Spain, Netherlands, Germany, Belgium, and France, enhancing cross-border police cooperation to combat terrorism, cross border crime, and illegal immigration.⁷⁷ This includes an online exchange of DNA profiles, fingerprints and vehicle register data.

⁷⁶ Signed 28 January 2003.

⁷⁷ Loi du 22 décembre 2006, "1. approbation du Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, ainsi que de la Déclaration commune, signés à Prüm le 27 mai 2005, 2. modification de la loi du 21 décembre 2004 portant approbation du Traité entre le Royaume de Belgique, le Royaume des Pays-Bas et le Grand-Duché de Luxembourg en matière d'intervention policière transfrontalière, signé à Luxembourg, le 8 juin 2004, 3. modification de la loi du 25 août 2006 relative aux empreintes génétiques en matière pénale, 4. modification de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire", available in French at <http://www.legilux.public.lu/leg/a/archives/2006/2342812/2342812.pdf#page=2>.

REPUBLIC OF MACEDONIA

I. PRIVACY AND DATA PROTECTION NORMATIVE AND INSTITUTIONAL FRAMEWORK

I. PRIVACY AND DATA PROTECTION FRAMEWORK

The Constitution of the Republic of Macedonia¹ recognises the rights of privacy, data protection, and secrecy of communications. Article 25 states, "Each citizen is guaranteed the respect and protection of the privacy of his or her personal and family life and of his or her dignity and reputation." No one may interfere in personal and family life except in cases in which the expression and conduct of the person threatens the generally accepted social norms. Article 26 states, "The inviolability of the home is guaranteed. The right to the inviolability of the home may be restricted only by a court decision in cases of the detection or prevention of criminal offences or the protection of people's health." Article 18 states, "The security and confidentiality of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing."

Equally guaranteed is the freedom and confidentiality of correspondence. Article 17 states, "The freedom and confidentiality of correspondence and other forms of communication is guaranteed. Only a court decision may authorise non-application of the principle of the inviolability of the confidentiality of correspondence and other forms of communication, in cases where it is indispensable to a criminal investigation or required in the interests of the defence of the Republic".

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

Several laws regulate the right of privacy in the Republic of Macedonia. The Law on Personal Data Protection (LPDP) was adopted on 25 January 2005.² The LPDP explicitly identifies the exceptions from its application, focusing on the processing of personal data performed by natural persons purely for personal or household activities, processing of personal data in criminal procedure, and protecting the interests of security and the defence of the Republic of Macedonia.³ According to the law, personal data shall be processed fairly and in conformity with the law, and shall be collected for specified, explicit, and legitimate purposes, and shall be processed in a manner consistent with these purposes; they shall be adequate, relevant, and not excessive in respect to the

¹ Published in the Official Gazette of the Republic of Macedonia, Nos. 52/91, 01/92, 31/98, 91/01, 84/03. The Constitution is available in Macedonian at the website of the Constitutional Court at <http://www.ustavensud.mk/>. For the English text see <http://www.ustavensud.mk/domino/WEBSUD.nsf>.

² Official Gazette No. 07/05.

³ LPDP, Article 4.

purposes they are collected or processed for.⁴ The data shall be accurate, complete, and updated as needed. Inaccurate or incomplete data, bearing in mind the purposes for which they were collected or processed, will be erased or rectified. Personal data shall be kept in a form that enables identification of the subject of personal data for no longer than is necessary to fulfil the purposes for which the data were collected or for which they are further processed. Data controllers are responsible for complying with the above-mentioned principles concerning the quality of personal data.⁵

The LPDP states that consent of the data subject is mandatory for processing of personal data.⁶ Personal data can be processed without the consent of the subject if doing so is necessary for performance of a contract to which the data subject is a contracting party, or upon request, prior to entering into a contract; for compliance with a legal obligation laid upon the data controller; for protection of the vital interests of the data subject; for performance of activities of public interest or of official authority vested in the data controller or a third party to whom the data were disclosed.⁷ Furthermore, the law prohibits the processing of special categories of personal data. The LPDP stipulates that processing must be specially designated and protected, while transfer over a telecommunications network is allowed if the data are specially protected by encryption to render them unreadable during transmission.⁸

The rights of the data subject include the right to examine the data collection; the right to submit a request to rectify, erase, or prevent the processing of personal data if the data are incomplete, inaccurate, or out of date, or if their processing does not conform to the provisions of this law; and the right to request that their personal data are not used for advertising purposes.⁹ Furthermore, the LPDP guarantees that no court decision that produces legal effects concerning the performance of a particular person can be based solely on automated data processing whose purpose is to evaluate certain personal aspects relating to that person.

The LPDP also established obligations for data controllers to notify the Directorate for Protection of Personal Data before performing wholly or partly automatic processing operations; to submit information about any newly opened collection of personal data;

⁴ *Id.*, Article 5.

⁵ *Id.*, paragraph 2.

⁶ *Cfr.* Directive 95/46/EC of on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, Official Journal L 281, 23 November 1995, at 31, Article 7.

⁷ LPDP, Article 6.

⁸ *Id.* Article 8.

⁹ *Id.* Article 10.

and any change of data from existing personal data collections.¹⁰ The records from the Central Register kept by the Directorate are publicly accessible and are published in the Official Gazette of the Republic of Macedonia.¹¹ Additionally, the transfer of personal data to other countries may be performed only if those countries provide an adequate level of protection for personal data.

Data controllers may make personal data available on the basis of a written request submitted by the user if the data are needed to perform activities within the user's legally established scope of competence. The LPDP prohibits providing personal data processing that cannot be carried out in accordance with the provisions of this law, and the purpose for requesting such personal data must be in accordance with specific, clear, and lawful purposes for which personal data is collected.¹²

During July 2008, the Parliament also enacted the Law that amended the LPDP,¹³ strengthening the legal framework in the area of personal data protection.

The Law on Amendments and Modification to the Law on Personal Data Protection stipulates that the articles referring to inspection will enter into force after a transitional period that expired on 28 of February 2009. With the implementation of the new inspection provisions, persons authorised to perform the inspection became inspectors for personal data protection, and are authorised to issue decisions in cases where a violation of the Law has been found. In disputed cases, an appeal to the Administrative Court may be applied for. If the inspectors determine there is a violation of the Law of Personal Data Protection, they take legal action to require adherence to the Law of Misdemeanours; if the alignment is rejected, the inspector files a request to initiate a misdemeanour procedure to the Misdemeanour Commissions of the Directorate.

Under Amendment XX to the Constitution of the Republic of Macedonia, the new Misdemeanour Law, and the Law on Amendments and Modification to the Law on Personal Data Protection, the Directorate for Personal Data Protection is granted the status of the misdemeanour adjudicating body. Prior to adopting the amendments and modifications to the LPDP, this function was performed by Macedonian courts. Now it is placed separately in a chapter of the law dedicated solely to the misdemeanours. In order

¹⁰ *Id.*, Article 29, paragraph 1: "Data Controller is obligate to submit a report to the Directorate, containing data which is in accordance to the Article 27 of the law, before performing wholly or partly automatic processing of personal data. Data Controller is obligate to report the Directorate for each change of the data from the existing personal data collections."

¹¹ LPDP, Article 30.

¹² *Id.*, Article 34, paragraph 1 and 3: "(1) Data Controller can make personal data available on the basis of a written request submitted by the user, if the data are needed to perform activities within the legally established scope of competencies of the user. (3) Providing personal data whose processing, i.e. use cannot be carried out in accordance with the provisions of this Law is prohibited."

¹³ "Указ за прогласување на Законот за изменување и дополнување на Законот за заштита на лични податоци" ("Decree for Enacting the Law for Changing and Amending the Law on Personal Data Protection"), Official Gazette of Republic of Macedonia, 19 August 2008.

to carry out this role, the Directorate for Personal Data Protection has already created a Misdemeanour Commission composed of three experienced lawyers, who will conduct and implement the misdemeanour procedure in practice. In general, this new arrangement will increase citizens' confidence in the legal system and, in particular, its ability to protect privacy and personal data.

The Law on Amendments and Modification to LPDP raised the fines for data protection breaches and created three graduated tiers that depend on the gravity of the infringement. For data controllers, fines range from €500 to €900 for ordinary persons; from €700 to €1,200 for persons acting as data controllers within legal entities; and finally from €2,000 to €4,000 for legal entities. For data processors the fine is €600; for persons acting as data processors within legal entities €700 and up; and for legal entities €2,500 and up.

LPDP adopted several bylaws in the form of rulebooks. These cover:

the evidentiary requirements for misdemeanours, the sanctions imposed, and the decisions adopted, as well as the manner of access to the information contained in the evidence files;¹⁴

1. the performance of inspections;¹⁵
2. the form and content of official identity card, as well as their issuance and revocation;¹⁶
3. notification requirements for the Central Register of personal data collections;¹⁷
4. the technical and organisational measures regarding the provision of secrecy and personal data protection.¹⁸

Sector-based laws

The constitutional guarantee to protect personal data is also regulated by the Criminal Code.¹⁹ The punishment for the offence of "Misuse of personal data" is under the Criminal Code consists of a prescribed fine or prison sentence of up to one year for the perpetrator who, contrary to conditions established by law and without the consent of the citizen, collects, processes, or uses his personal data. The same fine is levied against the person who breaks into computerised information systems with the intention of using the data directly or via a third party in order to gain benefit or to cause harm to another person. The criminal offence of "abuse of personal data" is aggravated if it is committed

¹⁴ Official Gazette of the Republic of Macedonia No. 136/08.

¹⁵ Official Gazette of the Republic of Macedonia Nos. 143/08 and 38/09.

¹⁶ Official Gazette of the Republic of Macedonia No. 143/08.

¹⁷ *Id.*

¹⁸ Official Gazette of the Republic of Macedonia No. 38/09.

¹⁹ Criminal Code, Official Gazette of the Republic of Macedonia Nos. 37/96, 80/99, 4/02, 43/03, and 19/04, available in English at <http://www.mlrc.org.mk/law/CriminalCode.htm>.

by officials in the course of duty, and is punishable by a prison sentence of three months to three years. The attempt to commit such a crime is also punishable by law. The 2004 amendments to the Criminal Code make it possible for fine legal persons to for committing the primary form of this crime.²⁰

The Law on Organisation and Operation of State Administrative Bodies²¹ prohibits state administrative bodies from disclosing data related to national security, official and business secrets, and personal data of citizens in accordance with the law that governs the protection of personal data of citizens.

The Law on Voter's List²² protects personal data collected in accordance with the LPDP. Such data may not be used for any purpose other than for exercising citizens' voting rights in accordance with the Law on Voter's List. Any citizen may, within the period defined by this law, file a request for registering, amending, or deleting data in the copies of the electoral rolls provided for public inspection in the event that they or others are not correctly registered. Copies of the voter's list, with data including the ordinal number, surname, name, gender, date of birth, and address, are provided to registered political parties and to independent candidates.²³

The Law on Reporting Dwellings and Residence of Citizens²⁴ stipulates that the Ministry of the Interior must provide protection from unauthorised access and use of the data contained in the records of citizens' dwelling, change of home address, and residence.

The personal data on asylum seekers, recognised refugees, and persons under humanitarian protection, as well as the data on their residence and the rights they enjoy in the Republic of Macedonia are contained in the Central Collection of Data, which is established, processed, and used by the Ministry of the Interior (Asylum Section) in accordance with the provisions of the LPDP. In accordance with the Law on Asylum and Temporary Protection,²⁵ the data from the Central Collection of Data cannot be exchanged with the data subject's country of origin or that of the members of his family.

²⁰ Criminal Code, Article 149: "(1) A person who collects, processes or uses personal data from a citizen without his permission, contrary to the conditions determined by law, shall be punished with a fine, or with imprisonment of up to one year. (2) The punishment from item 1 shall apply to a person who penetrates a computerised information system of personal data, with the intention of using them in order to attain some benefit for himself or for another, or to inflict some harm upon another. (3) If the crime from items 1 and 2 is committed by an official person while performing his duty, he shall be punished with imprisonment of three months to three years. (4) The attempt is punishable. (5) If the crime from item 1 is committed by a legal entity shall be punished with a fine."

²¹ Official Gazette of the Republic of Macedonia, Nos. 58/00 and 44/02.

²² Official Gazette of the Republic of Macedonia Nos. 42/02 and 35/04, available in English at <http://faq.macedonia.org/politics/elections/law.on.voters.lists.html>.

²³ Law on Voter's List, Part III: "Protection of the personal data of the Voter's list," Article 28.

²⁴ Official Gazette of the Republic of Macedonia Nos. 36/92, 12/93 and 43/00.

²⁵ Official Gazette of the Republic of Macedonia No. 49/03.

Every citizen's personal identification number is a unique designation on that person's identification documents. In accordance with the Law on Personal Identification Number,²⁶ the Ministry of the Interior assigns a personal identification number to the citizen according to the place of registration in the Registry of Births kept on the territory of the Republic of Macedonia. The Ministry of the Interior provides for the retention, use, and protection of the data from unauthorised access in accordance with law.

The Law on State Statistics²⁷ regulates the protection of individual data (of natural or legal persons) collected and processed for statistical purposes. The data related to a legal or natural person are collected and processed for statistical purposes, and are confidential data and as such can be used individually for statistical purposes only. An exception allows access to such data for scientific purposes (without information identifying the data subject). Publication or preparation of statistical data must be conducted in a way that prevents the identification of the data subject unless the data subject has agreed to publication. Data providers must be notified of the data protection rules. The measures and techniques for protecting individual data collected and processed for statistical purposes are established in an internal document, a Rulebook on the Measures and Techniques on the Protection of Individual Data Collected for Statistical Purposes (SSO, which has been adopted by the Director of the State Statistical Office. A Commission for Data Protection has been established within the above state administrative body to supervise the protection of data.²⁸

Illegal invasion of the privacy of communications are prohibited and punishable. In accordance with the Law on Electronic Communications, both operators of telecommunication networks and media and the providers of public telecommunication services are obliged to provide inviolate message confidentiality within their technical abilities.²⁹ Furthermore, the law contains provisions requiring protective measures for providing networks and services, communications, caller or connecting line identification, and location information (where it is not traffic information, automatic call diverting, etc. The law provides privacy protection by prohibiting unauthorised wiretapping and data retention, limiting lawful wiretapping, and, in compliance with EU standards, prohibiting unwanted communications including telemarketing and spamming (requiring opt-in for inclusion in mailing lists, and the right to opt out for users of existing mailing lists).³⁰ The Act creates an inspectorate within the Agency for Electronic Communications, stipulates monetary penalties of 4 to 7 percent of annual income for

²⁶ Official Gazette of the Republic of Macedonia No. 36/92.

²⁷ Official Gazette of the Republic of Macedonia No. 54/97.

²⁸ The website of State Statistical Office is available at <http://www.stat.gov.mk/>. According to the LPDP, Commission for Protection of Data is to be elected six months after the law goes into force, 1 August 2005.

²⁹ Official Gazette of the Republic of Macedonia No. 13/05 adopted on 22 February 2005.

³⁰ *Id.*

legal entities and an additional €327 to €410 levied against the individuals responsible.³¹ In April 2007, the Ministry of Transport and Communications initiated amendments to this Law which would increase the penalties for the offenders to €1,500 to €8,000 for individual offenders.³² The changes in the Law on Personal Data Protection also tackle the issues of unwanted direct marketing, with fees of €500 if the offender is an individual citizen, €2,000 for legal entities plus €700 for the responsible executive.³³ The Parliament is presently discussing changes to the Law on Electronic Communications, including "universal deep telco/Internet wiretapping," obliging telecommunications operators to provide direct and uninhibited access to traffic and other kinds of data to the Ministry of the Interior without prior notice or court order.³⁴

Other regulations partially or indirectly regulate the right to privacy. The Law on Single Registry of the Population in the Republic of Macedonia³⁵ provides for the introduction, retention, and contents of the single automated registry of the population in the Republic of Macedonia, specifies the authority charged with keeping the registry, and regulates the protection of the data from the registry as well as the processing, publishing, and use of registry data.

The Law on Personal Identification Records of the Insured and Beneficiaries of Pension and Disability Insurance Rights³⁶ provides for protection of these records. This protection encompasses undertaking measures and activities for protecting the data from: unauthorised access, unauthorised processing, and destruction, loss, modification, abuse, and unauthorised use of the data.

The Law on Keeping Labour Records³⁷ stipulates that the data contained in these records may be used for statistical purposes and for other official needs.

The Law on Social Care³⁸ provides an obligation for the social security institution and its employees to keep professional and official secrets. The law protects data and facts

³¹ Agency for Electronic Communications website is available at <http://www.aec.mk>.

³² Vlado Apostolov, "Имејл рекламите - бизнис или прекршок?" ("Commercials via email – business or offensecrime?"), Špic, 11 June 2007, available at [http://www.dzlp.mk/index.cfm?*%3EK*UY%5CO!Q1%5E\)%%3FP%20%20%0A](http://www.dzlp.mk/index.cfm?*%3EK*UY%5CO!Q1%5E)%%3FP%20%20%0A). See also Filip Stojanovski, "Спамот е забранет во Македонија!" ("Spamming is prohibited in Macedonia!"), Razvigor (blog), 18 May 2007, available at http://razvigormk.blogspot.com/2007/05/blog-post_18.html.

³³ Natali N. Sotirovska, "За несакани спам-пораки казни од 500 до 2,000 евра" ("Fees ranging from 500 to 2,000 Euros for unwanted spam-messages"), Dnevnik, 29 August 2008, available at <http://r.ping.mk/11n8>.

³⁴ See Section "Wiretapping, access to, and interception of communication," *infra* in this report.

³⁵ Official Gazette of the Socialist Republic of Macedonia No. 46/90.

³⁶ Official Gazette of the Republic of Macedonia No. 16/04.

³⁷ Official Gazette of the Republic of Macedonia No. 16/04.

³⁸ Official Gazette of the Republic of Macedonia Nos. 50/97, 16/00, 17/03 and 65/04.

discovered during procedures as well as decision-making concerning the rights of the beneficiaries of social security, of legal family protection, and the competencies established by criminal regulations.

DATA PROTECTION AUTHORITY

The Directorate for Protection of Personal Data (DPDP or the Directorate), as an independent supervisory body, was established in June 2005.³⁹ The LPDP provisions regulate the establishment of the Directorate as an independent and autonomous state body with the rights of a legal entity. The Directorate is managed by a director who is nominated by the Governor of the Republic of Macedonia and appointed by Parliament. The director is appointed for a five-year term, with the right to be re-elected only twice. The director and deputy director are accountable to Parliament. The director and the employees of the Directorate must keep as official secrets the data that they have encountered in their work, both during their terms of office or employment and afterwards. Directorate employees have the status of civil servants. The Directorate's work is fully funded by the Budget of the Republic of Macedonia. The Directorate is a separate beneficiary of the Budget.⁴⁰

From the establishment of the Directorate in June 2005 through the end of 2006, 11 new civil servants were hired, respecting the principle of equal opportunity. In 2007, three new employees were hired (one was transferred) bringing the Directorate to 15 employees and two elected officials. The Directorate was supposed to be fully staffed with 50 employees by 2010; however, currently it has 20 employees and three volunteers.

The Directorate has adopted all the necessary regulations for the implementation of the LPDP within the legally required term of six months. These are: Rulebook on the technical and organisational measures for secrecy and protection of personal data; Rulebook on the manner of record-keeping, and the record form for personal data collections; Rulebook on the form, contents, and manner of administration of the Central Register; Rulebook on personal data processing operations representing a special risk to the rights and freedoms of the data subject; Rulebook on the format, contents, and manner of record-keeping for the transfer of personal data to other States. Data controllers had two years (until 19 December 2007) to implement the LPDP regulations within their own business operations. When the two-year period expired the penal provisions of the LPDP entered into force.

The Directorate assesses the legality of the processing of personal data; publishes the principles of the processing of personal data and ensures that data controllers respect them; investigates and has access to the collections of personal data created by data controllers according to type of subjects and aims; control the operations for processing personal data that data controllers use; collects the data necessary for proper performance

³⁹ See The Directorate's homepage in English at <http://www.dzlp.mk/INDEX.CFM?NTREE=1603&ID=5471&CONT=0>.

⁴⁰ *Id.*

of its tasks; maintains a central register of collections of personal data; maintains records of transfers of personal data to other countries; receives reports or complaints related to the processing of personal data by data controllers; issues prohibitions on further processing of personal data to data controllers; provides opinions on the secondary legislation to data controllers; and performs other tasks established by law. The Directorate also provides expert opinions and interpretations in the area of personal data protection. For example, the Directorate issued recommendations for providers of social network services and users of social network services that are published on the Directorate's website. The most important recommendation for users of social networks is to be careful and think twice before publishing personal data.

Raising public awareness and informing the citizens about the right of personal data protection and privacy remains a key imperative of the work of the Directorate. To this end, the Directorate organises press conferences, interviews, and reports in printed and electronic media, and also holds a number of meetings, workshops, and roundtables for various target groups.

The Directorate followed the Norwegian example to raise public awareness of data protection among young people.⁴¹ The Directorate invited three secondary schools to the promotion of a data protection brochure it had developed in cooperation with the Metamorphosis Foundation.⁴² As part of its promotion activities, scholars participated in debates about how best to protect personal data when using the Internet and in everyday situations.

The Central Register of Data Controllers functions as part of the Directorate's website.⁴³ The controllers, who were required to register their personal data filing systems with the Central Register (by 19 December 2007) will be allowed to do so automatically once a system for electronic identification has been set up.

If violations of the provisions of the LPDP are found in the course of processing of personal data, within 30 days of the date the violations were detected the data controller must: bring its work in line with the provisions of the law and rectify the violations; complete, update, correct, disclose, or maintain the confidentiality of the personal data; adopt additional measures for protecting the data; halt the transfer of personal data to other states; secure the data or their transfer to other entities; and erase the personal data. There is a right of appeal.⁴⁴

According to the Directorate's report, from October 2006 to June 2007 the most frequent violations of personal data, based on citizens' complaints, include: unlawful collection and processing of Personal Identification Number; unauthorised disclosure of personal

⁴¹ "You decide", at <http://www.dubestemmer.no>.

⁴² This project was done in the framework of the CRISP project, see *infra*.

⁴³ Central Register of Data Controllers is available at <http://www.dzlp.mk/cr/>.

⁴⁴ LPDP, Article 47, paragraphs 1 and 2.

data; processing personal data on the Internet without the subject's consent; identity theft; the unlawful revelation of personal data to users and unauthorised transfer of personal data to other countries; and unauthorised recording and publication of photographs on the Internet.⁴⁵

Priority areas for inspection in 2009 included: education, health, social security, telecommunications, property insurance, and local self-government. Inspections were carried out at the premises of state bodies, local self-government, NGOs, health institutions, public enterprises, and other legal persons with different activities. From 1 January to 30 June 2009, the Directorate's section for inspection performed three inspections in the area of electronic communications. Three others in the same area were performed between 1 July and 31 December 2009.

During 2009, citizens demanded investigations into video surveillance, the processing of biometrical data for purposes of employee control, the collection of citizens' Personal Identification Number without legal basis, and the retention of citizens' personal cards while inside the official premises of certain institutions. A further administrative dispute was initiated against two decisions issued by the Directorate; a decision from the Administrative court of the Republic of Macedonia is still awaited.

The Directorate has been continuously providing opinions on personal data matters. The majority of these opinions concern: clarifications of data processing procedures that personal data controllers have to carry out in accordance with different bylaws; draft laws and international agreements; assessments of the conditions required for the transfer of personal data to other countries; questions asked by natural or legal persons, particularly related to data protection on the Internet, at the workplace, and with respect to video surveillance. To enforce data protection provisions and principles as stated in the LPDP, the Directorate also issues reprimands to data controllers and processors.

From 1 January to 30 June 2009 the Directorate provided 16 opinions and one reprimand in the electronic communications area. From July 1 to 31 December 2009, the Directorate provided 34 opinions and four reprimands in the same area, making a total of 52 opinions and five reprimands.

In 2009, the issue which the Directorate focused on the most was the handling of complaints and requests filed by natural persons alleging the violation of their right to personal data protection. The Directorate is legally bound to investigate such cases. The term "complaint" refers to requests submitted for determining a violation of the right to private data protection *ex* Article 18 of the Law on Personal Data Protection. The term "request" refers to all other requests (not-Article 18) submitted by natural persons to the Directorate.

Of the total number of 32 complaints filed from January 1 to 31 December 2009, four were submitted for violations of data protection norms committed on the Internet: two

⁴⁵ Ivana Bilbilovska, "Everybody Collects Personal Data for PR Campaigns," *Vreme*, 21 March 2007, available at <http://www.metamorphosis.org.mk/content/view/871/4/lang,en/>.

concerned the disclosure and "abuse" of personal data on the Internet; two more concerned the "abuse" of personal data for the means of online social networks (like Facebook, Hi5, Twitter etc.). The total number of requests filed by citizens regarding the abuse of personal data on Internet social networks for the past year is 66. In the first semester of 2009, the number of requests by citizens regarding the "abuse" of personal data on social networks was 54. From 1 July to 31 December, citizens made 12 requests.

The most common violations included: identity theft, publishing on YouTube, creating blogs and fan groups using data from other persons, misuse of user names and passwords.

On 7 June 2010, the Foundation Open Society Institute Macedonia (FOSIM) and the Directorate for Personal Data Protection (DPDP) promoted the publications "Comments on the Law on Personal Data Protection" and "Guide for practical implementation of the Rulebook on technical and organisational measures for ensuring secrecy and protection of personal data processing".⁴⁶ The purpose of these publications is to raise the level of personal data protection. The publications are available for download in PDF format from the Directorate's website in Macedonian and English.⁴⁷

MAJOR PRIVACY & DATA PROTECTION CASE LAW

According to representatives of both the regulatory Broadcasting Council of the Republic of Macedonia⁴⁸ and the Association of Journalists in Macedonia,⁴⁹ media laws in Macedonia do not specifically address the protection of privacy. Article 62 of the Law on Broadcasting⁵⁰ includes the right to response and correction but includes no sanctions for revealing personal data.

Article 7 of Code of Journalists of Macedonia,⁵¹ adopted by the Association and enforced by the Council of Honour states: "The journalist shall respect the privacy of every person, except in cases when that is contrary to the public interest." Members of the association are "obliged to respect personal pain and grief," and must obtain consent of a parent or guardian to interview or photograph children or persons "with special needs who are not able to decide rationally."⁵²

⁴⁶ "Promotion of Publications on Personal Data Protection," Monday 7 June 2010, at <http://www.metamorphosis.org.mk/macedonia/promocija-na-publikacii-od-oblasta-na-zashtitata-na-lichnite-podatoci.html>.

⁴⁷ "Macedonia: Two Publications on Privacy Protection Available Online," Friday 09 July 2010, at <http://www.metamorphosis.org.mk/macedonia/privatnost-eknigi-privacy-ebooks.html>.

⁴⁸ Broadcasting Council of the Republic of Macedonia's website, at <http://www.srd.org.mk>.

⁴⁹ Association of Journalists in Macedonia's website, at <http://www.znm.org.mk>.

⁵⁰ Official Gazette of the Republic of Macedonia, Nos. 20/97 and 70/03.

⁵¹ Code of Journalists of Macedonia, available in Macedonian at http://www.znm.org.mk/index.php?option=com_content&view=article&id=47&Itemid=62&lang=mk.

⁵² *Id.*, Article 9.

After 2008, in addition to numerous suits against journalists for slander and libel (often used as political weapon for silencing the media by powerful politicians), there were several court cases with complaints for journalistic breach of privacy during the examined period. However, there is no consistent public record about these developments, and examination of this area requires further in-depth analysis.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

As reported above, Article 17 of the Constitution of the Republic of Macedonia guarantees the freedom and confidentiality of correspondence and other forms of communication.⁵³ In 2003, the article was amended in order to regulate wiretapping and other surveillance authorities. The revised Article 17 allows the violation of the confidentiality of correspondence and other forms of communication only in cases where it is indispensable to prevent or discover a crime, to a criminal investigation, or required in the interests of the defence of the Republic. Search of homes and personal search and seizure are regulated in the Law on Criminal Procedure.⁵⁴ In general, a judge's warrant must be issued prior to such searches.

Even though wiretapping is regulated and unauthorised wiretapping is prohibited, the wiretapping cases initiated in the past have not reached closure in court. The most notable example is the case against the State initiated by 17 journalists who were subject to surveillance in the "Big Ear" affair of 2001.⁵⁵ Over seven years, four different judges unsuccessfully presided over this trial; it was finally resolved at a retrial in June 2007. The State was found guilty, but the 17 plaintiffs remain dissatisfied with their compensation and the whole process.⁵⁶ Their representatives stated that they won't discontinue the trial based on their complaint that is already underway at the European Court of Human Rights in Strasbourg. The Appellate court of Macedonia has upheld the verdict of the lower court, but has lowered the damages from the initial €6,000 to approximately €4,000 per journalist. The journalists have stated that "they are not

⁵³ See *supra*.

⁵⁴ Official Gazette of the Republic of Macedonia No. 15/97 and No. 74/04.

⁵⁵ Natali N. Sotirovska, "Ново судење за 'Големото уво'", ("New Trial on the 'Big Ear' Affair"), Dnevnik, 31 May 2007, available at <http://r.ping.mk/11n6>.

⁵⁶ Each of the 17 wiretapped journalists received EUR 6,000 in damages, see "Прва пресуда за 'Големото уво', новинарите го добија процесот за прислушувањето" ("First 'Big Ear' Sentence, Journalists Win Wiretapping Trial") Utrinski vesnik, 16 June 2007, available at <http://r.ping.mk/11n7>.

satisfied with the compensation, and the precedent sends a signal that the violation of human rights is cheap in Macedonia."⁵⁷

In 2006, Members of Parliament accused the Government of conducting surveillance on over 1,400 individuals.⁵⁸ The executive and judiciary branches of the government have so far failed to provide adequate responses to statements by MPs dealing with wiretapping, while the major political parties refused to include this issue on the agenda of the relevant Parliamentary committee, blocking the official collection of evidence through testimonies.⁵⁹

The Criminal Procedure Code (CPC) established the "special investigation measures".⁶⁰ These measures ensure the gathering of evidence required for a successful criminal prosecution. These measures are applied only when the evidence cannot be obtained in any other way or the evidence gathering is related to serious crimes for which the prescribed punishment is at least four years' imprisonment or crimes for which the prescribed punishment is imprisonment up to five years where there are reasonable grounds to suspect that they have been committed by an organised crime group, gang, or other criminal association.⁶¹

⁵⁷ "Апелациониот суд потврди: Новинарите од Големото Уво биле прислушкувани" ("Appealate Court Confirms: The Big Ear Journalists Were Wiretapped") Večer, 2 September 2008, available at <http://www.vecer.com.mk/?ItemID=C50F895AE5A071478301A8CF24F47A51>.

⁵⁸ Jasminka Dogova, "1400 лица прислушкувани?!" ("1,400 Persons Wiretapped?!"), Špic, 28 April 2006, available at <http://www.spic.com.mk/DesktopDefault.aspx?tabindex=1&tabid=1&EditionID=261&ArticleID=11821>.

⁵⁹ Statement of MP Tito Petovski given at the public debate on privacy in Macedonia, 4 June 2010. More information about this event are available at <http://www.metamorphosis.org.mk/macedonia/odzrana-trkalezna-masa-na-tema-qprivatnosta-vo-makedonijaq.html>.

⁶⁰ Criminal Procedure Code, Official Gazette of the Republic of Macedonia No. 15/2005. According to Article 146 of the CPC, "special investigation measures" are: "1) Communication interception and entry into the home and other premises or transportation vehicles for purposes of creating conditions for communication interception under conditions and in a procedure established by law; 2) Inspection of and search of a computer system, seizure of a computer system of parts thereof or the electronic database; 3) Secret surveillance, following, and visual-sound recording of persons and items using technical devices; 4) Simulated purchase of items and simulated giving bribe and simulated acceptance of a bribe; 5) Controlled delivery and transportation of persons and items; 6) Use of undercover agents for surveillance and gathering information or data; 7) Opening a simulated bank account into which criminal proceeds are to be deposited; and 8) Registering simulated legal entities or use of existing legal entities for purposes of gathering information".

⁶¹ Criminal Procedure Code, *supra*, Article 8: "Communication interception in respect of a person may be ordered in cases in which there are reasonable grounds to suspect that the person has committed a crime for which at least four year prison sentence has been prescribed or a crime for which a prison sentence of up to five years has been prescribed and in respect of which there are grounds to suspect that it has been perpetrated by an organised group, gang or other criminal association, for the purpose of ensuring information and evidence required for the successful criminal prosecution which cannot be otherwise gathered."

The order for the application of special investigation measures may be issued by the Public Prosecutor's Office, or by the Investigative Judge in the preliminary investigative procedure, or by only an Investigative Judge in the course of an investigative procedure.⁶²

According to Article 149, paragraph 2 of the CPC, the order should include: the name of the person against whom special investigation techniques will be applied (when the alleged perpetrator is known); the grounds to suspect that the crime has been committed; facts justifying the application of the special investigation techniques; as well as a determination of the mode, scope and duration of application of the techniques. The CPC established that the evidence gathered with use of special investigation measures is admissible only if the measures have been used and applied following the procedure set forth by law.

The application of the special investigation measures of communication interception is furthermore regulated with the Law on Communication Interception (LCI), which is the *lex specialis* in respect of the CPC and the application of these measures.⁶³ The application of the investigation measures envisaged in the LCI requires secondary legislation that would further elaborate the application of such measures.⁶⁴

The LCI also envisages the establishment of a Parliamentary Committee to supervise the application of communication interception techniques by the Ministry of the Interior and the Ministry of Defence. This Committee has been established *de facto* at the Parliament of the Republic of Macedonia, but it has yet to issue a report.

In May 2010 the Ministry of Transport and Communications proposed to the Parliament changes to the Law on Electronic Communications, including "universal deep telco/ Internet wiretapping,"⁶⁵ obliging telecommunications operators to provide direct and uninhibited access to traffic and other kinds of data to the Ministry of the Interior without prior notice or court order.

Protest by the civil society and legal experts about the unconstitutional nature of these proposed amendments were ignored by the government and the Parliament. The DPDP – whose director was ousted by the end of May 2010 – first submitted a negative opinion to Parliament,⁶⁶ and then withdrew it from the parliamentary procedure. Even though

⁶² *Id.*

⁶³ Official Gazette of the Republic of Macedonia No. 121/2006.

⁶⁴ Article 42 of the LCI. The deadline envisaged in the LCI expired on 22 February 2007.

⁶⁵ Cory Doctorow, "Macedonia Introduces Universal, Deep Telco/Internet Wiretapping; Hardly any MPs Bother to Vote," BoingBoing, 16 June 2010, available at <http://www.boingboing.net/2010/06/16/macedonia-introduces.html>.

⁶⁶ Мислење на ДЗЛП за Законот за електронски комуникации (Opinion of the DPDP on the Law on Electronic Communications), DPDP, 7 June 2010, available at <http://metamorphosis.mk/publications/informatichko-opshtestvo/mislenje-na-dzlp-za-zakonot-za-elektronski-komunikacii/details.html>.

leading opposition MPs spoke against this law,⁶⁷ very few opposition deputies turned out at the critical voting session to cast their votes against it.⁶⁸

National security legislation

Law enforcement officers, in accordance with the Code of Police Ethics,⁶⁹ are obliged to adhere to the citizens' right to privacy in accordance with the Constitution and the laws of the Republic of Macedonia. The collection, retention, and use of personal data by the police is performed in accordance with the law and the ratified international agreements for protecting personal data, restrictively and only to the extent necessary for carrying out legal duties.

The Law on Classified Information⁷⁰ establishes the measures and activities for protecting classified information. The measures and activities for security of individuals, such as issuing a security certificate, are significant. The satisfaction of the conditions for issuing a security certificate is established through a security audit carried out upon prior written consent of the person to whom a security certificate is to be issued. The data from the completed security questionnaire are used for the purposes of the audit. The law incorporates the NATO and EU standards on classified information.⁷¹

Data retention

The amendments to the Law on Electronic Communications proposed in May 2010 stipulate a period of 24 months for retention of traffic data by the telecommunication operators, including ISPs.

National databases for law enforcement and security purposes

The Law on National Criminal-Counterintelligence Data Base was adopted by the Parliament of the Republic of Macedonia on 28 September 2009.⁷² The Law was proposed by the Ministry of Interior, on behalf of the Government of the Republic of Macedonia, in order to establish a central and integral information system for processing and exchanging data among the institutions with expertise in combating organised crime. In addition, the Law should harmonise domestic legislation with EU *acquis* and

⁶⁷ "Macedonia: New Law on Electronic Communications Proposed," Metamorphosis Foundation, 14 May 2010, available at <http://metamorphosis.mk/macedonia/makedonija-usvoen-noviot-zakon-za-elektronski-komunikacii.html>.

⁶⁸ "Macedonia: Assembly passed legislative amendments against privacy," Metamorphosis Foundation, 17 June 2010, available at <http://metamorphosis.mk/macedonia/2010-06-17-12-03-20.html>.

⁶⁹ Official Gazette of the Republic of Macedonia No. 03/04.

⁷⁰ Official Gazette of the Republic of Macedonia No. 9/04.

⁷¹ "Macedonian Parliament resumes 53rd session," 10 February 2005, MT.net News.

⁷² Official Gazette of the Republic of Macedonia No. 120/09.

especially with the EU Council's decision establishing the European Police Office (EUROPOL).⁷³

Both the governing and the opposition parties considered the law necessary to overcome the lack of lawful procedures for exchanging data held by the relevant institutions. However, many aspects of the Draft Law were seriously criticised by the opposition and by the civil society organisations participating in the open session of the Parliamentary Standing Inquiry Committee for the Protection of Civil Freedoms and Rights.⁷⁴

The provisions regulating the contents of the database⁷⁵ were subject to many discussions and amendments during the debate in the Parliament. In addition, the provisions concerning the establishment of the Commission, whose task is to provide for efficient cooperation among the relevant institutions sharing the data, were also largely criticised in particular because, critics said, the Commission was not given the status of an independent body.⁷⁶ Critics pointed out that the provision on the adoption of bylaws regulating access to the database and processing of stored data is an insufficient solution that also undermines the principle of the separation of powers.

In accordance with the Law on National Criminal-Counterintelligence Data Base, the aforementioned bylaws are expected to be adopted in mid October 2010.

National and international data disclosure agreements

No specific information has been provided under this heading.

Cybercrime

Computer crimes are regulated by Article 251 of the Criminal Code.⁷⁷ This article was added to the Criminal Code in 1996 and it is included in Chapter 23, Criminal Acts against Property of the Republic of Macedonia.

Law enforcement professionals base their actions on the provisions of the LPDP and must obtain a court order (a warrant) in order to obtain information from private companies such as Internet providers (ISPs) or cybercafés. None of the five major ISPs displays a

⁷³ Council Decision establishing the European Police Office (Europol), 6 April 2009, Official Journal L 121, 15 May 2009, at 37-66.

⁷⁴ The Committee held a public session at the first reading stage of the Draft Law on 1 September 2009.

⁷⁵ In addition to the provisions stating that the database should contain the data of individuals suspected to have committed or have attempted to commit a criminal act, the Law also includes a vague provision that extends its scope to "certain persons, criminal-law events or criminal occurrences organised in criminal dossiers" (literal translation). Furthermore, the Law also extends over any person who may in the future appear as a witness not just in a criminal, but also in any judicial procedure.

⁷⁶ The Commission is made up of members from the Ministry of Interior; the Customs Directorate, the Financial Police Directorate; the Directorate for Public Revenues; the Directorate for the Protection of the Personal Data and the Directorate for the Security of Classified Information. The Commission's administrative-technical functions will be carried out by the Ministry of Interior.

⁷⁷ Criminal Code, *supra*.

public copy of their privacy policy, and their Internet access and Web hosting contracts do not include information about either privacy or the rights of users under to the LPDP, nor do they outline the internal procedures and responsibilities for dealing with sensitive information.

Cybercafés operate under the Law for Entertainment. Games, and Games of Chance,⁷⁸ and are not required to implement additional standards in regard to the protection of their users' privacy. The only provision in that law related to privacy is the obligation of confidentiality in regard to winning or losing.⁷⁹ As a result, customers use the cybercafés at their own risk, and the number of cases of publishing excerpts of private conversations (IMs, IRC) suggests that many cafés retain activity logs and monitor the traffic in their establishments without making that clear to their customers. Users are also threatened by other users, who use low security in the cafés to install spyware and harvest data.

Critical infrastructure

The amended Law on Electronic Communications enables wiretapping of telecommunication networks by the police. Where critical infrastructure is concerned, government representatives have frequently used excuses related to confronting security risks through surveillance to silence the few dissenting voices that occasionally take a public stand for civil liberties.

INTERNET & CONSUMER PRIVACY

Low public awareness on privacy issues remains the major obstacle to the development of the information society in general and e-commerce in particular. This refers to public awareness of both basic data protection principles and rights and the procedures to enforce these rights. The lack of awareness about the complementary right of free access to information hampers increasing the (much-needed) transparency and accountability of public institutions.

According to research conducted by Metamorphosis in 2009 and 2010 and published in the report "Privacy in Macedonia 2010", the majority of Macedonian websites lack privacy policies. Metamorphosis's research included automatically and manually processing large samples of URLs, including more than 13,000 domains from MARNet's register (all second and third-level MK domains), and over 2,000 links from the Macedonia Search Directory.⁸⁰

The research, which consisted of two waves of surveys in March 2009 and February 2010, proceeded in two phases. First, automatic crawling determined whether domains

⁷⁸ Draft Law for Modification and Amendment to the Law on Games of Chance and Entertainment Games, Official Gazette of the Republic of Macedonia No. 10/97 and 54/97.

⁷⁹ Law on Games of Chance and Entertainment Games, Article 82.

⁸⁰ "Privacy in Macedonia 2009," a report by Metamorphosis Foundation, published in June 2010, available at <http://www.metamorphosis.org.mk/publications/informatichko-opshtestvo/macedonia-online-privacy-in-2009-report-draft/details.html>.

led to an active website and whether selected keywords appeared on its front page. Second, the sites containing these keywords, which were supposed to be part of a link to a privacy policy, were checked manually. Out of these two samples, only a few dozen Macedonian websites were found to have privacy policies.

This research also found that no websites that use second- and third-level *.gov.mk* domains have privacy policies. A significant portion of new e-commerce websites also lack this basic feature, although there has been some improvement over time.

E-commerce

By 2000, Macedonia had acquired a bad reputation, as most of the transactions initiated from its territory on e-commerce websites proved fraudulent. The absolute number of such transactions was not significant, but the fact that a high percentage involved some sort of abuse – resulting from sharing stolen credit card numbers among IRC users from other Balkan countries, – resulted in the country's IP addresses' being blacklisted over the next decade.

Blacklisting meant that Macedonian Internet users could not use services provided by foreign e-shops, who declined transactions and delivery. In addition, e-commerce was not developed for domestic use, as financial institutions reluctantly kept postponing investing in e-banking and e-commerce, while the Government kept failing to complete the legal framework.

Through various projects, USAID invested in improving overall business conditions, including hiring consultants from VeriSign in 2006 to help in regard to improving the situation with cybersecurity and remove Macedonia from blacklists by providing factual data on levels of use (increasing use of Internet and credit cards) and abuse (lowered percentage due to increased overall number and enforcement). Local actors, such as the Metamorphosis Foundation and some private sector companies promoted the concept of information security through awareness-raising and educational campaigns,⁸¹ and by offering services to assist in the implementation of ISO standards, respectively.

The government assigned a Minister to take charge of Information Society Development; he announced the drafting of a special law on e-commerce that was adopted in November 2007.⁸² In contrast to similar policy efforts in the past – including the landmark National Strategy for Information Society Development (2004-2005) and the National Strategy for Electronic Communications and IT Development (January-April, 2007) – the task force working on this law failed to include civil society representatives. This law, based on the EU's e-Commerce Directive, does not include additional stipulations on personal data protection, since they are covered by other laws.

⁸¹ "Information Security Initiative Project," Metamorphosis Foundation. Deliverables such as guides and other materials are available at <http://www.metamorphosis.org.mk/programs/e-governance-information-security-initiative.html>.

⁸² Official Gazette of the Republic of Macedonia No 133.

The opening of the domestic payment processor *Casys* in 2008 was one of the most important developments of that year. By September 2009, at least 16 e-shops offered transactions via Visa or MasterCard using three banks as intermediaries.⁸³ However, by the end of that year e-commerce in Macedonia was still not popular: at most a few thousand people performed no more than a few thousand transactions of relatively small size.

Many of these new e-shops (56 percent) adopted privacy policies in strict consultation with the DPDP.. However, a research carried out by the NGO Metamorphosis showed that while the number of local e-shops rose to 29 by the beginning of 2010, a surprisingly large percentage of them (38 percent) do not feature privacy policies, even though the overall situation is improving. Metamorphosis' team surveyed them all based on the links offered by the banks that act as intermediaries for e-commerce accounts (please see Appendix I for details).

In addition, a survey by New Moment in early 2010 established that e-commerce customers from Skopje "do not know if the Macedonian e-shops offer safe purchasing,"⁸⁴ confirming the lack of confidence in online transactions.

Cybersecurity

No specific information has been provided under this heading.

Online behavioural marketing and search engine privacy

The Agency for Electronic Communications is in charge of enforcing the Law on Electronic Communications through an inspectorate, but so far no information has been made public about its efforts to enforce the privacy provisions contained in the law, including those regulating direct marketing by legal entities.

A public panel on privacy in Macedonia held on 26 August 2008, as part of a public consultation to debate the Macedonia Report for Privacy and Human Rights Report 2007, reiterated the assertions from the previous year that no cases have been made public of in which the privacy protection provisions of the Law on Electronic Communications have been enforced. Spamming remains widespread practice in the Macedonian business sector. Moreover, at least one company provides spamming services for other companies.⁸⁵

This situation remained unchanged until June 2010, even though the commercial spamming services have been less prominent since 2009. In general, Macedonian companies continue to use mailing lists compiled without the recipients' explicit

⁸³ Filip Stojanovski, *Impact of Social Media on Internet Marketing in Macedonia* (University Paris 1 Panthéon Sorbonne, 2009). (Graduate thesis for Master of e-Business Management @ IAE de Paris).

⁸⁴ Darko Buldioski, "Резултати: Истражување за Интернет трговија" ("Results: Internet Commerce Research"), *Komunikacii*, 22 April 2010, available at <http://komunikacii.net/04/22/internet-trgovija-2/>.

⁸⁵ "Debate on Privacy in Macedonia," Metamorphosis Foundation, 29 September 2008, available at <http://www.metamorphosis.org.mk/content/view/1250/3/lang,en/>.

permission as one of their primary marketing tools. However, a number of consulting companies and marketing agencies specialising in online promotion have reacted to increased action on the part of the DPDP and digital rights NGOs by adding an opt-out footer in their e-mails.

There's no evidence of advanced user profiling via local search engines; advertising networks and portals mostly serve banner ads and claim that they do not profile their users.

Online social networks and virtual communities

The most significant development on the Macedonia-related Internet in 2009 has been the explosive growth of social media use resulting from the increasing popularity of Facebook. The number of Facebook users from Macedonia, which had already begun rising in 2008, dramatically increased in 2009 from around 83,000 in January to almost 500,000 by the end of December.⁸⁶

One factor influencing this trend was overcoming the language barrier, identified in a 2004 survey by Metamorphosis and FOSIM.⁸⁷ Multilanguage interfaces introduced in August 2008 – including Macedonian and Albanian – effectively opened Facebook to the three-quarters of the Macedonian population lacking a working knowledge of English.

The existing cultural preference for social networking as a form of interpersonal communication and entertainment provided strong potential for a fit with ICT solutions that support these activities. In 2009, even the customarily slow-to-catch-up traditional media begin to provide frequent coverage of Facebook-related developments, which supports the argument that online social media have become an integral element of mainstream culture in Macedonia.

The trend of the increasing online presence of politicians from 2008⁸⁸ continued in 2009. During the March and April elections, presidential and mayoral candidates started using social media such as Facebook and blogs as part of their election campaigns, alongside personal or political party websites.

Research by the NGO Metamorphosis revealed that candidates failed to address all potential voters by using the relevant local languages in their Web presence, did not provide regular updates or respond to e-mail, and in general did not seem to grasp the new technologies. This research also found a surprisingly high correlation between the level of support provided to the presidential candidates on Facebook and the number of

⁸⁶ Info sources used: Komunikacii.net, IT.com.mk, and Facebakers.com.

⁸⁷ "General Data About the Situation Regarding the ICT in Macedonia," Metamorphosis Foundation, 6 February 2004, at <http://www.metamorphosis.org.mk/publications/english-publications/>.

⁸⁸ "Macedonia: Flirting online with the politicians," Metamorphosis Foundation, 29 October 2008, available at <http://www.metamorphosis.org.mk/macedonia/macedonia-flirting-online-with-the-politicians.html>.

actual votes gained in the two election rounds, suggesting that social media could be an effective market research tool on issues that mobilise a critical mass of users.⁸⁹

State institutions were affected by the rise of Facebook's popularity. Some, including Parliament, blocked the use of this service on their office networks.

On the other hand, the Ministry of Interior Affairs (MOI) opened a short-lived "unofficial" personal profile in April causing some journalists to question the motives of invitations to become "friends" with the Ministry, since accepting those invitations would enable the Ministry to view their profiles and activities.⁹⁰ Facebook shut down the MoI profile because it violated the company's terms of service, which allow only individuals to have personal profiles. Legal entities are required to use pages.⁹¹

The still very low level of public awareness of privacy, especially digital privacy, issues has been noted as a major obstacle by the stakeholders.

Online youth safety

The Metamorphosis Foundation launched the "Children's Rights on the Internet – Safe and Protected" (CRISP) project in 2007; it ended in December 2008. The project involved the Directorate for Personal Data Protection of the Republic of Macedonia and a network of 11 NGOs working on the promotion and safeguarding of children's rights within their communities. CRISP was co-funded by the European Initiative for Democracy and Human Rights (EIDHR) and Metamorphosis. CRISP's objective is to create educational content intended to teach the skills needed to protect personal data for the Macedonian public education system. CRISP's activities included creating educational content for children, parents, and teachers and designing leaflets and posters in Macedonian and Albanian.⁹²

The project's activities covered 50 primary and 20 secondary schools in 12 cities and seven villages in the Republic of Macedonia, with the participation of 8,482 students, 1,170 teachers, and 1,138 parents. The website received over 10,000 visits during its first year of operation. With support from OSI and FOSIM, Metamorphosis continued its

⁸⁹ Filip Stojanovski, Elena Ignatova & Iirina Sumadjeva, "Користење на новите медиуми од кандидатите за изборите 2009" ("Usage of New Media by the Individual Candidates for the 2009 Election"), Metamorphosis Foundation, June 2009, available at <http://metamorphosis.org.mk/dmdocuments/2009-Izbori-Makedonija-internet.pdf>.

⁹⁰ Citizens can now be Facebook friends with the Ministry of Interior, Metamorphosis Foundation, 6 April 2009, available at <http://www.metamorphosis.org.mk/macedonia/citizens-can-now-be-facebook-friends-with-the-ministry-of-interior.html>.

⁹¹ Filip Stojanovski, "Macedonia: Facebook Removes Ministry of the Interior's Personal Profile," Global Voices Online, 9 April 2009, at <http://globalvoicesonline.org/2009/04/09/macedonia-facebook-removes-ministry-of-the-interiors-personal-profile/>.

⁹² CRISP project's website at <http://www.crisp.org.mk> ; more information in English are included in the Case Study at the ePractice.EU portal available at <http://www.epractice.eu/cases/crisp>.

efforts to raise public awareness of youth-related privacy issues through the Online Privacy Made Easy project in 2009 and 2010.

The Parliament adopted the Declaration for Safer Internet⁹³ drafted by MP Aleksandar Spasenovski and supported by MPs from both majority and opposition parties on 1 March 2010.⁹⁴ The Declaration⁹⁵ incorporates analysis and recommendations against censorship and Internet filtering based on information given by EDRI and provided by the Metamorphosis Foundation in official expert testimony at the public hearing and direct consultations with MPs.

During 2010 there were two other notable initiatives in the area of protection of children and youth. The first concerns the creation of a national hotline dealing with online abuse and crime. This initiative is promoted within the framework of the EU's "Safer Internet" Programme and is run by the NGO Internet Hotline Macedonia with the participation of Metamorphosis and children's rights NGO Megjashi. The second initiative was to found the new NGO, National Internet Watch Forum,⁹⁶ which focuses on cooperation with ISPs and the mobile operators.

TERRITORIAL PRIVACY

Video surveillance

Video surveillance is regulated by the LPDP, which includes provisions regarding notice to the people who are in range of the cameras.

Several ISPs and local TV stations have webcams pointed at busy city streets or squares. Those that have come to the attention of the DPDP, such as T-home, have disabled zooming or other features of their services that would enable personal identification of passers-by.

In August 2010, the media expressed concerns about the growing number of police cameras monitoring highways and busy spots in cities. The Ministry of Interior claimed that these cameras will improve traffic safety and law enforcement.

⁹³ Предлог декларација за побезбеден интернет (донесена) (Draft Declaration for Safer Internet (Adopted), Assembly of the Republic of Macedonia, 1 March 2010, available at <http://www.sobranie.mk/ext/materialdetails.aspx?Id=4d1989be-8a15-42b8-a90c-f62318518891>.

⁹⁴ "Парламентот со Декларација иницира заштита на децата од заканите на Интернет" (Parliament Initiates Protection of Children from Internet Threats via Declaration"), MIA, 1 March 2010, available at <http://r.ping.mk/11n5>.

⁹⁵ "Declaration on Safer Internet Proposed in the Macedonian Parliament," Metamorphosis Foundation, 25 February 2010, available at <http://www.metamorphosis.org.mk/macedonia/vo-sobraniето-na-rm-e-predlozhena-deklaracija-za-pobezbeden-internet.html>.

⁹⁶ National Internet Watch Forum's website at <http://www.nfin.org.mk>.

Location privacy (GPS, mobile phones, location based services, etc.)

Changes in the Law on Electronic Communications adopted in June 2010 included an obligation for service providers (telecommunications operators, ISPs) to enable direct access to their terminal equipment and location data by the Ministry of Interior, and to cover the costs for the necessary surveillance equipment. Since these requirements were adopted there has been no public record of either implementation or impact assessment.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Macedonian identification and travel documents use biometrics according to EU standards. The use of biometrics in these documents has been promoted as a positive feature enabling the liberalisation of the visa regime. Beginning in December 2010 the holders of new Macedonian passports can travel in the Schengen area without applying for a visa, while holders of "old passports" must apply at the appropriate embassies.

The LPDP includes biometric data in the category of special data, whose processing is prohibited (Article 8). Debate on the privacy and surveillance issues inherent in the implementation of biometrics remains absent from Macedonian public discourse.

NATIONAL ID & SMART CARDS

Like passports, Macedonian national ID cards use biometrics (images of face and fingerprints), but are not smart cards containing additional information relevant to transactions.

RFID tags

In Macedonia, RFID tags are used mainly by commercial entities. For example, several bookshops use them in theft-prevention scanners sited at their entrances/exits.

The private company Duna Kompjuteri developed a project for tagging domestic animals with RFID chips in cooperation with the Department for Livestock Production of the Faculty of Agricultural Sciences and Food from Ss. Cyril and Methodius University in Skopje.⁹⁷ Although this effort has no direct impact on individual privacy, it shows a general trend to develop and use this technology.

BODILY PRIVACY

LPDP deals with scanning as part of its regulations on video surveillance. Several institutions use scanners at their entrances for security reasons, including the buildings of the Parliament and the Government. Scanners are also present at airports. No information has been made public about how the images produced by these devices are handled.

⁹⁷ See <http://it.com.mk/najvljateljnite-lichnosti-vo-it-sektorot-vo-makedonija-spored-globus/>.

WORKPLACE PRIVACY

No special regulations govern workplace privacy, which is covered by the Law on Personal Data Protection.

HEALTH & GENETIC PRIVACY

Medical data, including genetic and biometric data, are considered special categories of data whose processing is prohibited by the Article 8 of the LPDP. Paragraph 8 provides an exception for processing these data in case they are "needed for the purposes of medical prevention, diagnosis, treatment, or management of a health service and is carried by a person whose profession is to provide medical protection under an oath of secrecy for the data revealed to her/him during the performance of her/his profession..." or if the data subject provides explicit consent or the processing refers to data made public by the data subject.

Medical records

The Law on Health Care⁹⁸ specifies that health sector workers are obliged to take care of patients, to respect their dignity, to adhere to medical ethics, and to keep professional secrets. The obligation to keep professional secrets applies to any worker who uses medical records or comes across data contained therein as any part of performing their jobs. In accordance with the Law on the Protection of the Population from Contagious Diseases,⁹⁹ the reporting of AIDS, HIV infection, and microbiological findings for *Treponema pallidum*, *Neisseria gonorrhoeae*, congenital infection with Rubella virus, *Toxoplasma gondii*, and *Chlamydia gondii* is anonymous.

A scandal erupted in January 2010 when a TV station republished photos from the Facebook profile of a doctor from the Emergency Ward of the main Clinical Centre in Skopje showing her and other medical staff posing with an unconscious and half-naked patient on a stretcher (presumably intoxicated during the New Year celebrations).¹⁰⁰ Within a few days the doctor was fired because of the damage to the reputation of the medical profession.¹⁰¹ As a continuation of this affair, debates continue about whether the journalists had the right to republish the incriminating photos and in what format, i.e., hiding the identity of some of the photographed persons by blurring.

⁹⁸ Official Gazette of the Republic of Macedonia Nos. 38/91, 46/93, 55/95, 17/97 – consolidated text and 10/04.

⁹⁹ Official Gazette of the Republic of Macedonia No. 66/04.

¹⁰⁰ Menche Atanasova Tonchi, "Скандал на хируршките клиники" ("Scandal in Surgery Clinics"), A1 TV, 4 January 2010, available at <http://a1.com.mk/vesti/default.aspx?VestID=118274>.

¹⁰¹ "Лекарката од Ургентен центар доби отказ" ("Female MD from Emergency Center Fired"), Vest, 6 January 2010, available at <http://www.vest.com.mk/?ItemID=65BF4D97C85223419A94E8C148FC33E6>.

Genetic identification

The Law on Family¹⁰² holds that the data on adoptions are an official secret.

FINANCIAL PRIVACY

The Law on the National Bank of the Republic of Macedonia¹⁰³ obligates the members of the Council of the National Bank and the employees of the National Bank to keep official and business secrets. This obligation binds these persons for five years following the end of their term. Data that are official or business secrets may be provided only upon written request of the court. Furthermore, the Banking Law¹⁰⁴ determines the categories of persons who may not reveal data and information classified as bank business secrets by law, statute, and other banking acts. The obligation to keep a business secret that persists after the termination of employment with the bank also relates to persons with special rights and responsibilities, bank employees, and other persons with access to bank operations. The data such as savings and bank deposits of natural and legal entities, as well as the account operations of natural and legal persons, are classified as business secrets of the bank. The above data may be provided only in the following cases: (1) If the client provides written consent to reveal the data; (2) Upon written request or order of the competent court; (3) Upon written request of the national bank or another body authorised by law for the purpose of monitoring; or (4) If the data are provided to the Directorate for Money Laundering Prevention in accordance with law. Additionally, in accordance with the Law on Securities,¹⁰⁵ the management and the employees of the Central Securities Depository, as well as certified auditors, are obliged to keep confidential the data learned through their employment unless they are obliged to provide such information in accordance with specified law.

E-GOVERNMENT & PRIVACY

The aforementioned Metamorphosis survey, "Privacy in Macedonia 2009", also examines the adoption of privacy policies by the government websites using *.gov.mk* domains. The survey is based on the available records in the MARNet's register (third-level domains only). The register contains the information about ownership of the active *.mk* domains, including the name, administrative, and technical contact of the owners (e-mail and telephone).

This segment of the research is limited by the fact that some governmental websites also use second-level domains (*e.g. www.vlada.mk*) or even *.COM* (*e.g., www.investinmacedonia.com*). The number of these websites seems small in comparison

¹⁰² Official Gazette of the Republic of Macedonia Nos. 80/92, 09/96, 38/04 and 83/04 – consolidated text.

¹⁰³ Official Gazette of the Republic of Macedonia Nos. 03/02, 51/03, 85/03 and 40/04.

¹⁰⁴ Official Gazette of the Republic of Macedonia Nos. 63/00, 103/00, 70/01, 37/02, 51/03, 85/03 and 83/04.

¹⁰⁵ Official Gazette of the Republic of Macedonia Nos. 63/00, 103/00, 34/01, 04/02, 37/02, 31/03, 85/03 and 96/04.

with the number of "regular" *gov.mk* websites, and it is the opinion of the research team that the results obtained through analysis of the larger segment can be generalised to the overall Web presence of the state and local public institutions.

All 269 *.gov.mk* domains from MARNet's register, excluding the 56 domains that returned errors during this phase, were subjected to automatic checking similar to the one for the general *.mk* sample. Those that were found to be functioning were then checked manually, and 33 of them were found to be non-functional. The remaining 180 front pages were examined for links leading to a privacy policy or a document serving such a purpose.¹⁰⁶ After excluding 15 duplicate domains that all led to the same website the remaining 165 functioning individual websites were examined. In effect, not a single website owned by the various levels of government in the Republic of Macedonia could be identified as having a functional privacy policy, a percentage even lower than the already established low presence of such documents on the Macedonian Web in general.

In 2009, several cases of the use of foreign-based services by government bodies also raised privacy concerns because the citizens' personal data were transferred outside the borders of the Republic of Macedonia. Namely, in order to conduct various official businesses, the representatives of several governmental bodies have required or invited the citizens to send their personal data via foreign services such as e-mail providers or social networks. In effect, citizens' personal data were placed outside the jurisdiction of the relevant Macedonian authorities (DPDP) as foreign companies are instead subject to the laws of their home countries.

In general, the use of free email providers remains widespread among the employees of all levels of government, who for correspondence often use their Yahoo!, Gmail, or Hotmail accounts for correspondence instead of an official email address on a *gov.mk* domain/their institutional domain. This practice also affects the establishment of ICT standards within public institutions and the archiving of correspondence, which should be part of the institution's system, and which needs to remain available for audits and other purposes.

For example, in an advertisement published on 9 July 2009 as part of the effort to "upgrade the concept of accountability and closeness to the citizens", the ruling political party published the e-mail addresses of its 52 MPs.¹⁰⁷ Most of them used foreign-based services, such as Yahoo! (50 percent), Gmail (4 percent), and Hotmail (1 percent), while the rest used the Parliament's email "*@sobranie.mk*" (38 percent) or other Macedonian providers (6 percent).

¹⁰⁶ Several government websites have functional "www.websitename.gov.mk" address, but failed to activate the redirection from the domain "websitename.gov.mk" without the "www." prefix.

¹⁰⁷ Advertisement by VMRO-DPMNE – Vnatrešna makedonska revolucionerna organizacija–Demokratska partija za makedonsko nacionalno edinstvo (Macedonian Revolutionary Organization–Democratic Party for Macedonian National Unity) – with email addresses of their members of the Parliament in a newspaper, *Vest*, 9 June 2009, available in Macedonian at http://www.scribd.com/full/31992778?access_key=key-wkktl6f0zhcnkwl6asy.

A particular example of this tendency involved the celebration of visa liberalisation within the EU, a round-trip to Paris for 100 randomly chosen citizens, organised by the Secretariat of European Affairs on 17 December 2009. To participate in the draw, the citizens had to possess a biometric passport and send their personal data (name, surname, passport ID number, and telephone) in hardcopy through regular mail or by e-mail to a Gmail account.¹⁰⁸

OPEN GOVERNMENT

Free access to information and the freedom of reception and transmission of information are guaranteed by the Macedonian Constitution. Article 16 paragraph 3 states, "The freedom of personal conviction, conscience, thought, and public expression of thought is guaranteed. The freedom of speech, public address, public information, and the establishment of institutions for public information is guaranteed. Free access to information and the freedom of reception and transmission of information are guaranteed. The right of reply via the mass media is guaranteed. The right to a correction in the mass media is guaranteed. The right to protect a source of information in the mass media is guaranteed. Censorship is prohibited".

After a drafting process of over four years, the Law on Free Access to Information of Public Character (Freedom of Information Law) came into force on 1 September 2006.¹⁰⁹ The Commission for Protection of the Right to Free Access to Public Information is in charge of monitoring of its implementation.¹¹⁰

For the first time after the adoption of the Law on Free Access to Information of Public Character in January 2006, the Law underwent substantial amount of changes in early January 2010.¹¹¹ The Ministry of Justice drafted amendments to the existing law in October 2009 in a non-transparent process, without the participation of the Commission, the experts in the area, or representatives of civil society, although the process for amendment of the law was initiated and supported by the FOSIM and the OSCE spill-over mission in Skopje.

After two years of monitoring the implementation of the law, the idea to amend it was launched in mid-2008 in order to correct some of the law's weaknesses and to improve

¹⁰⁸ Aleksandar Dimitrijevic, "Оглас 'За акција без визи' за 100 среќници кои ќе патуваат во Париз на 19 Декември 2009" ("Advertisement for 'No Visas Action' – 100 Lucky Guys to Travel to Paris on 19 December 2009"), *Volan*, 14 December 2009, available at <http://volanskopje.blogspot.com/2009/12/100-19-2009.html>.

¹⁰⁹ Law on Free Access to Information of Public Character, Official Gazette of the Republic of Macedonia No.13. 1 February 2006.

¹¹⁰ The Commission for Protection of the Right to Free Access to Public Information is an independent body responsible, among other things, for deciding upon appeals against rejected access to information requests. More information on the Commission are available at its official website at www.komspi.mk.

¹¹¹ The Law also underwent minor changes of the misdemeanor sanctions in 2008 in order to harmonize with the Misdemeanor Law that was adopted in 2007, *supra*.

free access to information. The two partner organisations, FOSIM and the OSCE spill-over mission in Skopje, established an expert task group that worked on drafting the amendments together with a team consisting of Ministry of Justice officials. The main goals of the working group were: improving the definition of information holder and information of public character; regulating the use of the harm test; imposing obligations on information holders to disclose information of public character such as relevant laws, bylaws, and draft legislation, improving the availability of statistical data, press releases, and reports on the work on institutions' official websites; improving and regulating the right to appeal in some circumstances in which the right of access to information was not effective; improving the independent status of the Commission for Protection of the Right to Free Access to Information of Public Character¹¹² (Commission) and redefining the composition of the Commission and conditions that a candidate for president, vice-president or a member of the Commission should fulfil; improving the administrative capacities of the Commission; redefining the content of the obligatory annual report that each information holder submits to the Commission; and improving the respect of the right of access to information by imposing various misdemeanour sanctions both against authorised officials and the official persons who fail to lawfully provide access to public information when asked.

Besides the joint work of the expert group and the Ministry of Justice, the amendments the Ministry submitted to the Parliament of the Republic of Macedonia had several substantial shortcomings. Therefore, FOSIM advocated improving the amendments by participating in the session of the Parliamentary Committee on the Political System and Inter-ethnic Relations in the stage of the first reading of the proposed amendments. Furthermore, FOSIM drafted amendments to the proposed changes and submitted them to the Assembly of the Republic of Macedonia through the Chairperson of the Standing Inquiry Committee for Protection of Civil Freedoms and Rights.

Most of the FOSIM's amendments were intended to stress the importance of charging the Commission with the ability to impose misdemeanour sanctions against information holders when they fail to provide access to information and also to legally bind the information holders to disclose the draft legislation. The latter was pointed out in order to strengthen the Commission's position and to improve the implementation of the law with the Commission's power to carry out misdemeanour procedures. However, this argument was not accepted by the Parliament and the courts continue to have the only jurisdiction for misdemeanour procedures. Although the importance of making draft legislation available was pointed out in the European Commission Report for the Progress of the Republic of Macedonia, the amendment that would have required information holders to make such information public was not approved either.

The amendments to the Law were enacted by the Assembly of the Republic in January 2010, encompassing some of the amendments proposed by FOSIM.

¹¹² The Commission for the Protection of the Right to Free Access to Information of Public Character, *supra*,

The Law on Local Self-Government of the Republic of Macedonia recognises the obligation to inform the public. Article 8 states: "(1) The organs of the municipality, the council committees, and public agencies established by the municipality shall be obliged to inform the citizens about their work, as well as about the plans and programmes which are of importance for the development of the municipality without any compensation, in a way determined by the statute. (2) The municipality shall be obliged to enable access to the basic information about the services that it provides to its citizens, in a way and under conditions determined by the statute of the municipality."¹¹³

In July 1999, the Republic of Macedonia signed and ratified the Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Århus Convention).¹¹⁴

FOSIM continues to promote the right to free access to information. Project activities in 2009 focused on monitoring the implementation of the Freedom of Information Law, providing free legal aid for rejected requests and strategic litigation to test the Law. FOSIM, in cooperation with Youth Educational Forum (YEF) and Macedonian Young Lawyers' Association (MYLA), submitted a total of 800 (115 FOSIM, 190 MYLA, and 495 YEF) requests to over 90 institutions.¹¹⁵ The process of providing free legal advice and protecting citizens' rights before the relevant institutions continued during 2009 by securing free legal representation in cases where access to information is denied. More than 20 trained attorneys from MYLA litigated nearly 115 cases of complaints to the Commission. Most of the appeals were successful. The monitoring results showed that while progress is noted in comparison to previous years since the adoption of the Free Access Law, its implementation is still not satisfactory. Silence on the part of the administration (mute refusal) continues to be a challenge to the implementation of the law since approximately 30 percent of the requests were answered only after appeals were submitted to the Commission. Also, there was one administrative court dispute initiated during 2009, while one dispute in the Administrative Court that was initiated in 2008 was finally settled in favour of the information requester in June 2009.

Free legal advice for citizens continued to be provided through a help line that gives interested persons the opportunity to ask questions relating to free access to information and receive answers. Fifty-one calls related to different legal issues were recorded in 2009, indicating that the population is aware of neither the existence of the law nor of the rights this law guarantees. Even so, through the help line MYLA has helped citizens to prepare request forms, providing them with information as to how they can maximise the information they obtain, as well as explaining matters of interest.

¹¹³ Official Gazette of the Republic of Macedonia No. 5/2002.

¹¹⁴ Official Gazette of the Republic of Macedonia No. 40/1999.

¹¹⁵ Based on the monitoring results, MYLA publishes monthly reports and an annual analysis concerning free access to information in Macedonia, which are regularly distributed to the media.

In cooperation with YEF, FOSIM organised training for students. The procedures and aims of the Freedom of Information Law were clarified and detailed for 35 participants. The purpose of the training was to encourage participants and equip them with relevant knowledge on the use of the right to free access to information. Following the training, 287 requests were submitted by the participants. On the basis of data collected through the submitted Freedom of Information requests, Youth Educational Forum, with the support of FOSIM, drafted and published a report on the implementation of the European Credit Transfer System in the Republic of Macedonia that also contained a report on the implementation of the Freedom of Information Law. These results were publicly presented by FOSIM at the launch of the publication.

Additionally, in cooperation with MYLA, two discussion sessions were held on the topic of the Law on Free Access to Information of Public Character and the potential for its use for research purposes. The first was held with a group of journalists and focused on the possibilities the law opened up for investigative journalism. The second discussion session was held in cooperation with the Faculty of Law Iustinianus I at the University Sts. Cyril and Methodius,¹¹⁶ where before a group of 30 teaching assistants and faculty researchers, the advantages of applying the Law on Free Access to Information to academic research were presented.

FOSIM, through a public bid, chose a research agency to conduct a public survey for citizens and public officials regarding the free access to information. The results of the survey were devastating; the vast majority of the citizens did not know the law even exists. In addition, there were major differences between the citizens' opinions and those of the information holders. A press conference was organised in May 2009 to present these findings; the highlights of which are provided in a separate document.¹¹⁷ Based on the survey findings, FOSIM produced recommendations to the authorities, aimed at increasing the transparency and accountability of their work.

OTHER RECENT FACTUAL DEVELOPMENTS

In 2009, the disclosure of classified information and wiretapped content on YouTube led to two political scandals in Macedonia. In both cases the person/s who uploaded the file have not been identified, and no information about possible police investigation has been made publicly available.

The first scandal took place in November and December 2009 and involved opposition party leader Ljube Boshkoski. A series of clips displaying his alleged "betrayal" of his comrade Johan Tarchulovski during their trial before the International Criminal Tribunal for the Former Yugoslavia were made available to the public. The clips showing

¹¹⁶ Faculty website's at <http://pf.ukim.edu.mk> ; University's website at <http://www.ukim.edu.mk>.

¹¹⁷ Perceptions of Citizens of the Republic of Macedonia in Regards to Exercising Their Right for Free Access to Public Information and Assessment of Holders of Information for the Application of This Right and the Problems They are Encountering, FOSIM, February 2009, available at http://soros.org.mk/dokumenti/Survey_Public_Perception_FOI_Law.pdf.

Boshkoski reading an allegedly incriminating document during a court procedure in Pula, Croatia, were first published on YouTube and then widely propagated by pro-Government traditional media including Sitel TV¹¹⁸ and the national broadcaster, Macedonian Radio and Television.¹¹⁹ This so-called "Internet War" escalated two weeks later, when new clips appeared featuring statements by Tarchulovski branding Boshkoski as a traitor,¹²⁰ Tarchulovski – through his lawyer – then claimed that the clips were forgeries.¹²¹ Even though one of the lawyers defending Boshkoski claimed that publication of the classified documents used in the Tribunal proceedings is a crime under Macedonian law,¹²² the law enforcement agencies have not publicly announced any investigation.

The second political scandal took place in late December and concerned the upload on YouTube of an audio recording of a apparently wiretapped conversation between the head of Market Inspectorate Sasho Akjimovski and a disothèque owner, during which they conspire to put a competitor out of business. The link spread through social and traditional media, which presented it as a scandal that revealed corruption within the current administration. Even though Akjimovski claimed that he was framed,¹²³ he was fired two days later.¹²⁴ The Minister of Economy announced a comprehensive investigation,¹²⁵ but the Public Prosecutor announced that the clip cannot be used as sufficient evidence to start an investigation of the accusations of corruption.¹²⁶ The authorities have not tackled the issue of discovering the source of the recording, either.

¹¹⁸ Filip Petrovski, "Интернет-војна" ("War on the Internet"), *Utrinski Vesnik*, 9 January 2010, available at <http://r.ping.mk/11pz>.

¹¹⁹ Svetlana Unkovska, "За оцрнување на Бошкоски се впрегна и МРТ" ("MRT Employed to Blacken Boshkoski's Name"), *Utrinski Vesnik*, 9 December 2009, available at <http://www.utrinski.com.mk/?ItemID=773CA2844760514A9D2C1D093A0FDCB5>.

¹²⁰ Olivera Vojnovska, "Македонско кодошко сценарио 'фатете го предавникот'" ("Macedonian Snitch Scenario: 'Catch the Traitor'"), *Utrinski Vesnik*, 5 December 2009.

¹²¹ Ivona Talevska and Dejan Mishevski, "Јохан ги тужи Љубе и А1 за фалсификат!" ("Johan Will Sue Ljube and A1 for Forgery"), 5 December 2009, available at <http://www.vecер.com.mk/default.asp?ItemID=A313D5B1EA03674487CC6C910C5EF5F6>.

¹²² Jasminka Dogova, "Хашкиот трибунал ќе го бара изворот" "Hague Tribunal Looking for the Source"), *Vreme*, 7 December 2009, available at <http://r.ping.mk/11pv>.

¹²³ "Власта молчи за државниот рекет на дискотеките" (Government Keep Numb About State Racket over Disco Clubs"), *Utrinski vesnik*, 26 December 2010, available at <http://www.utrinski.com.mk/?ItemID=F80AD48A1B953248BBA8D0F0EBCDF628>.

¹²⁴ Daniela Trpchevska, "Валканици на 'Јутјуб'" ("Dirty Laundry on YouTube"), *Utrinski Vesnik*, 4 January 2010, available at <http://r.ping.mk/11pw>.

¹²⁵ Mirkica Popovik, "Скандалот со аудиоклипот на 'Јутјуб' во ќор-сокак" ("Dead End for the 'YouTube' Audio Clip Scandal"), *Utrinski Vesnik*, 29 December 2009, available at <http://r.ping.mk/11px>.

¹²⁶ S.K.D., "Скопското обвинителство стои на располагање за скандалот на Јутјуб" ("Skopje Public Prosecutor Says They are at Disposal for YouTube Scandal"), *Vest*, 29 December 2009, available at <http://www.vest.com.mk/?ItemID=6AA0F50D12B8494C80FF0E87C9666C50>.

As reported above, the government body websites generally lack privacy policies. Moreover, in some cases, users' additional data – not relevant to the service provided by the website – are collected without providing any explanation about what is to happen to those data, how they will be archived, and how they will be used. For example, the *.gov.mk* website run by the Ministry of Information Society has no privacy policy and collects private data (email addresses) from everyone who downloads a package of free Macedonian Cyrillic fonts.¹²⁷ Other institutional websites that do not use *.gov.mk* domains include the Parliamentary site, which uses a second-level *.mk* domain,¹²⁸ and the Government's anti-drugs campaign, which uses a *.com.mk* domain that is outsourced to a private advertising agency.¹²⁹ Neither of these two sites has a privacy policy, even though they collect personal data. In the case of the Parliamentary website, users who want to communicate with the deputies via online forms must input their name, surname, and e-mail address.¹³⁰ The government's campaign against drugs asks visitors to participate in an online survey about their illegal drug use, i.e., to provide incriminating information that could potentially be linked to their IP address or other personal data left on the website, such as forum postings.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

There is no strong Macedonian human rights NGO that specialises in privacy and personal data protection. However, several NGOs cover the issue with a specific focus in line with their mission and types of activities. Two particular subjects of concern in the reported period were the protection of the human rights of children on the Internet – including children's privacy – and the protection of privacy by the police and law enforcement agencies.

The NGO Metamorphosis Foundation organises an annual International Conference on Privacy Protection and Open Government that provides a forum for regional cooperation and networking among decision makers and activists from the Western Balkans with the purpose of Euro-integration, especially as it always includes representatives of the EU-based European Digital Rights (EDRI).¹³¹ The Open Society Institute Macedonia (FOSIM) advocates open government through public monitoring, educational and lobbying efforts aimed at promoting the Law on Free Access to Information of Public

¹²⁷ Ministry of Information Society, Macedonian Fonts, 24 August 2010, available at <http://www.mio.gov.mk/?q=node/2241>.

¹²⁸ Assembly of the Republic of Macedonia website is available at <http://sobranie.mk>.

¹²⁹ Campaign "Животот е мојот филм" ("Life is My Movie") is available at <http://zivototemojotfilm.com.mk>.

¹³⁰ "Fill out the form and send your comments to the Assembly of the Republic of Macedonia," form available at <http://www.sobranie.mk/default.asp?section=kontaktPratenik>.

¹³¹ Metamorphosis Foundation at <http://www.metamorphosis.org.mk> ; E-society Conference's webpage at <http://www.e-society.org.mk> . The E-society Conference is supported by OSCE and FOSIM; FOSIM's website at <http://www.soros.org.mk> ; European Digital Rights at <http://www.edri.org>.

Character, the LPDP, and the Law on Classified Information in cooperation with the relevant state bodies and Metamorphosis.

On the occasion of International Data Protection Day, 28 January 2007, Metamorphosis and the Directorate, in cooperation with the EU project for Technical Assistance to the Establishment of the Directorate and Enforcement of the Data Protection Principles, prepared and published a special issue of the Metamorphosis ICT Guide entitled "Privacy as a Fundamental Human Right." Five hundred printed copies were distributed to government officials, MPs, media, and other stakeholders including university students free of charge, and the e-version of the Guide remains available for download on Metamorphosis website.¹³²

Legal experts and human rights activists have raised concerns about the extensive use of detention as it relates to privacy violations and the presumption of innocence. The Macedonian Helsinki Committee¹³³ and the network of five local NGOs¹³⁴ that work with victims of alleged police abuse continuously condemned the spectacular arrests by the police that included inviting the media to film the handcuffed suspects escorted by law enforcement officers. In order to raise public awareness and condemn specific violations and spectacular arrests, nine media events were organised. As a result, TV Telma, one of the then six television stations licensed for national coverage, adopted the policy of no longer broadcasting any arrests and police-escorted transports.

Individual citizens have contributed to raising public awareness on privacy protection issues. The media gave significant attention to the public disclosure of the effects of 40 years of communist regime surveillance of the late poet Jovan Koteski, provided by his daughter, Jasna Koteska. In addition, a number of Macedonian bloggers have tackled privacy issues in posts about information society development or politics on a national level.

The Metamorphosis Foundation also provided opportunities for raising awareness on the part of opinion and decision makers. For example, the Metamorphosis Foundation included data protection sessions within the 2007 agenda of the Third International Conference e-Society.Mk. This conference served as a tool for establishing the e-Government Western Balkans Network. This conference was also organised in Albania, Bosnia and Herzegovina, Croatia, Montenegro, and Serbia, and included the participation of EU-based experts, in particular members of EDRI.¹³⁵

¹³² Privacy as Fundamental Human Right – Third Metamorphosis ICT Guide, Metamorphosis Foundation, posted on Thursday 25 January 2007, available at <http://www.metamorphosis.org.mk/content/view/829/61/lang,en/>.

¹³³ More info on Helsinki Committee for Human Rights of the Republic of Macedonia can be found on their website <http://www.mhc.org.mk>, including their very significant monthly reports.

¹³⁴ The Human Rights Support Project's website is available at <http://www.hrsp.org.mk>.

¹³⁵ The project was supported by FOSIM and the East-East program of the Open Society Institute (OSI).

In November 2007, the Recommendations for ICT Standards in the Civil Service in the Republic of Macedonia were published. The document stressed that privacy is a key right for e-government development.¹³⁶ The government failed to provide any public response to these recommendations. However, during the June 2008 campaign, the leading political party announced that it will introduce IT standards in public institutions by 2010.¹³⁷

During 2009 the Metamorphosis Foundation conducted two privacy-related projects: "Online Privacy Initiative" and "Online Privacy Made Easy". For the former project, Metamorphosis served as a watchdog, monitoring, reporting, and raising public awareness about privacy issues, as well as proposing practical solutions to some of the technical and legal challenges. In addition, Metamorphosis continued to provide two-way translations (Macedonian-English) of at least one to two privacy-related articles every week from Macedonia and the EDRI-gram, and to promote good practices and useful websites and initiatives through the regular column "website of the day" in *Vreme* daily and its affiliated blog. For the latter project, building upon the CRISP project that finished in 2008, Metamorphosis continued to cater to the needs of children and teenagers for more educational e-content by continuing to provide age-relevant information through a column of the weekly supplement for kids *Kolibri* in *Nova Makedonija* daily, on the "Safely on the Internet" project website,¹³⁸ and through commencing production of educational videos and games.

As part of the International Action Day "Freedom not Fear 2009 – Stop Surveillance Mania!"¹³⁹ Metamorphosis, FOSIM, and six other NGOs (Internet Hotline Provider Macedonia, Macedonian Young Lawyers Association, Youth Educational Forum, ELSA-RM, and Macedonian Centre for European Education), joined the DPDP in organising the distribution of flyers in Macedonian and Albanian, and in providing expert consultations/hands-on-education for citizens on 12 September 2009 in Skopje.¹⁴⁰

¹³⁶ Miroslav Jovanovic, Zoran Janevski, Bardhyl Jashari, Karina Donevska, Aleksandar Ugrinoski, Kliment Kocovski, Andon Stefanovski, & Gjorgji Tasevski, Recommendations for ICT Standards in the Civil Service in the Republic of Macedonia, FOSIM, November 2007, available at http://gg.org.mk/pdf/recomendations_ICT.pdf. Good Governance website is available at <http://www.gg.org.mk>.

¹³⁷ "Program of VMRO-DPMNE for Rebirth 2008-2012: Rebirth in 100 steps, upgraded and expanded", VMRO-DPMNE, available at <http://www.vmro-dpmne.org.mk/Dokumenti/Programa%202008%20EN%20WEB.pdf>.

¹³⁸ "Safely on the Internet" is available in Macedonian at <http://bezbednonainternet.org.mk> and in Albanian at <http://internetisigurt.org.mk>.

¹³⁹ Freedom Not Fear website available at <http://freedom-not-fear.eu>.

¹⁴⁰ Macedonia: Freedom Not Fear 2009 – Activities for Citizen Education about Their Rights, by Metamorphosis Foundation, 12 September 2009, available at <http://www.metamorphosis.org.mk/activities/macedonia-freedom-not-fear-2009-activities-for-citizen-education-about-their-rights.html>.

Privacy and transparency issues were raised during the Fifth International Conference e-Society.Mk "I Media"¹⁴¹ organised in Skopje 2-3 December 2009, within the context of the development of new media and the enhancement of active civic participation. Localisation and adaptation of the applications built by the British NGO MySociety¹⁴² have been proposed as a solution to the need for establishing of multi-directional communication systems between citizens and the various levels of government. Metamorphosis and FOSIM undertook the initiative to adapt several of the applications from this open standards/FOSS-based suite. Applying this example of best practice will also affect the area of privacy, because the applications put minimum requirements for disclosing data by citizens, showing an alternative to the unnecessary collection and undefined retention by current government applications.

In May 2010, 16 NGOs including the Metamorphosis Foundation, Foundation Open Society Institute – Macedonia, Transparency Macedonia, and Helsinki Committee for Human Rights in Macedonia started an action supported by over 1,400 individual citizens against privacy-damaging changes of Law on Electronic Communications that give the police powers of unaccountable surveillance.¹⁴³ NGOs organised public debates and media events to provide opportunities for civic participation denied by the government. Governmental representatives did not participate in these events and avoided confrontation with legal experts and human rights activists. The conclusions by the NGOs, and the expert analyses were submitted to all MPs in hardcopy before the vote, together with a public petition.¹⁴⁴ However, the authorities ignored this effort and the rubber-stamping majority in the Parliament passed the law, which is currently being contested before the Constitutional Court by the original group of four NGOs.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Since 1994 Macedonia has been part of the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and of its First Optional Protocol, which establishes an individual complaint mechanism.¹⁴⁵

¹⁴¹ Fifth International Conference e-Society.Mk "I Media", official website available at <http://e-society.org.mk/portal/content/view/88/56/lang,en/>.

¹⁴² My society web page available at <http://mysociety.org>.

¹⁴³ "Call for Protection of Citizens' Privacy in the Republic of Macedonia, Metamorphosis Foundation," 8 June 2010, available at <http://metamorphosis.mk/activities/povik-za-zashtita-na-privatnosta-na-graganite-vo-republika-makedonija.html>.

¹⁴⁴ "The Call for Protection of Citizens' Privacy Submitted to the Assembly," Metamorphosis Foundation, 11 June 2010, at <http://metamorphosis.mk/activities/povikot-za-zashtita-na-privatnosta-predaden-vo-sobranie.html>.

¹⁴⁵ The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

The Republic of Macedonia is a member of the Council of Europe and has signed and ratified the Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁴⁶ In 2006, it signed and ratified Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data¹⁴⁷ and, in 2008, its Additional Protocol regarding Supervisory Authorities and Transborder Data Flow.¹⁴⁸ In 2004, the Republic of Macedonia ratified the Council of Europe Convention on Cybercrime.¹⁴⁹

* Updates to the Macedonian Report published in the 2010 edition of EPHR have been provided by: Bardhyl Jashari – Filip Stojanovski – Vesna Paunkovska – Nade Naumovska – Elena Stojanovska and Zoran Gligorov, Metamorphosis Foundation, Macedonia.

¹⁴⁶ Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005). All the international agreements adopted within the Council of Europe are available in English at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

¹⁴⁷ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), in force from 1 July 2006. Text published in the Official Gazette of the Republic of Macedonia No. 07/05.

¹⁴⁸ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), in force from 1 January 2009. See also Указ за прогласување на Законот за ратификација на Дополнителниот протокол кон Конвенцијата за заштита на поединците во поглед на автоматска обработка на лични податоци во врска со надзорните тела и прекуграничниот пренос на (Decree for enacting the Law of Ratification of the Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flow) Official Gazette of Republic of Macedonia, 19 August 2008, .Official Gazette of the Republic of Macedonia No. 103/08.

¹⁴⁹ Convention on Cybercrime (ETS No. 185), in force from 1 January 2005. Text published in the Official Gazette of the Republic of Macedonia No. 41/04.

KINGDOM OF THE NETHERLANDS

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Constitution grants citizens an explicit right to privacy.¹ Article 10 states: "(1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by, or pursuant to, Act of Parliament. (2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. (3) Rules concerning the rights of persons to be informed of data recorded concerning them, of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament." Article 12 states: "(1) Entry into a home against the will of the occupant shall be permitted only in the cases laid down by, or pursuant to, Act of Parliament, by those designated for this purpose by, or pursuant to, Act of Parliament. (2) Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions prescribed by Act of Parliament. A written report of the entry shall be issued to the occupant." Article 13 states, "(1) The privacy of correspondence shall not be violated, except in the cases laid down by Act of Parliament or by order of the courts. (2) The privacy of the telephone and telegraph shall not be violated, except in the cases laid down by Act of Parliament, by or with the authorisation of those designated for this purpose by Act of Parliament."

In May 2000, the government-appointed Commission for Constitutional Rights in the Digital Age presented proposals to make existing constitutional rights more technology-independent. According to this proposal, Article 10 will be expanded to include the right of persons to be informed about the origin of data recorded about them and the right to correct that data. Article 13 would be made technology-neutral and would give the right to confidential communications. In November 2004, the Dutch government announced that proposals to amend the Constitution would be delayed in order to incorporate upcoming international developments regarding human rights and the information society such as the Council of Europe's recommendation "Human Rights and the Rule of Law in the Information Society." The recommendation was adopted by the Council of Europe on 13 May 2005.²

¹ Constitution of the Kingdom of the Netherlands 2008, available in English at <http://www.rijksoverheid.nl/documenten-en-publicaties/publicaties-pb51/the-constitution-of-the-kingdom-of-the-netherlands-2008.html>.

² Warsaw Summit Council of Europe, 2005, Declaration of the Committee of Ministers on Human Rights and the Rule of Law in the Information Society, CM(2005)56 final, 13 May 2005, available in English at <https://wcd.coe.int/ViewDoc.jsp?id=849061>.

In 2009, the results of the evaluation of the Dutch Constitution were published.³ The evaluation states that the role and importance of the Dutch Constitution has been under pressure, especially because of the growing role of the European Convention of Human Rights and its interpretation by the European Court of Human Rights. In particular, in the Netherlands less value has been attached to the right to privacy than before. This development is generally attributed to the terrorist attacks of 11 September 2001 in New York but, seen from a more general point of view, the Dutch general public has developed a different approach towards privacy that amounts essentially to the willingness to trade privacy for safety (leaving aside the question whether such a trade-off exists).⁴

In July 2009 a new Commission was appointed by the government. Its assignment is to draft a Bill amending the Constitution *inter alia* in order to improve the accessibility of the Constitution and to adapt constitutional rights and freedoms to the digital age. The Commission was due to present its proposals before 1 October 2010.⁵

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The European Union Data Protection Directive 1995/46/EC was established as national law by the Act of 2000 (Dutch Personal Data Protection Act or PDPA).⁶ The PDPA is a revised and expanded version of the Data Registration Act of 1998 that brings Dutch law in line with the EU Directive and regulates the transfer of personal data to countries outside of the European Union.

Pursuant to the PDPA, the Decree on Regulated Exemption was enacted to exempt certain organisations from the registration requirements of the PDPA.⁷

³ T. Barkhuysen, M.L. van Emmerik, W.J.M. Voermans, *De Nederlandse Grondwet geëvalueerd: anker- of verdwijnpunt?* ("The Dutch Constitution Evaluated: Anchor Point or Vanishing Point?"), Alphen aan den Rijn, (Kluwer, 2009).

⁴ H.B. Winter et al. *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk* (What the Eye Doesn't See the Heart Doesn't Grieve Over. An Evaluation of the Dutch Data Protection Act), Den Haag, The Research and Documentation Centre (WODC), 14 (2008).

⁵ Decision of 3 July 2009, No. 09.001852.

⁶ *Wet Bescherming Persoonsgegevens* (Dutch Data Protection Law). Act of July 2000, Bulletin of Acts, Orders and Decrees 302 (concerning regulations regarding the protection of personal data). Unofficial translation available at http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml.

⁷ Decree on Regulated Exemption, 7 May 2001.

In 2007, the report of the first stage of the evaluation of the PDPA was published, followed in 2008 by the report of the second stage of the evaluation.⁸ The evaluation reports concluded that the PDPA leads to administrative burdens.⁹

On 5 February 2009 the bill to amend the PDPA was submitted to Parliament.¹⁰ In the explanation of the amendment to the bill after investigation and consultation with the parties involved (including the CPB and the Dutch Association of Entrepreneurs and Employers), a number of its proposals appeared not to be feasible.¹¹ Overall, it was determined that completing many of the act's new proposals imposes a serious administrative burden.¹²

One of the amendment clauses aims to remove the permit obligation for third-country transfers. In the Netherlands a transfer permit is required even if the transfer is made under the standard contractual clause for the transfer of personal data to third countries.¹³ The bill explaining the amendment makes it clear that the cancelled obligation only occurs when the standard contractual clauses are applied unaltered.¹⁴ This means that no clauses in the model contract may be altered.¹⁵

A second amendment mitigates the controller's obligation to provide information to data subjects¹⁶ if personal data are used for direct marketing.¹⁷ For example, a data controller intending to provide data to third parties so that they can use the data for direct marketing purposes must now inform the data subjects of the transfer and give them the opportunity to raise an objection by advertising in one or more newspapers or free local papers.¹⁸

In addition, as of 1 October 2009 there is an explicit obligation for those engaging in the widespread and largely detested practice of telemarketing to include in each unsolicited

⁸ First phase of the evaluation: G.-J. Zwenne, A.-W. Duthler, M.M. Groothuis, H.H. Kielman, W.I. Koelwijn en L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Den Haag, , WODC 209 p (2007). Second phase of the evaluation: H.B. Winter et al, *supra*. Cf. Hester De Vries, Netherlands: DP Bill retains administrative burdens, *Privacy Laws and Business International Newsletter*, Issue 98 (April 2009).

⁹ De Vries, *supra*.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ Section 77(2) of the PDPA.

¹⁴ De Vries, *supra*.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

telephone call information about the existence of the "do-not-call registry" (i.e., an opt-out register).¹⁹ Further, as of the same date the anti-spam rules for e-mail and other forms of electronic communications, which previously protected only natural persons, have been extended to provide protection to other subscribers (i.e. legal persons, companies etc.). As a result, commercial unsolicited emails, SMS, and other forms of electronic communication to consumers and businesses fall within an opt-in regime. An important exemption applies to electronic contact details (i.e., email addresses, SMS numbers, etc.) that are collected while selling services or products. Such contact details may be used to inform the recipient about the sellers' own similar products. On its website, telecoms regulator OPTA (*Onafhankelijke Post en Telecommunicatie Autoriteit* or Independent Post and Telecoms Authority) has published guidelines and answers to frequently asked questions explaining its interpretation of the telemarketing and anti-spam rules.²⁰

Sector-based laws

In the Dutch legal order, there are also sector-based privacy laws regulating the Dutch police,²¹ medical exams,²² medical treatment,²³ social security,²⁴ and the search of private homes.²⁵ A series of laws concerning the Dutch social security number regulates the allowable uses of this number for identifying citizens and for general administrative purposes, as well as in health care (regarding electronic patient records).²⁶

DATA PROTECTION AUTHORITY

The Dutch data protection authority (*College Bescherming Persoonsgegevens* or CBP) supervises the operation of personal data files in accordance with the PDPA.²⁷ Previously known as the *Registratiekamer*, the CBP's functions have remained largely the same since the implementation of the PDPA, although it has been given new powers of enforcement. It can now apply administrative measures and impose fines for non-compliance. It can also levy fines, of up to €4,500 for breaches of the notification

¹⁹ *Id.*

²⁰ See OPTA's Frequently Asked Questions on Spam, to be found at <http://www.opta.nl> or <http://www.spamklacht.nl> (both in English and in Dutch).

²¹ Dutch Police Registers Act 1990 (no longer in force), Dutch Police Data Act 2008.

²² Dutch Medical Examinations Act 1997.

²³ Dutch Medical Treatment Act 1997.

²⁴ Dutch Social Security System Act 1997, Compulsory Identification Act.

²⁵ Dutch Act on the Entering of Buildings and Houses 1994 (*Algemene wet op het binnentreden*).

²⁶ Dutch Act on general regulations with respect to the citizens' service number (*Wet algemene bepalingen burgerservicenummer*).

²⁷ At <http://www.dutchdpa.nl/>.

requirements.²⁸ Otherwise, the CBP advises the government, deals with complaints submitted by data subjects, institutes investigations, and makes recommendations to controllers of personal data files.

On 28 January 2008, the chairman of the CBP called for an increase in its supervisory power to strengthen the enforcement of the data protection law and to take direct actions regarding investigations and fines.²⁹ In November 2009, the Minister for Justice announced that the CBP would be awarded more powers, particularly the power to impose fines for violations of the PDPA. A bill to that effect has not yet been published.

The Dutch CBP has 84 full-time positions.³⁰ The CBP generally relies on a network of privacy officers within companies and (government) institutions to produce annual privacy reports and discuss procedures with the CBP. In 2009, the CBP performed 108 investigations, a slight increase over 2007 and 2008. It performed 188 prior investigations, almost doubling the figures of 2007 and 2008.³¹

In the previous version of this report, several cases were described in which the CBP had serious doubts about compliance with the PDPA. These cases concerned the public transport chipcard, the exchange of financial records via SWIFT, and the electronic patient file.³² Further cases are outlined below.

The CBP also condemned the illegal transfer of financial records of European citizens to the United States via SWIFT.³³

In December 2007, the CBP approved guidelines on the processing of personal data in publications on the Internet based on the Dutch Data Protection Act.³⁴ They explain whether, when, and in what format online publications containing personal information are permitted. The guidelines also advise citizens on what options are available when their personal data is misused.³⁵ Subsequently, in August 2009, the CBP publicised new guidelines for active publication of governmental information containing personal data

²⁸ Art. 75 PDPA also contains penal sanctions, but imposing these is the prerogative of the judiciary.

²⁹ Straks niemand meer onbespied door het leven: Toezichthouder CBP koerst op stevige handhaving van de privacyregels (CBP Called to Increase Powers for Strong Enforcement of Privacy Law), available in Dutch at http://www.cbpweb.nl/Pages/pb_20080128_dataprotectedag.aspx.

³⁰ CBP Annual Report for the Year 2009, available in Dutch at http://www.cbpweb.nl/downloads_jaarverslagen/Jaarverslag_2009.pdf.

³¹ *Id.*

³² See Privacy and Human Rights 2006, Kingdom of the Netherlands, online updated version of 18 December 2007, at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559513](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559513).

³³ See http://www.cbpweb.nl/Pages/ind_nieuws_publ.aspx.

³⁴ Dutch DPA Publication of Personal Data on the Internet, December 2007, available in English at

³⁵ *Id.*

such as citizens' service numbers.³⁶ As publishing such information could lead to identity fraud, the CBP recommends adhering to strict guideline whose objective is to enable administrative authorities to make a good judgment as to the extent to which the information can be published.

The BSN (Burger Service Number or Citizen's Service Number) was introduced at the end of November 2007.³⁷ "At the BSN management facility, a personal public service point will be created that local authorities and citizens can approach with questions."³⁸ The CBP is the authority with competence to intervene in the event of real problems with implementation of the Act.³⁹

The CBP has expressed criticism of the proposal for a *verwijsindex risicjongeren* (VIR or national reference index of young people at risk).⁴⁰ The CBP wants to achieve better and faster help for children and young people with problems, "but it is not yet clear whether the sole objective of the reference index is the provision of assistance, or whether its aim is also to help maintain public order."⁴¹

In January 2009, the CBP published guidelines for the application of automatic number plate recognition in the Netherlands.⁴² In its report, the CBP concludes that this method of obtaining personal information can only be used when the police detects a "hit" between the number plates it scans and the reference file against which it is comparing the scans. The CBP argues that if "non-hits" are stored by the police, everyone who uses that particular road is treated as a suspect, leading to an invasion of personal privacy that the CBP considers unlawful.⁴³

³⁶ CBP-richtsnoeren. Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, at http://www.cbpweb.nl/downloads_rs/rs_20090813_actieve_openbaarmaking.pdf.

³⁷ 11th Annual Report of the Article 29 Data Protection Working Party (2007), 24 June 2008, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² CBP, De toepassing van automatische kentekenherkenning door de politie ("Application of Automatic Number Plate Recognition by the Police"), January 2009, in Dutch at http://www.cbpweb.nl/downloads_rs/rs_20090109_anpr.pdf.

⁴³ *Id.*

In January 2010, the CBP concluded that two police agencies, Rotterdam-Rijnmond⁴⁴ and IJsselland,⁴⁵ had violated the PDPA by processing "non-hits" from an automatic licence plate recognition system. They are only allowed to process "hits", i.e., licence plates that, scanned, matched a licence in the database.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In July 2008, the judge in the preliminary injunction Court in Arnhem ruled that the research group of the University of Nijmegen could publish their paper on the security breaches found in the Mifare Classic chip.⁴⁶ The chip, which was intended for use in a national public transportation card, has severe security flaws such as an "easy method to retrieve cryptographic keys."⁴⁷ In March 2008, the University researchers claimed that: "Because some cards can be cloned, it is in principle possible to access buildings and facilities with a stolen identity. This has been demonstrated on an actual system."⁴⁸ After the manufacturer of the chip, NXP, sued the University, "the Rechtbank Arnhem court decided that prohibiting the publication of the article would violate the researchers freedom of expression covered by article 10 of the European Convention of Human Rights. Restrictions in such matters are applicable only in order to protect a pressing social need, which has to be convincingly demonstrated."⁴⁹ The judge's opinion was that "the potential damage that NXP claims is not a result of the publication of the research results but of the production of a chip that has shown deficiencies, which is the responsibility of NXP itself."⁵⁰

On 24 August 2006, the Subdistrict Court of Amsterdam ruled that an Internet Service Provider (ISP) can in certain circumstances be required to release the name, address, and

⁴⁴ CBP, Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Number Plate Recognition Regionaal politiekorps Rotterdam-Rijnmond ("Investigation into Processing of No-Hits with Automatic Number Plate Recognition for the Regional Police Department of Rotterdam-Rijnmond"), January 2010, in Dutch at http://www.cbpweb.nl/downloads_pb/pb_20100128_defintieve_bevindingen_rotterdamrijnmond.pdf.

⁴⁵ CBP, Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Number Plate Recognition Regionaal politiekorps IJsselland ("Investigation into Processing of No-Hits with Automatic Number Plate Recognition for the Regional Police Department of IJsselland"), January 2010, in Dutch at http://www.cbpweb.nl/downloads_pb/pb_20100128_defintieve_bevindingen_ijsselland.pdf.

⁴⁶ Radboud University allowed publishing Mifare Classic Chip article, July 2008, at http://www.infrasite.net/news/news_article.php?ID_nieuwsberichten=10591&language=en.

⁴⁷ Security Flaw in Mifare Classic, 12 March 2008, available at http://www.infrasite.net/news/news_article.php?ID_nieuwsberichten=9548&language=en.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ *Id.*

domicile data of a subscriber (referred to as "NAW-data").⁵¹ BREIN, a Dutch foundation that protects the rights of the entertainment industry, requested NAW-data on the top three uploaders on *Dikke Donder*, a BitTorrent network where films, television series, music, software, and games were being offered without the permission of the rights holders.⁵² The court ruled in favour of BREIN and required the ISP to provide the requested data as long as two conditions were met: (1) it must be sufficiently plausible that the unlawful act has been committed; and (2) there must be no reasonable doubt that it was committed by the subscriber whose NAW-data is being requested.⁵³

BREIN announced in April 2005 it would launch 32 court cases against individuals who were allegedly peer-to-peer file-sharing users. In order to obtain the identifying data of the users behind IP addresses from which music was unlawfully uploaded, BREIN sued five Dutch ISPs who had agreed to forward to their customers complaints from the copyright holders but refused to reveal the customers' identities. In total, BREIN sent 50 cease-and-desist letters demanding that the recipients identify themselves, agree to pay an average fine of €2,100, and sign an unlimited, binding agreement never to "directly or indirectly be involved in any way or have an interest in unlawfully distributing materials on the Internet". If ever again caught in such a broadly defined act, the signed agrees to pay a fine of €5,000 per day.⁵⁴ In June 2004, the Appeals Court of Amsterdam ruled against Lycos in *Lycos v. Pessers*; Lycos had refused to disclose the identity of one of its customers when it was demanded for alleged defamation.⁵⁵ Although the Appeals Court acknowledged that the content on the website was not "apparently unlawful", the court nevertheless felt that Lycos was required to hand over the user's identity. On 25 November 2005, the Dutch Supreme Court upheld the appeals court's decision, requiring Lycos to disclose the name of the previously anonymous website owner.⁵⁶ *The Register* reported that BREIN, who paid the legal bill of Pessers, was delighted with the verdict, believing the ruling would be beneficial to its case against ISPs who refused to identify illegal file swappers.⁵⁷ Legal experts fear the ruling may have consequences for

⁵¹ Dutch ISP Ordered to Release Personal Data of a Subscriber, 23 Computer Law & Security Report 2, 145 (2007).

⁵² *Id.*

⁵³ *Id.*

⁵⁴ "New Wave of Lawsuits against European P2P Users," EDRI-gram, Number 3.8, 20 April 2005, available at <http://www.edri.org/edrigram/number3.8/P2P>.

⁵⁵ "Court attacks Dutch internet anonymity," EDRI-gram, July 2004, at <http://www.edri.org/edrigram/number2.14/anonym>.

⁵⁶ Jan Libbenga, "Lycos Loses Dutch ID Disclosure Case," *The Register*, 25 November 2005, at http://www.theregister.com/2005/11/25/lycos_lose_iddisclosure/.

⁵⁷ *Id.*

anonymous whistleblowers who want to put up a website and speak out without reprisal.⁵⁸

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Interception of communications is regulated by the Criminal Code and requires a court order.⁵⁹ The intelligence services do not need a court order for interception, but obtain their authorisation from the Minister of the Interior. The Special Investigation Powers Act, which came into effect in February 2000, streamlines criminal investigatory methods.⁶⁰ A Telecommunications Act was approved in December 1998, and requires all telecommunications providers to have the capability to intercept all traffic (phone and Internet) when presented with a court order.⁶¹ The Netherlands Radiocommunications Agency is responsible for enforcing the wiretap capabilities of the telecommunications sector.⁶² The ISP XS4ALL launched a court case in March 2005 against the Dutch State, seeking compensation for the cost of making its network ready for wiretaps. XS4ALL considered it unreasonable that these costs are not reimbursed because the investment is made purely in the interest of law enforcement and does not benefit the ISP in any way. According to XS4ALL, the law requiring providers to pay for the costs of wiretapping is a violation of property rights and an obstruction to freedom of speech. Moreover, the cost division also violates the principle of equal discharge of public burdens and European rules on free movement of services.⁶³ In a decree, the government ordered a dramatic reduction in cost reimbursement to telecommunications companies for the handover of personal data or wiretaps.⁶⁴ As of 1 April 2005, the companies only receive €13 for a wiretap and €6.75 for an extensive investigation into historical traffic data.

⁵⁸ *Id.*

⁵⁹ Article 125m of the Code of Criminal Procedure.

⁶⁰ See Ministry of Justice Fact Sheet, Special Powers of Investigation Act, 8 August 2006, available at <http://english.justitie.nl/currenttopics/factsheets/>.

⁶¹ Telecommunications Act 1998.

⁶² Home Agentschap Telecom homepage <http://www.agentschap-telecom.nl/>.

⁶³ XS4ALLI subpoena, English translation available at <http://www.xs4all.nl/nieuws/pdf/XS4ALLdagvaarding-en.pdf>.

⁶⁴ Ministry of Economic Affairs, Decree on Cost Reimbursement for Legal Access to Telecommunications, 1 April 2005, in Dutch at http://www.bof.nl/docs/OPT_Concept_regeling_aftapkosten_23_maart_2005.pdf.

The Intelligence and Security Services Act also authorises the interception, search, and keyword scanning of satellite communications.⁶⁵ It allows intelligence services to store intercepted communications for up to one year. Previously, irrelevant communications had to be deleted immediately. Encrypted data can be stored for an unlimited time to facilitate possible decryption in the future. In 2003, the National SIGINT Organisation (NSO) was established. The NSO operates all satellite communications interception by the Dutch intelligence services. The interception capabilities expanded from two satellite dishes at *Zoutkamp* to 20 dishes at *Burum*.

Over the past few years there have been several proposals to grant law enforcement increased authority. In 2001 the Mevis Committee issued a report proposing a wide range of increased powers for police to allow them to carry out "proactive investigations" (*verkennend onderzoek*). For the purpose of determining crime patterns, the proposals would grant police access, without the need to obtain judicial warrants, to the personal information of whole groups of citizens stored by a wide variety of private entities such as banks, telephone companies, credit card companies, hospitals, and travel agents.⁶⁶ The Mevis Committee specifically recommended that telecommunications data be excluded from the constitutional right to confidential communications, stating that it should not always be necessary for police to obtain a warrant to intercept communications.⁶⁷ A draft law incorporating the Mevis proposals (*Wet vorderen gegevens*) passed the House of Representatives in 2005. The Federation of Organisations of Libraries (FOBID) asked the Senate in an April 2005 letter not to pass the law, fearing that allowing law enforcement to seize library records would create a chilling effect on the use of libraries.

In May 2008, the Dutch police issued an oral press release stating that it would launch a pilot project to look for criminals on the Dutch social networking site *Hyves*.⁶⁸ The 'Team Digital Expertise' developed software that profiles the social network on which a suspect operates. This software will first be tested on police officers. If the pilot succeeds, a national roll-out of the software will be considered. Alongside this pilot, regional police departments have launched their own initiatives to use *Hyves* as a platform to gather crime-related information. The police department of IJsselland created a profile on *Hyves* to obtain information on a double homicide in a remote area of the region.⁶⁹ Because the police obtained essential information to solve the case from *Hyves*, the department

⁶⁵ Stb. 2002, 148.

⁶⁶ Jelle van Buuren, "Dutch Law Enforcement Should Get Easier Access to Personal Data Stored by Companies," *Telepolis*, 21 May 2001.

⁶⁷ Report of the Mevis Commission, May 2001.

⁶⁸ Novum, "Politie spoort criminelen op via Hyves" ("Police Finds Criminals via Hyves"), *Trouw*, 21 May 2008.

⁶⁹ *Algemeen Dagblad*, "Politie gebruikt Hyves bij opsporing criminelen" ("Police Uses Hyves to Track Down Criminals"), 12 August 2010, in Dutch at <http://www.ad.nl/ad/nl/1000/Nieuws/article/detail/504458/2010/08/12/Politie-gebruikt-Hyves-bij-opsporing-criminelen.dhtml>.

decided to start a joint venture with *Hyves* to use the website to find information to help in solving cases and look for missing persons.⁷⁰ This website contains information about suspects and missing persons.⁷¹

The CBP, in collaboration with the Ministry of Justice and the Ministry of the Interior and Kingdom Relations, has researched the appropriate balance between the effort to achieve a safe society and the effort to safeguard the right to privacy.⁷² Further research and investigation will take place when the police tap telephone calls in the context of criminal investigations, particularly when conversations between lawyers and their clients are recorded.⁷³ The CBP maintains that these "conversations with holders of confidential information entitled to privilege must be erased as soon as possible."⁷⁴ The CBP investigation of the national wiretapping rooms shows that this is not generally the case and this privilege is rarely protected.⁷⁵ As a result, the Public Prosecution Service has announced that measures for the improvement of this situation will be implemented.⁷⁶

National security legislation

In August 2004, the Crimes of Terrorism Act came into force. Recruitment of fighters for the Islamic armed struggle or *jihad* and conspiracy to commit a serious act of terrorism will each be a separate, punishable criminal offence under the Act. The maximum prison sentence for crimes such as homicide, gross maltreatment, hijacking, or kidnapping will be higher if they have been committed with a "terrorist purpose." In addition, the conspiracy to commit serious acts of terrorism will be made a separate punishable criminal offence.

"At the end of 2007, at the request of the Senate, the CBP issued advice on a legislative proposal that would extend the powers that the intelligence and security services, in their efforts to combat terrorism, have to obtain data on travelling, payment traffic, and Internet use by citizens."⁷⁷ The CBP believes that the need for these measures has not been sufficiently demonstrated and considers that the consequences of this data analysis for individual citizens may outweigh the policy goals.⁷⁸

⁷⁰ *Id.*

⁷¹ "De politie zoekt" ("The Police Investigates"), 30 October 2010, at <http://depolitiezoekt.hyves.nl/?pageid=5183D0JKZ88WS88OG>.

⁷² 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.*

Data retention

In September 2004, a new Act came into force that amends the power to request telecommunications data.⁷⁹ The law (*Vorderen gegevens telecommunicatie*) enables the public prosecutor to request traffic data from providers of public telecommunications networks and services. This power may be applied when there is suspicion of a serious offence. In the event of suspicion of a criminal offence, any investigating officer can request a subscriber's personal information. A proposal to notify suspects when the subscriber's data has been requested was rejected by the Parliament. Members of the Senate questioned the scope of the powers requested and required mandatory registration of all data retrievals in order to review their proportionality and effectiveness.

On 4 April 2007, the Dutch Cabinet agreed to proposed legislation designed to implement the European Directive on Data Retention, a directive that requires member countries to set statutory retention of telephone and Internet traffic data.⁸⁰ The legislative proposal sets the retention period at 18 months, a period the Ministry of Justice says is needed to accommodate the needs of police and judicial authorities.⁸¹ The CBP has criticised the proposed legislation, saying the need for a retention period of 18 months has not been demonstrated satisfactorily.⁸² The CBP argues, "retaining historical telephone and Internet information on every citizen in the Netherlands is an extremely radical measure whose need must be demonstrated irrefutably."⁸³ The CBP has also criticised other aspects of the proposed legislation, including the categories of information that must be retained, the parameters for access to information currently in the bill, and the lack of control mechanisms for the lawful use of information.⁸⁴

On 22 May 2008, the Dutch House of Representatives passed the Telecommunications Data Retention Act (*Wet Bewaarplicht Telecommunicatiegegevens*), which amended the data retention period from 18 months in the first draft to 12 months.⁸⁵ The Act has been sent to the Senate for review. The Senate's Justice sub-committee found a lack of documentation for the necessity and proportionality of the Data Retention Act, and agreed to a hearing with an independent expert to address issues of technical feasibility. Specifically, Senators were concerned about the compatibility of the Act with Article 8 of

⁷⁹ Stb. 2004, 105.

⁸⁰ Press Release, Ministry of Justice, "Dutch cabinet: telecommunications data to be retained for one and a half years," 4 April 2007, at <http://english.justitie.nl/currenttopics/pressreleases/archives2007/-Dutch-cabinet-telecommunications-data-to-be-retained-for-one-and-a-half-years.aspx>.

⁸¹ *Id.*

⁸² Press Release, CBP, "European Directive on Data retention," 24 January 2007, at http://www.dutchdpa.nl/documenten/en_med_20070124_european_directive.shtml.

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ Dutch Telecommunications Data Retention Act 2008, available in Dutch at http://wetten.overheid.nl/BWBR0026191/geldigheidsdatum_15-08-2010.

the European Convention on Human Rights, the reimbursement of the costs for Internet Service Providers, and the security measures concerning the retained data.⁸⁶ The law⁸⁷ was approved by the Senate and went into force on 1 September 2009.⁸⁸

National databases for law enforcement and security purposes

No specific information has been provided under this section.

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

No specific information has been provided under this section.

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

In May 2004 the EU Directive on Privacy and Electronic Communications (2002/58/EC) was partly implemented by outlawing spam. Senders of commercial electronic messages will need prior consent from the email address holder. During a hearing in the Dutch Parliament in August 2003, the NGO Bits of Freedom asked for an obligation for senders to prove prior consent. An amendment including this proof of consent was added into the law. The ban on spam does not cover work email addresses, a concession made after fierce industry lobbying to prevent such a proposal. Several persons and companies have since been fined for spamming. More recently, proposals have been announced to include work email addresses in the law after the direct-marketing industry failed to agree on self-regulation regarding business-to-business e-mail marketing. The Dutch Telecom Regulator, OPTA, has been very active in banning spam sent from the Netherlands since May 2004.⁸⁹ Through the website *www.spamklacht.nl*, OPTA collects over 20,000 consumer complaints annually.⁹⁰ In 2009 OPTA initiated 68 investigations, issued 51

⁸⁶ Letter from the Dutch Senate, Justice subcommittee, 8 July 2008 <http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vhwginn7thzd/f=y.pdf>.

⁸⁷ Wet bewaarplicht telecommunicatiegegevens ("Dutch Telecommunications Data Retention Act"), 18 July 2009, available in Dutch at http://wetten.overheid.nl/BWBR0026191/geldigheidsdatum_15-02-2010.

⁸⁸ Bits of Freedom, "Wet bewaarplicht telecommunicatiegegevens van kracht" ("Data Telecommunications Data Retention Act in Force"), 30 October 2009, available in Dutch at <https://www.bof.nl/2009/10/30/wet-bewaarplicht-telecommunicatiegegevens-van-kracht/>.

⁸⁹ Cf. Gerit-Jan Zwenne, Dutch Telecoms Regulator Fights Spam, 7 BNA International World Data Protection Report 3, 10 (March 2007).

⁹⁰ Id.

warnings, and imposed several fines, with the highest of these in the amount of €250,000.

In May 2004, the Parliament passed the law on e-commerce (*Wet elektronische handel*) implementing the EU E-Commerce Directive (2000/31/EC). Under the law, hosting providers risk liability for illegal content posted by their customers. Once service providers have been notified, and the unlawfulness is "apparent," they should take immediate action to block or remove the content. There is no unified notice-and-takedown procedure in the Netherlands that implements these legal obligations.

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

On 14 July 2008, the European Data Protection Supervisor, Peter Hustinx, awarded the first European Union (EU) Privacy Seal by EuroPriSe to the Dutch search engine Ixquick.⁹¹ The European Privacy Seal ensures that Internet technology products and services comply with EU laws and regulations on privacy and data security.

Online social networks and virtual communities

In December 2008, the CBP investigated alleged illegal data collection by Advance Concepts. This company owned multiple online Web quizzes, for example for people to determine their "real age". The agency concluded that Advance Concepts used these tests to obtain personal information such as medical histories, and without the users' consent sold on the data to third parties for marketing purposes.⁹² In response to the findings of the CBP, *Advance Concepts* changed its policies and implemented an opt-in policy.⁹³

Online youth safety

With regard to personal data that is published via the Internet in the Netherlands, the CBP developed and published guidelines in order to clarify what is and is not permitted.⁹⁴

⁹¹ <http://english.justitie.nl/currenttopics/pressreleases/archives2007/-Dutch-cabinet-telecommunications-data-to-be-retained-for-one-and-a-half-years.aspx>

⁹² CBP, "Onderzoek door het College bescherming persoonsgegevens (CBP) naar de verwerking van persoonsgegevens door Advance Concepts B.V." ("Investigation into Processing of Personal Data by Advance Concepts B.V."), 15 December 2009, available in Dutch at http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf.

⁹³ "CBP: internetbedrijf Advance in overtrading" ("CBP: Internet Company Advance Breaks the Law"), De Telegraaf, 18 December 2009, available in Dutch at http://www.telegraaf.nl/digitaal/5601197/_CBP_internetbedrijf_Advance_in_overtreding_.html.

⁹⁴ Dutch DPA Publication of Personal Data on the Internet, *supra*. See also 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

Regarding minors, "the Dutch DPA takes a proactive stance in providing the rules applicable for social networking and for online marketing."⁹⁵

In March 2009, the CBP investigated the practices of youth social network site Zikle. In a letter to the site's owner, the CBP concluded that the website did not provide enough information to its users about the purposes of personal data collection and did not have enough security measures in place to restrict the publication of users' data on the Internet.⁹⁶

TERRITORIAL PRIVACY

Video surveillance

As of 2004, the use of covert video surveillance in public places requires notice. The Hidden Camera Surveillance Act 2003 (*Heimelijk Cameratoezicht*) makes it unlawful to use hidden cameras in public places without notification. The use of hidden cameras in the workplace remains lawful if there is suspicion of criminal behaviour and if workers are notified. Journalists can still use hidden cameras for their work. In April 2005, the House of Representatives passed the Camera Surveillance Act, which allows images to be retained for up to four weeks and also facilitates the use of cameras for law enforcement purposes, whereas before the main purpose of camera surveillance was keeping public order.

Location privacy (GPS, mobile phones, location based services, etc.)

In December 2007, several professors of information technology advised the government to pay explicit attention to privacy concerns when developing plans for the new pay-per-kilometre car tax system. Specific concerns included collecting more (personal) data than was technically needed to run the system and using the data for purposes other than those for which was collected.⁹⁷

In January 2010, the second Chamber committee for road and water works asked the CBP to comment on legal proposals for the pay-per-kilometre system. The new system includes two user-definable ways to collect the location: one uses a built-in device that only transmits aggregate data to the tax authority; the other option is to have a thin client

⁹⁵ *Id.*

⁹⁶ CBP, Letter of final decision regarding data collection practice www.zikle.nl, 19 March 2009, available in Dutch at http://www.cbweb.nl/downloads_pb/pb_20090324_eindbeslissing_zikle.pdf. See also CBP, "Bijlage definitieve bevindingen onderzoek naar het door Diginus via de website www.zikle.nl verzamelen en verwerken van persoonsgegevens" ("Appendix Final Findings Research by Diginus into Personal Data Collection and Processing at www.zikle.nl"), 22 September 2008, available in Dutch at http://www.nrc.nl/binnenland/article1856515.ece/Privacy_kilometerheffing_goed_regelen.

⁹⁷ Privacy kilometerheffing goed regelen' ("Privacy Aspects Pay per Kilometer Should Be Well Arranged), NRC Handelsblad, 5 December 2007, available in Dutch at http://www.nrc.nl/binnenland/article1856515.ece/Privacy_kilometerheffing_goed_regelen.

that transmits data to a trusted third party for aggregation.⁹⁸ CBP explicitly advised that data collection for payments should take place only periodically and that third-party aggregation providers should conform to strict data protection regulations,⁹⁹ in line with the CBP's advice of September 2008.¹⁰⁰

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Like all EU countries the Netherlands includes biometric information in its passport. Both fingerprints and facial images are stored in a contactless chip in Dutch passports.¹⁰¹ In January 2005, the Minister of the Interior announced plans to also store the biometric data in a central database, making it possible to identify, via fingerprints or facial recognition, people who are not carrying their passports.¹⁰² The CBP held a meeting in February 2006 to discuss the potential disadvantages of this large-scale storage of data.¹⁰³ The results of the meeting were mixed: "central collation of biometric data can on the one hand protect identities by having one central reference point, but on the other hand it can undermine that protection as a result of security risks and potential use of biometric data for other purposes."¹⁰⁴ Those present at the meeting pointed out to the government the risks of identity fraud and inadequate security associated with biometrics.¹⁰⁵

According to the CBP's 2007 Annual Report, the *OV-chipkaart* system (Public Transport Chipcard or PTC) infringes Dutch Data Protection Law.¹⁰⁶ In 2007 a pilot programme conducted on the Amsterdam Metro network researched the impact of the card and concluded that the *OV-chipkaart* system is being used unlawfully.¹⁰⁷ Changes were made to the technical design for data storage so that there is now a distinction between name

⁹⁸ CBP, "Advies CBP inzake wetsvoorstel kilometerprijs" ("Advice CBP Regarding Legal Proposal Pay-per-Kilometer System"), available in Dutch at http://www.cbpweb.nl/downloads_adv/z2009-01380.pdf.

⁹⁹ *Id.*

¹⁰⁰ CBP, "Het advies van 30 september 2008 inzake het wetsvoorstel kilometerprijs" ("Advice of 30 September 2008 Regarding Legal Proposal Pay-per-Kilometer System"), available in Dutch at http://www.cbpweb.nl/downloads_adv/z2008-01050_2.pdf.

¹⁰¹ Biometry in passports, page maintained by Professor of Software Security and Correctness Bart Jacobs, available at <http://www.sos.cs.ru.nl/research/society/passport/>.

¹⁰² Databank vingerafdrukken alle Nederlanders (Database Fingerprints all Dutch Citizens), Bits of Freedom, February 2005, available at http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_3.html.

¹⁰³ CBP Annual Report for the Year 2006, *supra*.

¹⁰⁴ *Id.*, at 88.

¹⁰⁵ *Id.*, at 91.

¹⁰⁶ CBP Annual Report for the Year 2009, *supra*.

¹⁰⁷ *Id.*

and address details and travel movements.¹⁰⁸ The aim of these changes is to decrease the risk that individuals' travel behaviour can be unlawfully monitored.¹⁰⁹ In 2009, the country-wide roll-out of the PTC started. The system tracks all travellers' movements (departure and end points for each leg of every journey), in most cases combined with the traveller's identity (although these data may be stored separately). It retains these data for seven years. Travellers can consult the stored data via special websites.¹¹⁰

In a 2010 investigation, the Dutch news website *Webwereld* concluded that it was not possible to travel anonymously on public transportation with a discount card (available for the elderly and students).¹¹¹ Furthermore, they found that people who hold a monthly or yearly transport pass were required to check in and out every time they entered or exited, which was not technically necessary.¹¹² When they confronted politicians, their findings drew angry reactions from the liberals, socialists, and Christian Democrats.¹¹³ Furthermore, the NGO Bits of Freedom demanded that the *OV-chipkaart* system be stopped.¹¹⁴

On 25 January 2008 the CBP warned Dutch hotels that they are breaking data protection laws by photocopying guests' passports and identification cards.¹¹⁵

In May 2008, the Article 29 Working Party, made up of representatives from all European privacy protection agencies, issued a statement on the European Commission's initiatives on intensifying border patrol, visa policy, and visa enforcement.¹¹⁶ In a letter to the Barrot Commission, the Working Group, in which the CBP participates, reacts to the increase in border controls by writing that "[a]ny general surveillance poses unacceptable risks to the

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ See <http://www.ov-chipkaart.nl/>.

¹¹¹ "CBP negeert privacyschending OV-chipkaart" ("CBP Ignores Privacy Intrusions by OV Chipcard"), *Webwereld*, 26 January 2010, in Dutch at <http://webwereld.nl/nieuws/64947/cbp-negeert-privacyschending-ov-chipkaart.html>.

¹¹² *Id.*

¹¹³ "Politiek fel over privacyschending OV-chipkaart" ("Politicians Angry about Privacy Intrusions by OV Chipcard"), *Webwereld*, 25 January 2010, in Dutch at <http://webwereld.nl/nieuws/64956/politiek-fel-over-privacyschending-ov-chipkaart.html>.

¹¹⁴ *Id.*

¹¹⁵ "Dutch Hotels Must Stop Copying Guests' Passports", *Privacy and Security Law Report*, BNA, Vol. 7, No. 4 28 January 2008.

¹¹⁶ CBP, "Volledige controle alle reizigers disproportioneel" ("Full Control All Passengers is Disproportional"), at http://www.cbpweb.nl/documenten/med_20080514_volledige_controle_reizigers.stm?refer=true.

freedom of individuals."¹¹⁷ Furthermore, the group mentioned that there has not been any evaluation of former measures that requires the intensification of border patrol and surveillance.¹¹⁸

NATIONAL ID & SMART CARDS

In January 2005, Extended Compulsory Identification Act came into force, making identification compulsory for all persons from the age of 14 with the stated goal of increasing general public safety. Many critics have claimed that the government failed to clarify the need to broaden the identification requirements. The Act is widely seen as a symbolic gesture to satisfy public concerns about security and crime, and will have huge civil liberties consequences. The Act does not require citizens to carry identification but to show it if asked to by police. No new identification card is introduced; the existing passport, European identification card, and driver licence are acceptable.

In March 2007, Justice Minister Ernst Hirsch Ballin asked authorities for their opinion of a bill expanding the use of photos and fingerprints to determine the identity of suspects and convicted persons.¹¹⁹ The bill would require all suspects to be immediately photographed and digitally fingerprinted on arrest.¹²⁰ The bill is designed to prevent suspects and prisoners from withholding their identity or hiding behind someone else's identity.¹²¹ While the bill attempts to prevent identity theft, whenever new information is collected and stored about a person new privacy concerns surface regarding access to and retention of the data.

RFID tags

The Netherlands has seen little public debate about the use of RFID technology among retailers and supermarkets until recently. The main reason is that there are very few pilot projects in stores that make use of RFID tags with unique serial numbers (such as the Electronic Product Code, EPC). ECP.NL, an e-commerce industry platform, has begun writing the first report on the privacy implications of RFID.

¹¹⁷ Article 29 Data Protection Working Party. Letter to Commission Barrot enclosing the joint comments of the Article 29 Working Party and the Working Party on Police and Justice on the Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, namely: "Preparing the next steps in border management in the European Union", COM (2008) 69 final, "Examining the creation of a European Border Surveillance System (EUROSUR)" COM (2008) 68 final, and "Report on the evaluation and future development of the Frontex Agency" COM (2008) 67 final", 15 May 2008, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp149_en.pdf.

¹¹⁸ *Id.*

¹¹⁹ Press Release, Ministry of Justice, "No Longer Possible to Hide Behind Another Person's Identity," 4 March 2007, at <http://english.justitie.nl/currenttopics/pressreleases/archives2007/-no-longer-possible-to-hide-behind-another-persons-identity.aspx>.

¹²⁰ *Id.*

¹²¹ *Id.*

Bits of Freedom has published a position paper on RFID,¹²² as has the small ChristenUnie faction in Parliament.¹²³ The CBP published a discussion document in October 2006, "in order to further stimulate the debate about the benefits and drawbacks of RFID."¹²⁴ The document discusses privacy concerns, the technology's effect on society, and general awareness of the issue.¹²⁵

BODILY PRIVACY

After a failed terrorist attack on an airplane travelling from the United States to Amsterdam's Schiphol Airport, the airport decided to buy 60 body scanners to be used to screen passengers on flights to the United States and all United Airlines flights.¹²⁶ Schiphol notes that these scanners are not body scanners, but security scanners where, "A computer analyses images instead of a human operator by means of harmless millimetre wave technology."¹²⁷

WORKPLACE PRIVACY

The CBP ruled in 2006 that in the event of a transition from one occupational health and safety service provider to another employees' records couldn't be transferred to the new service provider without a legal framework.¹²⁸ Further, the CBP did research in 2007 to determine whether a different approach is possible within the existing statutory framework.¹²⁹ The outcome was to distinguish, "...between data that is not subject to medical professional secrecy and data that is."¹³⁰ The final determination was that data that is not subject to medical professional secrecy may be transferred and data that is subject to medical professional secrecy may only be transferred under certain conditions.¹³¹

¹²² RFID position paper, Bits of Freedom, December 2004, available at <http://www.bof.nl/rfid/RFIDpositionpaper.html>.

¹²³ Report on RFID, ChristenUnie, May 2005, available in Dutch at <http://www.christenunie.nl/1/nl/library/download/19705>.

¹²⁴ CBP, "RFID: Promising or Irresponsible," October 2006, at http://www.dutchdpa.nl/documenten/en_av_29_rfid.shtml.

¹²⁵ *Id.*

¹²⁶ Schiphol Buys 60 Body Scanners, Denies Lax Security, Reuters, 4 January 2010, available at <http://www.reuters.com/article/idUSLDE6031RJ20100104>.

¹²⁷ Schiphol Airport, Security Scan at Amsterdam Airport Schiphol, at <http://www.schiphol.nl/Travellers/AtSchiphol/CheckinControl/SecurityChecksUponDeparture/SecurityScan.htm>.

¹²⁸ 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ *Id.*

HEALTH & GENETIC PRIVACY

Medical records

The CBP has been tracking the progress of the implementation of an electronic child file (the *Elektronisch Kind Dossier* or EKD) which will record a child's development and environmental indicators from birth.¹³² Bringing the EKD online for youth health care was postponed until 1 January 2008 and is not expected to become compulsory until 2010.¹³³ The CBP is particularly concerned about whether the data will be used outside the health care sector, for example to create a national reference index of young people at risk.¹³⁴

In the health sector, the CBP earlier issued an advisory on the draft legislation that introduces the electronic patient file (EPD). The CBP argues, "Making patient files available to all care providers is far too risky, partly with a view to the protection required for particularly sensitive personal data. With the exception of emergency situations, only care providers with a treatment relationship with a patient ought to have access to the record in question."¹³⁵ The first parts of the electronic patient file infrastructure are now in place, but actual access to patient files is still beyond only those providers that have a treatment relationship with patients. When balancing the usability of the system and the need to retain the confidentiality of patient records, the former still prevails, although there is a *post hoc* control mechanism enabling patients to check who accessed their files. (for more information see Guido van 't Noordende, "Security in the Dutch electronic patient record system", ACM 2nd annual workshop on security and privacy in medical and home-care systems (SPIMACS), Chicago, USA, Oct 2010.)

In February 2010, the CBP advised the Minister to regulate health insurers' access to the EPD by taking out the section that let health insurance companies access them as electronic patient file users.¹³⁶ The Minister responsible for health care implemented this advice.¹³⁷ Additionally, the CBP investigated two regional private EPD initiatives and

¹³² CBP Annual Report for the Year 2006, *supra*.

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ CBP Annual Report for the Year 2009, *supra* at 75.@@

¹³⁶ CBP, "Aanvullingen concept wijziging Besluit gebruik BSN in de zorg" ("Additions to Concept Change in Decree to Use SSN in Healthcare"), 28 May 2009, available in Dutch at http://www.cbpweb.nl/downloads_med/med_20100209_epd.pdf. See also "Advies van het College bescherming persoonsgegevens (CBP) over aanvullende bepalingen in het voorstel tot wijziging van het Besluit gebruik BSN in de zorg" ("Advice of the CBP on Additions to Concept Change in Decree to Use BSN in Health Care"), 14 July 2009, available in Dutch at http://www.cbpweb.nl/downloads_med/med_20100209_epd_bijlage.pdf.

¹³⁷ *Id.*

concluded that both were in violation of Dutch privacy law.¹³⁸ The authority found that there were no appropriate access controls to prevent doctors from looking into files of patients they were not treating, that the log files were not used to deter wrong use of personal data, and that the patients were not informed about the use of their data for the EPD.¹³⁹

In June 2009, the CBP ordered four hospitals to make periodic penalty payments, in order to force them to improve the level of security of their health data.

Genetic identification

In February 2005, the DNA Testing of Convicted Persons Act came into force. The law makes it possible to take DNA samples from all persons who are convicted of crimes carrying a maximum penalty of four years or more. The mouth swab sample will be investigated by the Netherlands Forensic Institute (NFI) in order to determine the DNA profile.¹⁴⁰

FINANCIAL PRIVACY

In March 2010, the CBP advised the Minister of Finance to include a privacy paragraph in a new legal proposal that would regulate the use of the Burger Service Number within financial institutions to prevent money laundering and terrorism. Because the proposal would govern all bank accounts in the Netherlands, the CBP said the privacy paragraph should enumerate all the specific circumstances under which financial data would be attached to a citizen's BSN.¹⁴¹

E-GOVERNMENT & PRIVACY

With regard to government usage of the Internet, in 2007, "the Dutch DPA conducted an investigation into the municipality of Nijmegen's publication of planning permission data."¹⁴² The outcome was a finding that personal data – application forms about certain properties and proposed alterations to them as well as information about applicants,

¹³⁸ CBP, "Definitieve bevindingen SPITZ Midden-Holland" ("Final Recommendations SPITZ Midden-Holland"), 18 May 2009, available in Dutch at http://www.cbpweb.nl/downloads_pb/pb_20090527_chp_gorinchem_def_bevindingen.pdf. CBP, "Definitieve bevindingen Centrale Huisartsenpost Gorinchem" ("Final Recommendations Central General Practitioners Office Gorinchem"), 18 May 2009, available in Dutch at http://www.cbpweb.nl/downloads_pb/pb_20090527_spitz_mh_def_bevindingen.pdf.

¹³⁹ *Id.*

¹⁴⁰ "DNA Samples to be Taken from Convicted Persons," Ministry of Justice, February 2005, available at <http://english.justitie.nl/currenttopics/pressreleases/archives2005/Dna-samples-to-be-taken-from-convicted-persons.aspx>.

¹⁴¹ CBP, "Wetgevingsadvies – Wet gebruik BSN in de financiële sector" ("Legal Proposal Advice – Law Regulating the Use of the BSN in the Financial Sector"), 23 March 2010, available in Dutch at http://www.cbpweb.nl/downloads_adv/z2010-00096.pdf.

¹⁴² 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

including their signatures – was published.¹⁴³ The CBP concluded that "...the municipality may only publish compulsory data on the Internet on the property in question and the alterations proposed," and not individuals' personal data.¹⁴⁴

To date, the public law requirement on the assignment of Internet and personal data, does not justify a situation where an administrative body automatically publishes all data on the Internet.¹⁴⁵

Many countries, including the Netherlands, have discussed or implemented electronic means for voting in elections. Usually the manipulation of election results, either by insiders (i.e., manufacturers) or outsiders (i.e., hackers) is a concern. The Dutch debate on electronic voting also has prominent privacy features.¹⁴⁶ Machines began replacing ballot boxes in most precincts in the early 1990s. Controversy was initiated in 2006 by a pressure group. Besides concern about the opportunities afforded by electronic voting to manipulate election results, researchers found that the machines produced radiation that could be captured with an antenna, thereby revealing the voter's choice.¹⁴⁷ The latter issue gave both the government and the pressure group a means of legally framing the problem, as election legislation provides for a secret ballot (Dutch Constitution, Art. 53.2; Election Law, Art. J 15), but not for verification of election results. This led first to the suspension of one type of voting machine, and finally, in 2007, to the withdrawal of the approval regulation, and thereby the abolition of all voting machines. In 2008, an expert group concluded that even with a printed ballot allowing voter verification (as proposed by the Election Process Advisory Commission, 2007),¹⁴⁸ the privacy problems could not be solved as long as any electronic device was used to select the candidate and/or cast the vote.¹⁴⁹ This shows that the secret ballot is seen as an important aspect of privacy.

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

¹⁴⁶ Wolter Pieters. *Combatting Electoral Traces: the Dutch Tempest Discussion and Beyond, E-Voting and Identity: Second International Conference, VOTE-ID 2009, Lecture Notes in Computer Science 5767*, Springer Verlag, 172-190 (2009), available at http://dx.doi.org/10.1007/978-3-642-04135-8_11.

¹⁴⁷ See R. Gonggrijp, W.-J. Hengeveld, A. Bogk, D. Engling, H. Mehnert, F. Rieger, P. Scheffers, and B. Wels, *Nedap/Groenendaal ES3B Voting Computer: a Security Analysis*, 6 October, 2006, at <http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf>.

¹⁴⁸ Election Process Advisory Commission, *Voting with Confidence*, 27 September 2007, at http://www.kiesraad.nl/nl/Overige_Content/Bestanden/pdf_thema/Pdf_voor_Engelse_site/Voting_with_confidence.pdf.

¹⁴⁹ See Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. *Vaststelling van de begrotingsstaten van het ministerie van binnenlandse zaken en koninkrijksrelaties (VII) voor het jaar 2008*; brief staatssecretaris met oordeel kabinet over uitkomsten nader onderzoek naar haalbaarheid stemprinter en stemmenteller (Letter from Deputy Minister with Government Judgement on Results of Further Study on Feasibility Ballot Printer and Vote Counter), *Kamerstuk* 2007-2008 31200 VII, nr. 64, Tweede Kamer, 21 May 2008, available at <http://wijvertrouwenstemcomputersniet.nl/images/c/c5/KST118412.pdf>.

Similarly, allegations that an election advice service provider was storing political preferences alongside IP addresses raised discussion.¹⁵⁰

In April 2010, the CBP responded to a letter from the director of Dutch government IT inquiring about the legality of the usage of the BSN by the Dutch government. Although the director concluded that this usage was legal in all cases, the CBP held that the usage is illegal because the law states that government bodies can only use the BSN if it is legally required for executing their task.¹⁵¹

OPEN GOVERNMENT

The Government Information (Public Access) Act of 1991 is based on the constitutional right of access to information. It creates a presumption that documents created by a public agency should be available to everyone. Information can be withheld if it relates to international relations of the state, the "economic or financial interest of the state," investigation of criminal offences, inspections by public authorities, or personal privacy. However, these exemptions must be balanced against the importance of the disclosure. Requesters can appeal denials to an administrative court, which renders the final decision.¹⁵²

OTHER RECENT FACTUAL DEVELOPMENTS

There have been some recent developments with regard to privacy and work and social security. In one recent project, the Waterproof project, old-age pensioners and recipients of social assistance benefits in 65 municipalities in Friesland, Groningen, and Drenthe were checked for fraud based on data concerning their water consumption and the water contamination surcharge.¹⁵³ The CBP investigated, found the computer files had been linked to water data, and ruled it unlawful.¹⁵⁴ As a result of this ruling, the Social Security and Investigation Service (*Sociale Inlichtingen en Opsoringsdienst*, SIOD) is now working on the development of risk analyses using Privacy-Enhancing Technology (PET).¹⁵⁵ Here, two goals are served: combating fraud and protecting personal data.

Another way of uncovering benefit fraud is through social security investigators. The CBP has laid down an efficient process for spotting illegal activity involving personal

¹⁵⁰ Bart Jacobs and Wouter Teepe, Raar dat stembulp alles van u weet (Strange that Voting aid Knows All About You). *Volkskrant*, 5 March 2007, at <http://repository.ubn.ru.nl/bitstream/2066/36383/1/36383.pdf>.

¹⁵¹ CBP, "BSN in bedrijfsvoering" ("BSN in [government] operations"), 26 January 2009, available in Dutch at http://www.cbweb.nl/downloads_med/med_20100427_gebruik_bsn_in_bedrijfsvoering_overheid.pdf.

¹⁵² Available at http://freedominfo.org/documents/NL%20public_access_government_info_10-91.pdf.

¹⁵³ 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

data connected with these activities.¹⁵⁶ Research completed in 2006 showed that compliance with the obligation to inform citizens of the fact that they had been observed was at best fleeting. Accordingly, the process description was tightened up in 2007.¹⁵⁷

At the end of 2007, the Netherlands decided to simplify the use of BCRs (Binding Corporate Rules) in outsourcing.¹⁵⁸ "The authority is developing an approach whereby a permit will be granted to a multinational company acting as a processor on behalf of its affiliates in countries without adequate data protection laws." The processor applies for a permit on the behalf of the controllers it works for.¹⁵⁹ The application is required to include practical examples of the kind of data processing involved.¹⁶⁰ "Companies then need to submit, every six months, an updated list of the controllers whose data the company processes to the Netherlands Data Protection Authority."¹⁶¹

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

The Bits of Freedom NGO initiated the Dutch Big Brother Awards in 2002.¹⁶² In January 2006, Bits of Freedom organised the fourth annual Dutch Big Brother Awards.¹⁶³ The group gave a negative Big Brother Award to Dutch Minister for Integration and Immigration Rita Verdonk because she supplied the status of rejected asylum seeker applicants to their country of origin.¹⁶⁴ She also repeatedly denied her actions in Parliament and attempted to minimise the impact of the information she gave.¹⁶⁵ A positive award was given for the first time to Hans Franken, a professor of Law and Information Science at the University of Leiden and member of the Senate for the Christian-democrat party, for his consistent resistance in the Senate to mandatory data retention.¹⁶⁶

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ Netherlands simplifies use of BCRs in outsourcing, Privacy Laws and Business: Data Protection and Privacy Information Worldwide, December 2007), at 24.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.*

¹⁶¹ *Id.*

¹⁶² "Privacyprizen schoppen tegen Nederlandse consensuscultuur" ("Privacy prizes against Dutch consensus culture," Netkwesties, 21 February 2002, in Dutch at <http://web.archive.org/web/20080504100555/http://www.netkwesties.nl/editie31/artikel2.html>.

¹⁶³ Big Brother Award for Dutch Immigration Minister, 28 January 2006 http://www.bigbrotherawards.nl/index_uk.html.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.*

¹⁶⁶ *Id.*

Bits of Freedom ceased its activities on 1 September 2006, after six years of successfully defending digital civil rights.¹⁶⁷ Nonetheless, its former members organised the 2007 Dutch Big Brother Awards, awarding the 2007 prize in the individual category to the Dutch citizen.¹⁶⁸ When people are asked about government surveillance and data mining, many people respond by declaring: "I've got nothing to hide." This attitude is the major threat to privacy in the Netherlands.¹⁶⁹ In the corporate category, the prize was granted to the Dutch National Railroad (NS) because of its proposal for the OV Chip Card. In the government category, the Dutch Central Bank (DNB) won because of its cooperation in the extra-legal transfer of Dutch financial records to American law enforcement agencies via SWIFT.¹⁷⁰ In the category "proposal", the electronic child file (EKD) won the prize.¹⁷¹

In August 2009 Bits of Freedom reformed. It strives to influence legislation and self-regulation on both the national and European levels.¹⁷²

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

The Netherlands has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and its First Optional Protocol, which establishes an individual complaint mechanism.¹⁷³

The Netherlands is a member of the Council of Europe (CoE) and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. It has signed and ratified the CoE's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)¹⁷⁴ and the CoE's Convention on Cybercrime.¹⁷⁵

¹⁶⁷ Bits of Freedom, at http://www.bof.nl/index_uk.html.

¹⁶⁸ Winner Dutch Big Brother Awards 2007: 'You', 9 September 2009, at http://www.bigbrotherawards.nl/index_uk.html.

¹⁶⁹ Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego Law Review, 745 (2007).

¹⁷⁰ *Id.*

¹⁷¹ *Id.*

¹⁷² See new website <https://www.bof.nl/over-ons/english/> (in English).

¹⁷³ The Netherlands signed the ICCPR and its First Optional Protocol on 25 June 1969 and ratified them on 11 December 1978. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁷⁴ Signed 7 May 1982; ratified 28 May 1993; entered into force 1 September 1993.

¹⁷⁵ Signed 23 November 2001; ratified 16 November 2006; entered into force 1 March 2007.

It is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.

* Updates to the Dutch Report published in the 2010 edition of EPHR have been provided by: eLaw@Leiden, Center for Law in the Information Society at Leiden University, The Netherlands; Wolter Pieters, Faculty of Electrical Engineering, Mathematics and Computer Science at University of Twente, The Netherlands; David Riphagen, former EPIC Fellow, The Netherlands.

KINGDOM OF NORWAY

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Norwegian Constitution of 1814 does not have a specific provision dealing with the protection of privacy.¹ The closest provision is Article 102, which prohibits searches of private homes except in "criminal cases." More generally, Article 110(c) of the Constitution places state authorities under an express duty to "respect and secure human rights."² In 1952, the Norwegian Supreme Court held that there exists in Norwegian law a general legal protection of "personality", which incorporates a right to privacy. This protection of personality exists independently of statutory authority but helps form the basis of the latter (including data protection legislation), and can be applied by the courts on a case-by-case basis.³

The Norwegian Constitution also protects freedom of speech (Article 100). Persons may not be legally liable for disseminating or receiving information, ideas, or messages if the information can be justified under the rubric of freedom of expression (i.e., the seeking of truth, the promotion of democracy, or the expression of an individual opinion) (Article 100(2)). Postal communications may be censored only within certain State institutions and by leave of a court of law (Article 100(4)).

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The processing of personal data and information in Norway was formerly governed by the Personal Data Registers Act of 1978, but this law has been replaced by the Personal Data Act of 2000 (PDA).⁴ The PDA, together with regulations issued pursuant to it,⁵ constitutes the central legislation on protection of personal data in Norway. The legislation protects the right to privacy by setting out safeguards to ensure that personal data are processed in accordance with fundamental respect for the right to privacy,

¹ The Constitution of the Kingdom of Norway, English version available at <http://www.constitution.org/cons/norway/dok-bn.html> (this URL (as of 20 July 2007) links to the text of the Constitution as it existed in 1995; more recent amendments to the Constitution, particularly to Article 100 (freedom of speech – see *infra*), are not reflected therein); the current Norwegian version (Kongeriget Norges Grundlov), with latest amendments as of 30 September 2004, is available at <http://www.lovdata.no/all/nl-18140517-000.html>.

² Lee A. Bygrave & Ann Helen Aaro, Norway, International Privacy, Publicity and Personality Laws 333 (M. Henry ed., 2001).

³ *Id.* at 340.

⁴ The Personal Data Act of 14 April 2000 No. 31, in English at <http://www.datatilsynet.no/upload/Engelsk%20lov%20ny%20utgave%20til%20publisering.pdf>.

⁵ Regulations on the Processing of Personal Data of 15 December 2000 No. 1265, in English at <http://www.datatilsynet.no/upload/Engelsk%20forskrift%20ny%20utgave%20til%20publisering.pdf>.

including the need to protect personal integrity and private life and to ensure adequate quality of personal data (PDA Section 1).

Although Norway is not a member of the European Union, the PDA was designed to bring Norwegian law into compliance with the EU Data Protection Directive 95/46/EC.⁶ The PDA covers all data that may be linked directly or indirectly to individuals.⁷ The PDA applies to both the public and private sectors, and it covers both manual and computerised registers (Section 3). As a point of departure, the PDA requires that the Data Inspectorate be notified in advance of data processing operations (Sections 31-32). In some instances, a licence must be acquired from the Data Inspectorate in order to process data. This is generally the case, for example, with the planned processing of sensitive information, such as information on racial origin, religion, or criminal record (Section 33), and with the processing of personal data by the insurance, banking and telecommunications sectors (Chapter 7 of the regulations supporting the Act).

The PDA provides strong protections for data subjects about whom data has been collected. The Act provides that all persons have a right to demand access to information that concerns them (Section 18). Also, according to the Act, all incorrect data must be corrected (Section 27), and all persons shall have the right to block their name from use in direct marketing (Section 26). The Act also restricts the flow of personal data to other countries in accordance with the rules laid down in Articles 25 and 26 of the EU Data Protection Directive (Sections 29-30). Again, similar to the EU Directive, data subjects must be informed that their personal data are being collected and of the name of the controller collecting the personal data (Sections 19-20). New in relation to the EU Directive, however, is that the Act imposes a duty of informing the subject when, on the basis of a personal profile, either the data subject is approached or contacted, or a decision directed at the data subject is made. In such a case, the data subject must be automatically informed of the data controller's identity, the data constituting the profile, and the source of these data (Section 21). Violations of the Act are punishable by fines or imprisonment (Sections 46 *et seq.*).⁸

A decision of principle by the Privacy Appeals Board in late 2002 defines the scope of the Act, specifically as it applies to human biological material such as blood samples. The board's decision overturned a Norwegian Data Inspectorate ruling on a case involving a medical researcher who wished to take human blood samples from his work at a university hospital with him to his new job.⁹ The Data Inspectorate ruled that blood samples constituted "personal information" for the purposes of the Act. On appeal, the decision was reversed by a majority of the Privacy Appeals Board, applying a view of

⁶ Bygrave & Aarø, at 336.

⁷ Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002) at 48.

⁸ See also Bygrave & Aarø, *supra*, at 339-340.

⁹ See appeal decision in case 8/2002, available at http://www.personvernemnda.no/vedtak/2002_8.htm.

"data" and "information" typical in the fields of informatics and information science. Further, the decision reflected a concern that the Act should not be radically extended in scope without such an extension being considered in Parliament.¹⁰

The Board found that audiotape recordings of a person's telephone conversation – recorded without the consent of that person by the other party to the conversation – do not fall within the scope of the PDA; such recordings *per se* could not constitute a "register" or "file" for the purposes of Section 3(1)(b), as they are not organised in a way that facilitates ready identification of specific individuals.¹¹ The board also found that the recordings could not qualify as a processing of personal data by automatic means (Section 3 (1)(a)), because manual intervention was needed to initiate and conclude the recording operation.

A decision by the European Court of Justice in the criminal proceedings against Bodil Lindqvist¹² has led to a change in policy of the Norwegian Data Inspectorate. The Inspectorate had exempted from the Act the posting of personal data on homepages for ostensibly private or domestic purposes. The *Lindqvist* decision, however, states that the exemption for "private" processing pursuant to Article 3(2) of the Data Protection Directive does not apply when the data can be accessed by an indefinite number of persons. Unless access to personal data posted on a website is restricted so that only a small number of persons can legally access the material, the disclosure of this data now falls within the scope of the Data Protection Directive and the PDA.¹³

In 2009, a chapter concerning the employer's right to examine an employee's email box, etc., was added to the Personal Data Regulations.¹⁴ Following this amendment, an employer may only explore, open, or read email in an employee's email box: when it is necessary to maintain daily operations or there is other justified interest of the business, such as in case of justified suspicion that the employee's use of email constitutes a serious breach of the duties that follow from the employment, or may constitute grounds for termination or dismissal.

The employee shall be notified wherever possible and given an opportunity to speak before the employer makes the examination, and also to be present during the examination, if possible.

¹⁰ Lee A. Bygrave, "The Body as Data? Biobank Regulation via the 'Backdoor' of Data Protection Law," 2 Law, Innovation and Technology, at 1–25 spec. 20 (2010).

¹¹ See appeal decision in case 1/2005, available at http://www.personvernemnda.no/vedtak/2005_1.htm.

¹² See decision of 6 November 2003 in Case C-101/01, *Bodil Lindqvist v Åklagarkammaren* in Jönköping, European Court Reports 2003 I-12971 § 47.

¹³ *Id.*

¹⁴ Personal Data Regulations, Chapter 9.

Sector-based law

In 2007, Norway amended its Working Environment Act to add provisions for whistleblowers. Under the amendments, workers may remain anonymous.¹⁵ In addition, the businesses must handle the employee's information according to the PDA.

In January 2006, a new statute was enacted which created a central register for political parties and their candidates.¹⁶ The legislation mandates disclosure of private individuals' financial support to political parties if this support is greater than a particular amount of money (Section 20), and prohibits anonymous contributions to political parties (Section 17(2)).

2006 also brought changes to the Child Welfare Act.¹⁷ These amendments make it mandatory for employees at private crisis centres that receive funding from the government to disclose information to the Child Welfare Authorities if they have reason to believe that a child is being neglected. The Data Inspectorate was very strongly opposed to this provision and "believes that it represents a serious infringement of the integrity of persons who contact a crisis centre in an emergency situation."¹⁸ The Act was amended again in 2009 to stipulate that all government institutions and all institutions working with parents and children have to disclose information necessary for the Ministry, the Child Welfare Authorities and the Health authorities to do their duty. When life or health is at stake child welfare workers can give information to health care workers. This includes the suspicion that a pregnant woman is abusing substances that can lead to the child being born with permanent damage. But the amendment also states that parents' and children's right to privacy shall be respected while they are in an institution (Section 5-9a).¹⁹

The Norwegian Nationality Act, Section 7, was amended in 2007 to require applicants for Norwegian nationality to provide a police certificate.²⁰ The police certificate shall contain preliminary charges and indictments, even in situations where the offence was not prosecuted. However, a proposed provision that would have suspended the duty of confidence of all public authorities, and at the same time subjected them to a disclosure

¹⁵ Act of 17 June 2005 No. 62, Working Environment Act, amended by Act of 23 February 2007 No. 10, available in English at <http://www.arbeidstilsynet.no/binfil/download2.php?tid=92156>.

¹⁶ The Political Parties Act of 17 June 2005 No. 102, entry into force 1 January 2006, available in English at <http://www.ub.uio.no/ujur/ulovdata/lov-20050617-102-eng.pdf>.

¹⁷ The Child Welfare Act of 17 June 1992 No. 100, amended 1 January 2006, available in Norwegian at <http://www.lovdata.no/all/nl-19920717-100.html>.

¹⁸ The Data Inspectorate's 2006 Annual report to the EU Art. 29 Data Protection Working Party, 31 May 2007, http://www.datatilsynet.no/templates/Page_____1857.aspx.

¹⁹ *Id.*

²⁰ The Norwegian Nationality Act of 10 June 2005, amended June 2007, available in English at <http://www.ub.uio.no/ujur/ulovdata/lov-20050610-051-eng.pdf>.

requirement if the immigration authorities needed information whilst processing nationality applications, was not adopted.

A statutory protection for privacy is granted by Section 390 of the Criminal Code 1902. Section 390 provides a penalty for violations of privacy caused by "public disclosure of information relating to personal or domestic affairs".²¹

DATA PROTECTION AUTHORITY

Monitoring and enforcement of the PDA is overseen by The Data Inspectorate (*Datatilsynet*), a body originally set up in 1980.²² The Inspectorate is placed under the administrative wings of the Ministry of Government Administration, Reform, and Church Affairs, but is otherwise expected to function completely independently of government or private sector bodies. The Inspectorate is generally regarded as an important institution in Norwegian society.

The responsibilities of the Inspectorate include verifying compliance with statutes and regulations that apply to the processing of personal data and verifying that errors or deficiencies are rectified; identifying risks to protection of privacy; and providing guidance on measures to avoid or limit such risks.²³ The Inspectorate also plays a role in raising public awareness of privacy through various campaigns and publications.²⁴

Complaints are normally handled by written procedures, but also by guidance meetings, by phone calls, and by email. In terms of complaints enforcement, the Data Inspectorate has the tools mentioned in PDA Sections 47-49. Decisions of the Inspectorate may be appealed to a quasi-judicial body, the Privacy Appeals Board (*Personvernneemnda*). Decisions of the Privacy Appeals Board may be appealed to civil courts on questions of law.²⁵

The Inspectorate has the power to make onsite visits to data register licencees to determine compliance with the PDA (Section 44). The Data Inspectorate also has the authority to issue fines. Physical persons may only be fined for a data offence involving deliberate or negligent violation. The Data Inspectorate may also impose a coercive fine which will run for each day from the expiry of the time limit set for compliance with the order until the order has been complied with.²⁶

The Data Inspectorate is responsible for the service/website *slettmeg.no* (delete me), which provides assistance to persons that have found information about themselves on

²¹ Bygrave & Aarø, *supra*, at 334.

²² See the Data Inspectorate's homepage, *supra*.

²³ *Id.*

²⁴ See for example http://www.datatilsynet.no/templates/Page____140.aspx.

²⁵ Bygrave & Aarø, at 337.

²⁶ *Id.*

the Internet which they need help to remove (for example taking down the Facebook account of a relative that has died). The establishing of this service was a result of a suggestion from the Privacy Commission, which was appointed by the Government in 2007 and submitted its final report in 2009.²⁷

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In June 2010 the Norwegian Supreme Court ruled in the case between Lyse Tele (Altibox) and Sandrew Metronome²⁸ on the disclosure of the identity of a subscriber with a given IP address at a given time. The subscriber had made available copyrighted material belonging to Sandrew Metronome, but they were not able to take out a law suit in a civilian court without the identity of the file-sharer. The Post and Telecommunications Authority exempted Lyse Tele's professional secrecy in the case, but Lyse Tele claimed that this was not enough. The Court of Appeal ruled that Lyse Tele would have to provide Sandrew Metronome with the identity of the file-sharer in this case, but that they should not be given access to his equipment as they had asked in order to secure evidence. Both parts appealed to the Supreme Court, but the appeals were rejected.

In 2007 a book on local history from life on a group of farms in the South of Norway was published. The author describes life on his own farm, including his divorce. His ex-wife subsequently sued to have the description of the divorce removed from the book. The case made its way to the Supreme Court, which ruled in favour of the author.²⁹ The judges emphasised the consequences for biographies and history works if the author were convicted. They stressed, too, that it is the author's own story that is told. As long as the descriptions are not incriminating, intimate or untrue, the ex-wife had no right to be protected from her former husband's description of their divorce.

Another relatively recent Supreme Court ruling of note concerned a suit instigated by an American snowboarder, Andy Finch, who claimed damages for the unauthorised use of a photograph of himself by a Tromsø-based organisation that had used the photograph as part of a campaign to promote Tromsø as a suitable venue for holding the Winter Olympics.³⁰ A problem for Finch was that while damages for unauthorised use of personal photographs are available under copyright legislation, such damages may only

²⁷ Government White Paper, NOU 2009:1 Individ og integritet (Individuals and Integrity), available at <http://www.regjeringen.no/pages/2143156/PDFS/NOU200920090001000DDDPDFS.pdf>.

²⁸ Norwegian Supreme Court, Case No 2010/226, "Begjæring om bevissikring utenfor rettssak" ("Request for the Securing of Evidence Outside of the Court"), available in Norwegian at http://www.domstol.no/DAtemplates/Article____23918.aspx?epslanguage=NO.

²⁹ Norwegian Supreme Court, Case No. 2009/1047, "Spørsmål om krenkelse av privatlivets fred ved utgivelse av lokalhistorisk bok" ("Question Regarding Violation of Privacy by the Publishing of a Book on Local History"), available at http://www.domstol.no/DAtemplates/Article____22343.aspx?epslanguage=NO.

³⁰ Norwegian Supreme Court case No. 2009/2318-A, reported in Norsk Retstidende (Norwegian Law Reports) 2009, at 1568.

be awarded to residents or citizens of Norway – and Finch did not fall into this category of persons. However, the Supreme Court upheld Finch's claim by finding that there exists a right to control the use of one's personal image in photographic form that is independent of statute and that this right inheres not just in residents or citizens of Norway. In making this finding, the Court relied on older case law, notably its famous decision of 1952 referred to at the beginning of this report.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Wiretapping normally requires the permission of a court and is initially limited to four weeks.³¹ Provisions of the Criminal Procedure Act allow for wiretapping in two circumstances. First, Section 216(a) allows wiretapping for narcotics investigations and in connection with cases involving national security, albeit with the permission of a magistrate court. Second, Section 216(b) allows wiretapping in connection with some less serious offences but requires the permission of a magistrate court. A Supervisory Board reviews the warrants to ensure the adequacy of the protections. This board also has detailed statistics on the use of wiretapping (number of cases, what type of method, how many phone numbers, IMEI number, network addresses, what police units were responsible, and what results came from or are expected to come from the investigation),³² but these are not available to the public. However, according to Section 216(d) of the Criminal Procedure Act, the prosecutor can permit interception without court order in urgent cases.

In 2009 the Government appointed a new Control Committee for Wiretapping. Its mandate is to control that the police use of wiretapping is within the framework of the law and that the use of such methods is as limited as possible.³³ The Committee publishes a yearly report on the number of times, in what type of cases and under what legal provision wiretapping has been used.³⁴

³¹ See generally Criminal Procedure Act, Chapter 16 a.

³² Regulation of 31 March 1995 No. 281, Forskrift om kommunikasjonskontroll (Regulation of Communications Control), § 10, available at <http://www.lovdata.no/for/sf/jd/td-19950331-0281-001.html#10>.

³³ The Ministry for Justice and the Police, "Nytt kontrollutvalg for kommunikasjonskontroll" ("New Control Committee for Wiretapping"), 19 June 2009, available at <http://www.regjeringen.no/nb/dep/jd/aktuelt/nyheter/2009/nytt-kontrollutvalg-for-kommunikasjonsko.html?id=567915>.

³⁴ Kontrollutvalget for kommunikasjonskontroll, Årsrapport 2009 (Annual report 2009), available at <http://www.regjeringen.no/upload/JD/rapport.pdf>.

The Criminal Code³⁵ first prohibited the publication of information relating to "personal or domestic affairs" in 1889.³⁶ The Criminal Code of 1902 also prohibits the unauthorised opening of sealed correspondence, including cracking security mechanisms.³⁷ It further prohibits covert monitoring or recording of telephone conversations or other conversations in closed settings.³⁸

A Parliamentary Commission of Inquiry was created in 1994 to investigate the post-World War II surveillance practices of Norwegian police and security services. The Lund Commission delivered a 600-page report in 1996, causing a great deal of public and political debate on account of its finding that much of the undercover surveillance practices, including wiretapping of left-wing political groups until 1989, had been instituted and/or conducted illegally and that the courts had not generally been strong enough in their oversight.³⁹ This included keeping files on children as young as 11 years old. Legislation to monitor the secret services was approved in 1995 following the Lund Commission's recommendations.⁴⁰ The legislation created a new Control Committee to monitor the activities of the Police Security Services, the Defence Security Services, and the Defence Intelligence Services. The Control Committee publishes an annual report to the Parliament.⁴¹

In April 2002, the Norwegian Parliament adopted amendments to the Norwegian Penal Code, which include prohibitions against "terrorist acts."⁴² Many privacy advocates and non-governmental organisations have expressed concern that the prohibition against "terrorist acts" is too broad and imprecise, and may result in persons becoming victims of arbitrary, inaccurate, or politically motivated charges.⁴³

A report from a government-appointed commission tackled the controversial issue of balance between crime prevention and privacy in the light of global terrorism and

³⁵ See generally Bygrave & Aarø, *supra*, at 334-335.

³⁶ See Prof. Dr. Juris Jon Bing, Data Protection in Norway, 1996, available at http://web.archive.org/web/20010221055602/http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html.

³⁷ Bygrave & Aarø, *supra*, at 334.

³⁸ *Id.*

³⁹ "Judicial Inquiry into Norwegian Secret Surveillance," Fortress Europe Circular Letter (FECL) 43 (April/May 1996), available at <http://www.fecl.org/circular/4305.htm>.

⁴⁰ Act of 3 February 1995 No. 7 on the Control of the Secret Services.

⁴¹ Annual reports for 2007 and 2008 available in English at <http://www.eosutvalget.no/hXGXCTgZfK5R.35.idium>.

⁴² International Helsinki Foundation (IHF) Report, "Human Rights in the OSCE Region: Europe, Central Asia and North America 2003 (Events 2002)", at http://web.archive.org/web/20071030105402/http://www.ihf-hr.org/viewbinary/viewdocument.php?doc_id=2261.

⁴³ *Id.*

organised crime.⁴⁴ In response, Norway passed a law that makes it easier for the police to use bugging of non-telephonic conversations between criminals, a practice known as "romavlytting" in Norwegian, and other means of covert investigation.⁴⁵

In 2009 a government commission appointed to evaluate the use of such covert methods delivered its report.⁴⁶ The conclusion is that most of the methods seem to be used as intended and that they have an effect in a significant amount of the cases used (40 to 50 percent of the cases). The commission also states that the number of cases where the police use covert methods have been stable over the last years, and that such methods are mainly used in drug cases, which is in line with Parliament's intention. One of the Commission's main concerns is that irrelevant conversations of a private character are often picked up. They also state that better statistics on the use and effect of the different methods would make it easier to review the effectiveness, and – following this – the appropriateness of the methods.

National security legislation

All information relating to national security legislation is found under other sections of this report.

Data Retention

The Data Retention Directive has not yet been implemented into Norwegian Law. There is much debate on the matter, both in public and within the ruling coalition. Within the coalition the Labour Party is in favour of implementing the directive, while the Socialist Left Party and the Centre Party oppose it. The Ministry of Transportation and Communication and the Ministry of Justice and the police have sent a proposal for an implementation of the directive on a wide national hearing.⁴⁷ To try to involve the general public in the debate, the Minister for Transport and communication has created a blog dedicated to the hearing.⁴⁸ It is believed that no formal proposal will be made to Parliament until the EU's evaluation of the directive – which is supposed to take place in autumn 2010.

⁴⁴ Government White Paper, NOU 2004:6 Mellom Effektivitet og Personvern (Between Efficiency and Privacy).

⁴⁵ The Norwegian Ministry of Justice and the Police (2005), Ot.prp nr. 60 (2004-2005), Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet) (About the Act on Changes to the Criminal Procedure Act and the Police Act (Use of Covert Methods to Prevent Serious Crime), available at <http://www.regjeringen.no/Rpub/OTP/20042005/060/PDFS/OTP200420050060000DDDPDFS.pdf>.

⁴⁶ Government White Paper, NOU 2009:15 Skjult informasjon – åpen kontroll (Hidden Information – Open Control), available (with summary in English) at <http://www.regjeringen.no/nb/dep/jd/dok/nouer/2009/nou-2009-15.html?id=569379>.

⁴⁷ The Norwegian Ministry of Transport and Communications, "Hearing letter", available at http://www.regjeringen.no/pages/2281081/hnotat_datalagring.pdf.

⁴⁸ At <http://datalagringsdirektivet.wordpress.com/>.

Currently, the telecommunications providers are only allowed to store data as long as they need it to provide their service.⁴⁹ This means that data is stored for billing purposes for three to five months (depending on how often the customer is billed). For Internet traffic data, the providers have to delete the communications data after three weeks. The police can get access to the data available if it is necessary for an investigation. Permission for this can currently be given by the Norwegian Post and Telecommunications Authority in the form of an exemption from professional secrecy.⁵⁰

National databases for law enforcement and security purposes

Norway created a database of asylum seekers that contains biometric information such as fingerprints.⁵¹ This database was opened to the police for use in criminal investigations even though the original intent of the database was to help establish the identity of asylum seekers.⁵²

In 2008 the police's storage of DNA samples was extended to everyone who is convicted to a prison sentence.⁵³ Previously only felons in cases of murder, violent crimes, and serious crimes related to narcotics had to give up their DNA. One year later the number of registered profiles has increased by 40 percent to 16,600.⁵⁴ According to numbers from the Ministry of Justice and the Police, around half of the DNA samples that are registered during criminal investigations match DNA profiles already in the register.

Currently, legislation related to different police databases is very fragmented. The Government has proposed to collect all legislation connected to such databases in a separate Act – the Police Register Act.⁵⁵ The Act is sanctioned by Parliament but not yet implemented into law. The Act specifically mentions the following police databases (Chapter 3):(1) the "Reaction register", containing information on physical persons or legal entities who have been sentenced for breaking the law; the information registered is personal, such as name and address and what disposition was made in regards to the

⁴⁹ The Electronic Communications Act of 4 July 2003 No. 83, Section 2-7, Unofficial English translation available at http://www.npt.no/ikbViewer/Content/ekom_eng.pdf?documentID=7922.

⁵⁰ Regulation of 10 November 1997 No. 1156, available at <http://www.lovdata.no/for/sf/dl/sd-19971110-1156.html>.

⁵¹ Data Inspectorate, 2005 Annual Report to the EU Art. 29 Data Protection Working Party, 3 October 2005, available at http://www.datatilsynet.no/templates/Page_____1383.aspx.

⁵² The Norwegian Ministry of Local Government and Regional Development (2003), Rundskriv H19/03: Ikrafttredelse av endringer i utlendingsloven og utlendingsforskriften (Effectuating the Changes to the Immigration Act and the Immigration Regulation).

⁵³ Regulation of 28 June 1985 No. 1679, § 11a-1, amended 1 September 2008, available at <http://www.lovdata.no/for/sf/jd/xd-19850628-1679.html#11a-1>.

⁵⁴ The Norwegian Ministry of Justice and the Police, "Økt bruk av DNA for å oppklare mer" ("Increased Use of DNA to Solve More Cases"), at <http://www.regjeringen.no/nb/dep/jd/tema/kriminalitetsbekjempelse/dna-register/-faktaark-okt-bruk-av-dna-for-a-opplare-.html?id=525398>.

⁵⁵ Act of 28 May 2010 No. 16, available in Norwegian at <http://www.lovdata.no/all/hl-20100528-016.html>.

offence they were convicted of (*e.g.* prison sentence, fines, *etc.*); (2) the "Journal", that is, a running record of all activities at a local police station; (3) The "Criminal Investigations register"; (4) the "DNA register", consisting of four parts: the "Identity register" with the DNA profile of everybody sentenced for a crime that qualifies for a prison sentence; the "Investigation register", with all DNA-material collected from persons suspected of a crime that may lead to a prison sentence (if they are convicted, the material will be transferred to the Identity register); the "Trace Evidence register" with DNA from unknown persons that may be of importance to an unsolved case; the "Elimination register" with information on people working in the police and other institutions who are often in contact with crime scenes and evidence; (5) The "Fingerprinting and Photo register", containing the fingerprints and photo of anyone suspected of a crime that may lead to a prison sentence. As with DNA, the police can also maintain an "Elimination register" of the fingerprints of people working in the police and other institutions who are often in contact with crime scenes and evidence.

The new Act has general chapters on how to deal with the information (purpose binding, relevance, data quality – Chapter 2), information security (Chapter 4), access to the information (Chapter 5), limits on professional secrecy (Chapter 6), duty to notify the data subject (and the subject's right to review the information – Chapter 8), deletion of information that is no longer needed (Chapter 8), and the data subject's right to protest a registration (Chapter 9).

The Data Inspectorate previously had a right to perform inspections in all databases with personal information, with the exception of the police databases. The new Act states that the Data Inspectorate also has a right to inspect the police's systems.⁵⁶

National and international data disclosure agreements

Norway has signed the Schengen agreement and will implement SIS II, the new Schengen Information System which allows for more extensive exchange of data among member countries.⁵⁷ Norway has also signed the Eurodac agreement⁵⁸ and the Prüm treaty.⁵⁹

⁵⁶ *Id.*, Chapter 10.

⁵⁷ PRISE 2006, "Overview of Security Technologies", available at http://teknologiradet.no/PRISE_rapport_engelsk_for_web_00fBh.pdf.file for a brief overview of the system.

⁵⁸ *Id.*

⁵⁹ Brief description at <http://www.eurocop-police.org/policies/policing%20europe/07-03-09%20FACT%20SHEET%20Prum%20Treaty.pdf>.

Cybercrime

Norway signed the Convention on Cybercrime in 2001. The necessary changes to comply with the convention were implemented into Norwegian law in 2005.⁶⁰

The National Criminal Investigation Service (NCIS or *Kripas*), together with the ISP Telenor, has developed a filter to contribute to limiting the distribution of child pornography. The Child Sexual Abuse Anti Distribution Filter is in use by most Norwegian ISPs. The filter contains a list of domain names compiled by *Kripas*. When a user tries to access one of these domains, the filter instead returns a warning page informing the user that he/she has tried to access a page with content that is illegal under Norwegian law. The page also says that the user has not been logged, and that there will be no follow-up.⁶¹ The filter has been debated on the grounds that it exists outside judicial control – it is maintained by *Kripas*, and there is no official list of the domains on it. There is, however, an opportunity to complain to *Kripas* if you are redirected to the stop-page while trying to access a domain with legal content.

In August 2008, the Minister for Justice and the Police, Knut Storberget, sent a letter to all ISPs encouraging them to implement the filter. He also states that the Government is considering making the filter compulsory, and the extent to which his request is followed will be a factor in this decision.⁶² The news generated some debate at the time, as Internet filtering is not presently incorporated into any Norwegian law. During a later debate about preventing Norwegians from gambling on Internet sites hosted abroad, the Minister for Culture, Trond Giske, stated that a filtering solution was out of the question, as this would threaten freedom of expression.⁶³

Critical infrastructure

NorCERT (Norwegian Computer Emergency Response Team) coordinates work preventing and responding to IT security breaches aimed at vital infrastructure in Norway. NorCERT is a department of the Norwegian National Security Authority (*Nasjonalt sikkerhetsmyndighet* or NSM). Since 2000, NorCERT has run the Early Warning System for Digital Infrastructure (*Varslingssystem for digital infrastruktur* or VDI) in Norway. VDI has break-in detection sensors on the Internet and at some major

⁶⁰ Government White Paper, NOU 2007:2 Lovtiltak om datakriminalitet (Legal Actions against Computer Crime), available at <http://www.regjeringen.no/pages/1937086/PDFS/NOU200720070002000DDDPDFS.pdf>.

⁶¹ See Kripas' home page, at <https://tips.kripas.no/cmssite.asp?c=1&h=41&menu=2>.

⁶² The letter has been leaked to Wikileaks, at http://www.wikileaks.org/wiki/Norway%27s_Knut_Storberget_tells_ISPs_to_deploy_secret_censorship_lists,_29_Aug_2008.

⁶³ Mads A. Andersen, "For drastisk å sperre internett" ("Blocking the Internet is Too Drastic"), *VG Nett*, 22 September 2008, at <http://www.vg.no/nyheter/innenriks/artikkel.php?artid=516872>.

businesses that are important for the functioning of Norwegian society.⁶⁴ According to NorCERT the VDI does not collect or store information about individual Internet users.

NorCert is the coordinating body for all major cybersecurity incidents related to Norway and the national point of contact for cyber defence.

Internet & Consumer Privacy

When the Norwegian law on property rights was amended in 2005, it was changed so that downloading material from the Internet is illegal if you have reason to believe that it has been uploaded without the permission of the owner. Uploading copyrighted material is still illegal. It is illegal to break digital copyright protection if it is "effective".⁶⁵ The background is that most of the copyright protection designed to stop people from playing and ripping CDs on a computer can be broken by holding down the "shift" key. During the debate preceding the final changes to the Copyrights Act of 1961 it was argued that it would not make sense to criminalise something that was easy for anyone to do and that did not really involve actual code-cracking.

The law also emphasises that private consumers should be able to play/view legally obtained works on what can be considered "relevant equipment".⁶⁶ This paragraph was added to ensure that consumers who had bought a CD could legally transfer that music to a cassette or a digital music player (iPod or mp3-player).

The property rights law is currently under revision again. The Government has appointed a working group to look into the challenges related to illegal file-sharing.⁶⁷

The International Federation of the Phonographic Industry (IFPI) has requested that Norwegian ISPs block access to known file-sharing domains such as the Pirate Bay, but so far ISPs have declined to do this. The law firm Simonsen was granted permission from the Norwegian Data Inspectorate to register the IP-addresses of file-sharers on behalf of IFPI. They were not granted permission to get the name of the user connected to that IP-address. Simonsen filed several complaints with the police, but only a few were investigated. The Data Inspectorate has since revoked the permission while awaiting clarification of the legality of private investigations by rights holders, for example, in

⁶⁴ Information from the NorCERT home page. Some information is available in English at <https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/>.

⁶⁵ Act of 12 May 1961 No. 2, amended 2009, § 53a, available at <http://lovdata.no/all/tl-19610512-002-045.html>.

⁶⁶ *Id.*

⁶⁷ The Norwegian Ministry of Culture, "Referansegruppe om ulovlig fildeling" ("Reference Group on Illegal File Sharing"), at <http://www.regjeringen.no/nb/dep/kud/tema/medier/opphavsrett/Referansegruppe-om-ulovlig-fildeling.html?id=597684>.

dedicated provisions to be inserted into the Copyright Act.⁶⁸ Simonsen appealed the Inspectorate's decision in September 2009. The Privacy Appeals Board's decision is expected at the end of 2010 or in early 2011.

E-commerce

Consumers in Norway can stop unwanted direct telephone marketing by opting out via the Central Marketing Exclusion Register at the Brønnøysund Register Centre.⁶⁹ All businesses that do direct marketing are required to remove all registrants from their list. By 2009, more than 1.7 million Norwegian consumers had opted out through this service.⁷⁰ It is also possible to get a sticker from the nearest post office to put on your mailbox to avoid direct marketing materials lacking an address. It is not legal to send out marketing emails to anyone who has not actively given consent (opt-in). Businesses may send out marketing material to customers who have done business with them previously, but only for their own goods or services in the same category as the previous purchase. A customer must be given an easy way to opt out.⁷¹

If a consumer has been subject to illegal marketing, he or she can issue a complaint with the Consumer Ombudsman.⁷² The Consumer Ombudsman has developed a series of guidelines for good marketing practice, including guidelines for e-commerce, telephone marketing and online marketing.

Under the pre-amended version of the Marketing Control Act, the Marketing Council and the Consumer Ombudsman could impose a suspended fine. This meant that the fine only had to be paid by repeat offenders. In 2009, the Act was updated to allow for an infringement fine as an alternative sanction. The fine can be issued for prior offences. However, this sanction can only be applied to cases that are in violation to clearly stated unfair practices, e.g., sending out "spam" to consumers via email.⁷³

Internet banking has very high penetration in Norway. In 2009, 85 percent of the adult (over 16) population used Internet banking. Even in the group over 65 years of age

⁶⁸ The Norwegian Data Inspectorate, "Simonsen får ikkje forlenga konsesjonen" ("Simonsen Does Not Get Extended Permission"), http://datatilsynet.no/templates/Page____2825.aspx.

⁶⁹ The Central Marketing Exclusion Register, at <http://www.brreg.no/english/registers/exclusion/exclusion.html>.

⁷⁰ The Consumer Ombudsman, "Endringer i den nye markedsføringsloven" ("Changes in the New Marketing Control Act"), 1 June 2009, at <http://www.forbrukerombudet.no/index.gan?id=11039418>.

⁷¹ Act of 9 January 2009 No. 02, Markedsføringsloven (The Marketing Control Act), available at <http://lovdata.no/all/hl-20090109-002.html>.

⁷² The Consumer Ombudsman's, homepage available in English at <http://www.forbrukerombudet.no/index.gan?id=490&subid=0>.

⁷³ All 2009 updates to the Marketing Control Act are available in English at <http://www.forbrukerombudet.no/index.gan?id=11039818&subid=0>.

penetration is 74 percent.⁷⁴ Most banks use a BankID for secure login. This type of login requires a token or a mobile phone that generates a code in addition to the customer's username and PIN. BankID can also be used as a digital signature.⁷⁵ So far, there have been very few security breaches related to Internet banking in Norway. If a customer falls victim to a security breach, the burden of proof is on the bank to show that the customer has exhibited gross negligence or wilfully tried to deceive the bank.⁷⁶

Norway implemented Directive 2007/64/EC on payment services in the internal market in 2009.⁷⁷

Cybersecurity

In 2006 a government-appointed commission delivered its report on the protection of critical infrastructure and critical societal functions in Norway.⁷⁸ One of the commission's recommendations is that all Internet service providers should be required to deliver security software as part of their service, and that all vendors of wireless networks should be required to deliver equipment with satisfactory security installations and user manuals in Norwegian.

Most Norwegian ISPs have agreed to follow a common approach to use a filter to stop both incoming and outgoing spam.⁷⁹ Customers must be informed of the filter and how it works. The ISP should have user contracts that make it possible to sanction users that distribute spam, they should provide their customers with information on how to avoid spam, and they should make it easy to report spam.

The Norwegian Centre for Information Security (*Norsk senter for informasjonssikring* or NorSIS)⁸⁰ is a Government-funded centre for information security. It targets small and medium-sized enterprises as well as public authorities and the general public. An important part of its mandate is to raise general awareness of information security matters through training and information. It also compiles and creates guidelines and tutorials

⁷⁴ Statistics Norway, "Purpose and Nature of Activities on the Internet the Last 3 months", available in English at http://www.ssb.no/english/subjects/10/03/ikthus_en/tab-2009-09-24-05-en.html.

⁷⁵ BankID's homepage, at <https://www.bankid.no/>.

⁷⁶ Act of 25 June 1999 No. 46 Finansavtaleloven (Financial Contacts Act), amended in June 2010, available at <http://www.lovdata.no/all/hl-19990625-046.html>

⁷⁷ Act 19 June 2009 No. 81, available at <http://www.lovdata.no/all/hl-20090619-081.html>.

⁷⁸ Government White Paper, NOU 2006:6 Når sikkerheten er viktigst, English summary available at http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commission_-_Report_NOU_2006_No_6_English_summary.pdf.

⁷⁹ IKT-Norge, Bransjenorm for felles innsats mot utbredelse av e-postspam (Business Norm for a Common Effort against the Proliferation of E-mail Spam), at <http://ikt-norge.no/PageFiles/348/bransjenorm%20-%20endelig.pdf>.

⁸⁰ See the NorSIS website, at <http://norsis.no/omsis/english.html>.

concerning information security topics. One example is a major identity theft project led by NorSIS with participants from several public and private organisations.⁸¹

Online behavioural marketing and search engine privacy

There are no laws against online anonymity in Norway, and the use of anonymous Virtual Private Networks (VPNs) or anonymous proxies is legal, although not very common. Norway is debating whether to implement the Data Retention Directive. Currently, ISPs are allowed to store IP addresses for three weeks to enable them to handle complaints. Previously, the storage period for this information varied depending on how long the ISP felt the information was needed. In 2009 the Norwegian Data Inspectorate instructed all ISPs that the storage of IP addresses beyond three weeks would be in violation of the Personal Data Act.⁸²

All the most common search engines used by Norwegian consumers (particularly Google) are run from other countries, and as such are beyond the control of Norwegian law.

Online social networks and virtual communities

There is very high Internet penetration in Norway – 86 percent of Norwegian households have an Internet connection, and only 11 percent have not used the Internet over the last three months.⁸³ According to TNS Gallup, in the first quarter of 2010 61 percent of Norwegian Internet users used Facebook daily or weekly, 57 percent said their communication is open on Facebook, while 40 percent were members of closed groups. Fifty-seven percent worried about privacy on Facebook.⁸⁴ Norwegians are also active on many other social networking sites, but Facebook is the most popular.

The Norwegian Data Inspectorate established the service *slettmeg.no* (delete me) in March 2010. This service offers advice and guidance to people of all ages who find offending material about themselves on the Internet. This might include photos published without permission, fake profiles on various Internet services, incorrect personal information, or harassment. The service provides guidance for removing already deleted Web pages from Google's (and other search engines') indexes, and for deleting accounts on various social networking sites, *etc.* Published statistics show that a majority of the requests received by *slettmeg.no* have been about Facebook (more than 35 percent during

⁸¹ See the project's website, with a identity theft self assessment test, available in English at <http://www.idtyveri.info/>.

⁸² Johansen, Hegtun, Haugnes, "Nettselskaper må slette dataspor" ("ISPs Must Delete Digital Traces"), *Aftenposten* 8 September 2009, available at <http://www.aftenposten.no/forbruker/digital/nyheter/data/article3112805.ece>.

⁸³ See Statistics Norway, at http://www.ssb.no/ikt_en/.

⁸⁴ See TNS Gallup, at <http://www.tns-gallup.no/?did=9091935>.

the initial two months).⁸⁵ It is also interesting to note that a lot of the requests are about deleting information that was published earlier by the person making the request.

Online youth safety

In practice, all young people in Norway use a computer and are on the Internet. The Norwegian Media Authority publishes a regular survey on young people's use of media. The survey poses questions to both young people and parents. The main findings from 2010 are: (a) children claim to have more alone time on the net than the parents believe; (b) parents claim to monitor Internet use by installing filtering/blocking software and checking log files to a greater extent than the children report; (c) most children have rules on how to use the Internet; the most common are not meeting anyone they only know from the Internet (54 percent) and not saying bad things to others on chat or via email (53 percent); (d) 50 percent of children say they are not allowed to pass out personal information on websites or in chat; (e) the trend over the last few years is that children know more on how to behave safely on the Internet; half of the children say that they do not pass out personal information because they have learnt about safe Internet use; (f) 23 percent have been asked for personal information by someone they don't know; most of the children ignored the request, but 5 percent say they gave the requested information and 22 percent gave some information; (g) 14 percent have experienced unwanted sexual comments on the Internet over the last year; 8 percent have been asked to send images of themselves naked over the Internet.⁸⁶

There has been a lot of focus on empowering young people to use the Internet safely, with privacy as the main focus, over the last few years. The campaign "Du bestemmer" (You Decide) has been used by more than 400,000 students between the ages of nine and 17.⁸⁷ In addition to focusing on safe Internet use, the campaign emphasised the children's right to privacy from teachers and parents as well. Open dialogue is encouraged as an alternative to filtering and "spyware". The campaign is funded by the Ministry of Government Administration, Reform, and Church Affairs and the Ministry of Education and Research.

NCIS (*Kripos*) has launched an initiative called "the Red Button". This is a button that organisations that provide Internet content aimed at young people can add to their site. When pressed, the button leads to the *Kripos* site, where the public can report sexual exploitation of children, human trafficking, or racism on the Internet.⁸⁸

⁸⁵ More information available at <http://www.slettmeget.no/5250-tall-og-statistikk-mars-2010> and <http://www.slettmeget.no/7675-tall-og-statistikk-april-2010>.

⁸⁶ Medietilsynet, *Barn og digitale medier* (Children and Digital Media) (2010), available at <http://www.medietilsynet.no/Documents/Trygg%20bruk/Rapporter/Barn%20og%20digitale%20medier/NYBarnogdigmed2010.pdf>.

⁸⁷ See <http://dubestemmer.no/en/>.

⁸⁸ In English at <https://tips.kripos.no/cmssite.asp?c=1&nm=0&menu=-1>.

In 2009 the so-called "grooming paragraph" was added to the Penal Code.⁸⁹ This means that it is now illegal to arrange a meeting with someone younger than 16 in order to engage in sexual activities. Paragraph 201 of the Code, which made it illegal to act in a sexually demeaning or indecent way in public without the other party's consent or in front of children under 16, was amended to include the use of telephones, Internet, or other means of electronic communication.⁹⁰

TERRITORIAL PRIVACY

Video surveillance

The PDA provides specific rules for video surveillance. Video surveillance that does not create actual files is more weakly protected than regular personal data registers. However, if the surveillance results in the recording of pictures, then the surveillance falls under the Act and the Data Inspectorate must be informed (Section 37). The Inspectorate has the power to intervene and prohibit surveillance if it does not conform to the Act. If video surveillance is performed in a public place, there must be clear notice given, such as through use of a warning sign (Section 40). However, the Criminal Procedure Act of 1981 allows police to perform covert video surveillance of public areas if permitted by court order and the surveillance is of "essential significance" for investigating suspected criminal conduct that can result in more than six months imprisonment (Section 202(a)).⁹¹

Location privacy (GPS, mobile phones, location based services, etc.)

On average, Norwegians have more than one mobile subscription per person. After adjusting for people with more than one subscription, mobile penetration in the Norwegian population is 96 percent.⁹² Ten percent have smart phones, while an additional 10 percent say they plan to buy one.⁹³ As smart phones are used much more actively than standard phones (because of applications such as "push" mail), there is a concern that this will generate more electronic traces. This has been addressed

⁸⁹ Act of 22 May 1902 No. 10 amended in June 2010, available in Norwegian at <http://lovdata.no/all/hl-19020522-010.html>.

⁹⁰ *Id.* at § 201.

⁹¹ Act of 22 May 1981 No. 25, amended by Act of 30 June 2006 No. 53 available in English at <http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf>.

⁹² The Norwegian Post and Telecommunications Authority, Det norske markedet for elektroniske kommunikasjonstjenester 2009 (The Norwegian Market for Electronic Communication Services 2009), available at http://www.npt.no/ikbViewer/Content/119027/Ekomrapport_2009_.pdf.

⁹³ Richard Nodeland, "NordMENN vil ha smarttelefon" ("Norwegian Men Want Smartphones"), VG nett 17 February 2010, at <http://www.vg.no/dinepenger/artikkel.php?artid=589521>.

specifically by the Data Inspectorate in its response to the hearing on the Data Retention Directive.⁹⁴

In 2010 the Norwegian telephone company Tele2 launched the service "Bipper". The service gives parents more control over their children's mobile use. Parents can control the numbers their children are allowed to call and block the mobile for use at certain times of day (for instance, between 11 pm and 7 am). In addition, children can use the phone as a safety alarm. However, "Bipper" also allows the parents to locate their children through an Internet service.⁹⁵ This has led to a debate on the balance between sound parental control and surveillance.⁹⁶

It is to be expected that the use of popular commercial location services such as Facebook Places, Gowalla, etc. are proportionate to Norway's high Internet and smart phone penetration rates.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

In October 2005, the production of biometric passports started in Norway.⁹⁷ The security mechanism was BAC (Basic Access Control).⁹⁸ The Data Inspectorate expressed serious concerns regarding the security of the passports because the data stored on the RFID chips is not encrypted.⁹⁹ The chip contains a digital photo and the holder's personal information. The digital photo in the chip can be measured against the facial features of the person travelling with the passport, intended to make it easier to authenticate passport holders and reduce the risk of theft and fraud.

In April 2010, Norway started deploying passports incorporating a digital representation of the holder's fingerprint onto the chip. The fingerprint is stored only on the chip and not in a central database. When the holder enters the country, the traveller's fingerprint is compared to the one stored on the passport. The print is only stored for long enough to

⁹⁴ The Norwegian Data Inspectorate, Høringsuttalelse – implementering av datalagringsdirektivet (2006/24/EC) (Response to Hearing on the Implementation of the Data Retention Directive), available at http://datatilsynet.no/upload/hoering/2010/hoering_datalagring.pdf.

⁹⁵ See the Bipper's homepage, at <http://www.bipper.com/>.

⁹⁶ Ole Petter Baugerud Stokke, "Mobiltjenesten Bipper overvåker barn" ("The Mobile Service Bipper puts Children under Surveillance"), VG Nett 8 August 2010, at <http://www.vg.no/teknologi/artikkel.php?artid=10017672>.

⁹⁷ Press Release, Ministry of Justice and the Police, "New Electronic Passports" 27 September 2005, in Norwegian at <http://www.regjeringen.no/en/dep/jd/Whats-new/News/2005/Nye-elektroniske-pass-og-personvernet.html?id=99556>.

⁹⁸ ICAO, Machine Readable Travel Documents, Part 1 Vol. 2, available at <http://www2.icao.int/en/MRTD/Downloads/Doc%209303/Doc%209303%20English/Doc%209303%20Part%201%20Vol%202.pdf>.

⁹⁹ Press Release, Data Inspectorate, "Personvernet utilfredsstillende ivaretatt" ("Passports Have Inadequate Security"), 10 October 2005, at http://www.datatilsynet.no/templates/Page_____1211.aspx.

make the comparison.¹⁰⁰ The biometric passports with fingerprints are protected with Extended Access Control (EAC). There has been some debate related to the implementation of biometric passports, and the Data Inspectorate has been critical of the security mechanisms in the chip.¹⁰¹ The initial suggestion to also store the fingerprint in the central passport database was abandoned because of arguments that this could be a threat to privacy.

Norway is part of the Schengen cooperation, and in theory Norwegian citizens may travel without a passport in the Schengen area. But because the passport is the only internationally accepted ID card available in Norway, in practice Norwegians must carry their passport anyway.

At most Norwegian airports it is possible to take fingerprints of airline passengers when they check in luggage for a flight for later verification at the gate. The prints are deleted when the plane has landed. This is optional, and the passenger may choose to show documentation (typically a passport) instead.

There are no security checks or ID checks to travel by train, but in order to travel to a foreign country by boat, ID has to be shown upon boarding.

NATIONAL ID & SMART CARDS

Identification is required to open a bank account. In practice the only internationally accepted ID in Norway is a passport. Because many people do not qualify to get a passport, the Government has decided to issue a national identity card.¹⁰² This will not be a compulsory ID, but an alternative to a passport. For Norwegian citizens it will also function as a passport in the Schengen region. The information and security mechanisms will be the same as for the passport. In addition, it is meant to function as a digital signature (with information on a separate chip for this). There are also other providers of digital signatures in Norway. Because the information on the cards will be encrypted, it should not be possible to read them remotely in order to identify or track people.

The Norwegian government is currently developing an e-identity hub (*ID-porten*) to facilitate interoperability between, on the one hand, electronic identities available on the market and, on the other hand, different e-government service providers, such as the tax authorities and the social security authorities. The basic idea is to allow the end user to choose from a catalogue of selected electronic identities (both government-issued and others) when accessing government services. Providers of e-government services select a required security level (on a scale from one to four) when they agree to let the identity

¹⁰⁰ Act of 19 June 1997 No. 82, amended in June 2009, available at <http://lovdata.no/all/hl-19970619-082.html>.

¹⁰¹ All the documents from the Data Inspectorate on passports are available at http://datatilsynet.no/templates/article___1251.aspx.

¹⁰² Ministry of Justice and the Police, Press release No. 25 2007, available at <http://www.regjeringen.no/nb/dep/jd/pressemelder/pressemeldinger/2007/foreslar-nasjonalt-id-kort-i-norge.html?id=457472>.

hub carry out the authentication of their users. Once the Norwegian national identity card is available, it is expected that it will include an electronic identity at the highest level of security (level four), which can also be used within the identity hub.

People have also to show ID to enter a central Government building and the Parliament building, and to buy alcohol or tobacco (if they are under 25). In practice, people can use any form of ID for this, such as a driver's licence or a bank card.

RFID tags

Most people living in or near a big city in Norway have an active RFID tag in their car, called an AUTOPASS tag.¹⁰³ This is used to register passing through toll booths for billing purposes. The trips are registered with AUTOPASS and also locally on the chip. The information is not encrypted and can be read remotely with the right equipment.¹⁰⁴ The Data Inspectorate has been very critical of the removal over recent years of the possibility of anonymous passage through toll booths; the option of paying in cash has been removed almost everywhere.¹⁰⁵

RFID is also used in libraries for checking books in and out. The tag in the book only contains an ID number. Information on the name of the book and the borrower are held in the library database.

RFID has been used to tag domestic animals for many years. RFID is also used in retail, but still mostly in the back end systems and not to tag individual products that are purchased by the consumers.

There has been some debate about the use of RFID tags in tickets for public transportation. Many of these systems register every time the cardholder enters or exits a means of transportation, and the information is made available to the user online. Critics feel that this means that the individual's pattern of movement can be exposed to others, and that this information is not necessary in order to provide the service. In response to pressure from privacy advocates, there is now also a prepaid anonymous option.

In a recently published strategy for intelligent transport systems (ITS)¹⁰⁶ the Ministry for Transport and Communication states that effective use of ITS can be a threat to privacy. The implementation of ITS can create excess information that makes it possible to map people's patterns of movement in relative detail. The Government states that there should

¹⁰³ The AUTOPASS website, in English at http://www.autopass.no/_attachment/110482/binary/310433.

¹⁰⁴ The Norwegian Data Inspectorate, "Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon" ("The Norwegian Road Authority Withheld Important Information on AutoPASS"), (2007), at http://datatilsynet.no/templates/article____1728.aspx.

¹⁰⁵ The Norwegian Data Inspectorate, "Heilautomatisering av Oslo-bomringen" ("Fully Automated Toll in Oslo") (2008), at http://datatilsynet.no/templates/Page____2151.aspx.

¹⁰⁶ The Norwegian Ministry for Transport and Communication (2010), *Intelligente Transportsystemer* (Intelligent Transport systems), available at http://www.regjeringen.no/Upload/SD/Vedlegg/rapporter_og_planer/its-strat-2010.pdf.

be more emphasis on shaping such solutions to keep the personal information captured to a minimum. Travel information should not be exchanged between sectors in order to enable the tracking of individual travel patterns. The Ministry of Government Administration, Reform and Church Affairs has developed a guideline for public privacy impact assessments.¹⁰⁷ The ITS strategy document, as well as the National Transport Plan 2010-2019,¹⁰⁸ states that this shall be used for all relevant cases in the transport sector.

BODILY PRIVACY

In 2007 the Norwegian Aviation Authority, Avinor, proposed to try out body scanners in the security checkpoints at Stavanger Airport. Strong negative reaction from the public and politicians led Avinor to cancel the plan.¹⁰⁹

For many years it was unclear how biometrics related to the Personal Data Act: are fingerprints sensitive data that should be treated as such, or are they more like a person's name? This has been clarified to some extent by a series of rulings by the Privacy Appeals Board.

In case PVN-2006-7¹¹⁰ a Norwegian municipality, Tysvær, had implemented a system using fingerprinting to log into its computer system. The need for secure identification in the case was not disputed, as access to the computer system would also allow access to sensitive personal data. The Data Inspectorate acknowledged this, but stated that other means of identification, such as a smart card and password, could provide the same level of security. The Appeals board ruled in favour of Tysvær, and stated that its use of fingerprinting is within the scope of the Personal Data Act. In the reasoning they stated that there are risks associated with smart card solutions that are not found in solutions that are based on fingerprinting.

In two other cases – PVN-2006 8 and 9¹¹¹ – two fitness centres wanted to use fingerprinting as a means of access control. In these cases the Appeals Board agreed with the Data Inspectorate that other, less secure means of identification would be sufficient.

¹⁰⁷ The Ministry for Government Administration, Reform and Church Affairs (2008), *Vurdering av personvernkonsekvenser* (Privacy Impact Assessment), available at <http://www.regjeringen.no/upload/FAD/Vedlegg/Statsforvaltning/Personvernveileder.pdf>.

¹⁰⁸ The Ministry for Transport and Communication (2010), *St. meld nr. 16 (2008-2009) Nasjonal transportplan 2010-2019* (National plan for transport 2010-2019), available at <http://www.regjeringen.no/nb/dep/sd/dok/regpubl/stmeld/2008-2009/stmeld-nr-16-2008-2009-.html?id=548837>.

¹⁰⁹ NTB, "Avinor utsetter testing av kroppsskanner" ("Avinor Postpones Body Scanner Test"), in *Aftenposten*, available at <http://www.aftenposten.no/nyheter/iriks/article2109513.ece>.

¹¹⁰ Full ruling available at http://personvernemnda.no/vedtak/2006_7.htm.

¹¹¹ Full rulings available at http://personvernemnda.no/vedtak/2006_08.htm and http://personvernemnda.no/vedtak/2006_09.htm.

In case PVN-2006-10,¹¹² the Data Inspectorate had ruled that Esso Norway could not use fingerprinting as part of its entry control at four facilities where only trained and authorised personnel have access. The Appeals Board overturned this, and stated that in this case there was a real need for secure identification, and that an ID card combined with a fingerprint reader could provide it.

In case PVN-2006-11,¹¹³ the retailer REMA 1000 wanted to use fingerprints for authentication when its employees checked in and out for work. The Appeals Board ruled that REMA 1000 could not use fingerprinting as there are other, even though less accurate, means of satisfying its need for authentication.

These five cases have established precedents for when fingerprinting can and cannot be used.

WORKPLACE PRIVACY

Surveillance and control measures in the workplace are regulated by the Working Environment Act.¹¹⁴ The Act states that employers wishing to implement control measures must have a legitimate reason based on the nature of the business, and that the measures should not be an unnecessary burden on the workers. Information collected has to be handled in accordance with the Personal Data Act.

Employers should discuss the need for control measures and how they should be implemented with the union representatives. All workers shall be informed before the measure is put into place, and there should be regular evaluations.

In a recent study by Fafo¹¹⁵ (Institute for Labour and Social Research) 6,022 Norwegian workers answered a Web survey on monitoring and surveillance in the work place. The most common means of surveillance and monitoring are electronic access control (31 percent), systems that register time use or productivity (22 percent), surveillance of Internet sites visited by employees (20 percent), and monitoring of telephone use (16 percent).

As described earlier, in 2009 a chapter concerning the employer's right to examine an employee's email box, etc., was added to the Personal Data Regulations.¹¹⁶ This chapter clarified an issue that had previously been unclear, and restricted employers' access to employees' email in contrast to previous practice. In 2010, the Data Inspectorate issued a fine of NOK15,000 (approx. €2,000) to an organisation (*Nordenfjeldske*

¹¹² Full ruling available at http://personvernnemnda.no/vedtak/2006_10.htm.

¹¹³ Full ruling available at http://personvernnemnda.no/vedtak/2006_11.htm.

¹¹⁴ Act 2005-06-17 No. 62: Working Environment Act, amended 2007-02-23 No. 10, *supra*.

¹¹⁵ Mona Bråten, "Kontroll og overvåking i arbeidslivet" (Control and Monitoring at Workplace"), Fafo 2010, available (summary in English) at <http://www.fafo.no/pub/rapp/20166/20166.pdf>.

¹¹⁶ Regulations on the Processing of Personal Data, Chapter 9, *supra*.

Kunstindustrimuseum) for accessing an employee's email without legal grounds and without notifying the employee.¹¹⁷

HEALTH & GENETIC PRIVACY

Medical records

In 2005 Parliament approved the establishment of the Norwegian Labour and Welfare Organisation (NAV) to provide comprehensive welfare reform.¹¹⁸ NAV is a merger of three organisations: the National Insurance Organisation, the National Employment Service and the Social Welfare System. As of July 2007, NAV had data on more than 2 million users from these combined databases.¹¹⁹ The merger has raised concerns because the number of people with access to sensitive personal data has doubled, and the access restrictions are inadequate.

As part of the reform, NAV was granted access to clients' health records as part of its control regime. The Data Inspectorate objected to this, but was ignored. When the Data Inspectorate found that NAV did not give notification upon accessing health records, it issued an order requiring NAV to establish new routines where such notification should be given within four weeks. According to the Data Protection Act notification should always be given when accessing personal data from an external source. NAV appealed the order to the Privacy Appeals Board (case PVN-2009-22),¹²⁰ but the board upheld the Data Inspectorate's ruling, emphasising that the right to information is important because it gives the data subject the opportunity to correct and supplement the information. The Appeals board cannot see that not informing the data subject serves this purpose.

Genetic identification

No specific information has been provided under this section.

FINANCIAL PRIVACY

The Competition Act, Money Laundering Act, and Foreign Register Act all came into force in 2005, and allow the tax administration to request audit information from financial institutions and the tax collector to obtain audit information from third parties.¹²¹ The police are allowed to access this kind of information during open

¹¹⁷ Norwegian News Agency, "Får 15000 I bot for å ha lest e-post til ansatt" ("Fined NOK 15.000 for Reading Employee Email"), in *Aftenposten*, 11 August 2010 available at <http://www.aftenposten.no/jobb/article3764372.ece>.

¹¹⁸ Norwegian Labour and Welfare Organisation, at <http://www.nav.no/page?id=1073743655>.

¹¹⁹ *Id.*

¹²⁰ Full ruling available at http://www.personvernemnda.no/vedtak/2009_22.htm.

¹²¹ The Ministry of Justice and the Police and The Ministry of Finance, "The Norwegian Government's Action Plan for Combating Crime 2004-2007" at 5, available in English at http://www.regjeringen.no/upload/kilde/jd/rap/2004/0035/DDD/PDFV/247688-action_plan_for_combating_economic_crime.pdf.

investigations. In 2006, amendments were proposed giving the police access if the information is needed to prevent and combat crime.¹²²

The Money Laundering Act requires employees in financial, gaming, and other institutions involved in the transfer of funds to notify the Norwegian Economic Crime Unit if they suspect that a client may be laundering funds.¹²³

The law regarding the transfer of funds into and out of Norway was amended in 2009 to give even more people access to the register of these transfers.¹²⁴ Established in 2004 as part of the fight against money laundering and terror financing, the register contains information on transactions in and out of Norway. The following actors now have access to the register: the police (previously only a limited part of the police force working with financial crimes), the National Bank, the Financial Supervisory Authority, the tax authority, Customs and Excise, the Norwegian Labour and Welfare Administration, and the Ministry of Foreign Affairs.

There is a long tradition in Norway for making data on tax-assessed personal income publicly available. Traditionally, the data were set out on lists that were available in paper form at a local city hall or tax office. The press has been given access to the information electronically for many years. With the development of the Internet and newspapers' online platforms, some newspapers decided to make the income data available to their readers in a searchable database. In 2004 the rules governing the publication of such data were tightened, making the lists available for individual searches for only three weeks after initial publication. The data lists were then posted electronically on the tax authority's website and provided in hardcopy at local tax offices, and it became illegal for the general media to publish their own database. In 2007 an amendment to the law again gave the mass media access to complete lists of income data. The Government said its reasons included a wish to strengthen the critical debate on the tax system.¹²⁵ The mass media presently offer gratis online search facilities for looking up personal income data. The Privacy Commission appointed by the Government in 2007 recommended scaling back the online availability of income data so that such online search facilities would only be available from the tax authority's website.¹²⁶ In 2010 the opposition parties in Parliament proposed banning the publication of assessed taxes. Part of their reasoning is that technological development has made the information more entertainment than

¹²² The Data Inspectorate's 2006 Annual report to the EU Art. 29 Data Protection Working Party, *supra*.

¹²³ Act of 6 March 2009 No. 11 on Measures to Counter Money Laundering and Funding of Terrorism, especially Section 18.

¹²⁴ Lov 2004-05-28 No. 29 om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge (valutaregisterloven), (Law of 28 May 2004 NO. 29 on the Register of Information on Currency Exchange and Transfer of Funds into and out of Norway (Currency Registry Act)), amended in June 2009, available at <http://lovdata.no/all/hl-20040528-029.html>.

¹²⁵ The Data Inspectorate's 2007 Annual report to the EU Art. 29 Data Protection Working Party, 12 June 2008, at http://datatilsynet.no/templates/Page_____2327.aspx.

¹²⁶ NOU 2009:1, *supra*, Section 13.5.6.

grounds for debate on the tax system – there are now iPhone applications to search the "tax lists", a Facebook application that lists your friends' income, etc. The proposal failed, but the majority of the Parliamentary Standing Committee on Finance and Economic Affairs recommended that the rules for publication should be changed, so that the access given to the tax information is more in line with the original intention of the system (public debate and control) and less for entertainment purposes.¹²⁷

E-GOVERNMENT & PRIVACY

The services portal *norway.no* offers e-services to all citizens since the end of 2005.¹²⁸ Since this year, the portal has been managed by a public agency entitled Norway.no, subordinate to the Ministry of Government Administration, Reform and Church Affairs. The original conception of such a portal first appeared as a project in 1999 under the government programme called "A Simpler Norway" and was launched in January 2000 in cooperation with the Norwegian Association of Local and Regional Authorities.¹²⁹

The *norway.no* portal provides information on the public sector, structured around topics of interest (e.g., employers, jobseekers, etc.) and also includes a comprehensive inventory of Norwegian public authorities. In addition to information and services through the Internet, the *norway.no* agency features a citizen's help desk, which may be contacted by telephone, SMS, fax, post, email, and chat. The desk can direct users to other public agencies as well. Norway.no itself has recently been given further responsibilities on information policy in the public sector, national evaluations of public websites, supervision of conformance to accessibility guidelines and categorisation systems for public information.

There is currently a pilot project on online voting in Norway. In 2011 voters in 10 municipalities (out of a total of 431) will be able to use the system, but it is not clear yet how extensively it will be used in the future. While many politicians think online voting will make voting more popular with young people, others fear that it may lead to the buying and selling of votes, and that family members may unduly influence each other. A recent proposal from the political party *Høyre* (Conservative), suggests that even if the pilot is successful the technology should only be used by people with special needs.¹³⁰

¹²⁷ Innst. 134 S (2009–2010), available at <http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2009-2010/inns-200910-134/>.

¹²⁸ See <http://www.norway.no>.

¹²⁹ ePractice, eGovernment Factsheet – Norway – Infrastructure (May 2010), available at <http://www.epractice.eu/en/document/288463>.

¹³⁰ Dokument 8:128 S (2009–2010), available at <http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2009-2010/dok8-200910-128/1/>.

The Government has set up an information site¹³¹ and a blog¹³² on e-voting. The blog is open for debate by the public.

OPEN GOVERNMENT

Norway first introduced comprehensive legislation on open government in the form of the 1970 Act on Public Access to Documents in the (Public) Administration, which provided for a broad right of public access to government-held records. That legislation was repealed and replaced in 2006 by a new Act which contains broadly similar provisions as the old Act but in a more technology-neutral form.¹³³ The legislation does not apply to records held by the Parliament, the Office of the Auditor General, the Ombudsman for Public Administration, or other parliamentary institutions; nor to the courts. There are numerous exemptions to the right of access, including exemptions for internal documents (Sections 14-16); information that could be detrimental to the security of the realm, national defence, or relations with foreign states or international organisations (Sections 20-21); information subject to a duty of secrecy; the minutes of the Council of State, photographs of persons entered in a personal data register; complaints, reports, and other documents concerning breaches of the law; answers to examinations or similar tests (Section 26); and documents prepared by a ministry in connection with annual fiscal budgets. If access is denied, individuals can appeal to a higher authority under the act and then to a court.

The EU Directive on Public Sector Information¹³⁴ was implemented into Norwegian law in January 2009.¹³⁵ Implementation is reflected in the above-cited legislation on open government.

In May 2010 a portal (*Offentleg elektronisk postjournal*, OEP) where you can search for public documents from all parts of government administration was launched. Previously, the press had access to such a portal for the majority of the ministries, but with the new portal the general public is allowed the same rights, and the portal is extended to all ministries and the cabinet office.¹³⁶

All documents sent from ministries, directorates and state agencies are indexed and stored in an online database. Through OEP, anyone can access the database, search for a document of their interest and order it. This order will then be sent to the public agency

¹³¹ See <http://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2009-2010/dok8-200910-128/1/>.

¹³² See <http://www.e-valgbloggen.no/>.

¹³³ Act of 19 May 2006 No. 16 amended in January 2009, available in English at <http://www.ub.uio.no/ujur/ulovdata/lov-20060519-016-eng.pdf>. The primary right of access is set out in Section 3.

¹³⁴ Full text in English available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf.

¹³⁵ Act of 19 May 2006 No.16, *supra*.

¹³⁶ See <http://oep.no/nettsted/fad>.

responsible for the document; it will be considered as a disclosure request. The user will receive an answer to their request directly from the public agency in charge of the document. When a request is rejected, information about the right to appeal against refusals and the time limit will appear in the refusal message. On another note, the responsible public agencies have an obligation to consider that the principles of public openness and confidentiality apply only to the information, not to the entire document.¹³⁷ In order to protect the individual citizen's privacy, it is not possible to search for all documents related to one individual. Documents that contain sensitive information are either withheld from public altogether, or the sensitive parts are redacted.

OTHER RECENT FACTUAL DEVELOPMENTS

In 2007 the Norwegian Government appointed a Privacy Commission which had as its primary remit (i) to stimulate societal discussion about privacy issues, (ii) to assess the challenges facing protection of personal privacy, and (iii) to recommend measures to meet those challenges. The Commission's report was published in early 2009.¹³⁸ It contains a large number of proposals, including: (i) introducing more explicit and direct provisions on privacy and data protection in the Constitution, (ii) encouraging possibilities for transactional anonymity, (iii) placing a moratorium on the establishment of health registers until a thorough analysis of the privacy implications of existing registers is undertaken, (iv) scaling back the online availability of personal income data, and (v) promoting greater use of privacy impact assessments. The Government is presently considering these proposals. Some proposals have already been acted upon. For example, the Government has established a committee to examine media liability issues with respect to new media platforms, as recommended by the Commission.

Sandok, the Norwegian Armed Forces Health Register came into force in 2006.¹³⁹ The register may contain personal, service and health data about Defence personnel; information about physical and social environments; and health information – all obtained without the person's consent.¹⁴⁰

The Ministry of Government Administration, Reform and Church Affairs has developed guidelines for public privacy impact assessments.¹⁴¹ The guidelines are a supplement to

¹³⁷ ePractice, eGovernment Factsheet – Norway – Infrastructure, *supra*.

¹³⁸ NOU 2009:1, *supra*.

¹³⁹ Ot. Prp. 60 (2003-2004) Om lov om personell i forsvaret (Legal Proposition to Parliament No. 60 (2003.2004) on the Defence Personnel Act), Chapter 9.6.3, available in Norwegian at <http://www.regjeringen.no/nb/dep/fd/dok/regpubl/otprp/20032004/otprp-nr-60-2003-2004-/9/6/3.html?id=178131>.

¹⁴⁰ *Id.*

¹⁴¹ The Ministry for Government Administration, Reform and Church Affairs (2008), Vurdering av personvernkonsekvenser (Privacy Impact Assessment), available at <http://www.regjeringen.no/upload/FAD/Vedlegg/Statsforvaltning/Personvernveileder.pdf>.

the Instructions for Official Studies and Reports.¹⁴² The purpose of these instructions is to ensure the proper preparation and administration of all work relating to official reforms, amendments to regulations, and other measures. The guidelines for privacy impact assessment are meant to help in evaluating which cases require a privacy impact assessment, and to provide instructions for how to conduct such an assessment.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

In 2009 organisations such as Electronic Frontier Foundation Norway (EFN) were very active in opposing the implementation of the Data Retention Directive into Norwegian law.¹⁴³ In addition, quite a few "*ad hoc*" organisations/movements such as "*Stopp datalagringsdirektivet*" ("stop the data retention directive") emerged.¹⁴⁴ It is also noteworthy that the Privacy Commission appointed by the Government in 2007 expressed strong scepticism about implementing the Data Retention Directive, raising serious questions about the proportionality of the Directive's requirements.¹⁴⁵

In general, privacy advocacy in Norway has been handled by the Data Inspectorate. Norway does not have a strong tradition of NGOs working with privacy issues.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Norway has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and its First Optional Protocol, which establishes an individual complaint mechanism.¹⁴⁶

Norway is a member of the Council of Europe (CoE) and has signed and ratified the European Convention on Human Rights.¹⁴⁷ It has signed and ratified the CoE's Convention for the Protection of Individuals with Regard to Automatic Processing of

¹⁴² The Ministry for Government Administration, Reform and Church Affairs (2005), Instructions for Official Studies and Reports, at http://www.regjeringen.no/upload/FAD/Vedlegg/Statsforvaltning/Utreddningsinstruksen_eng.pdf.

¹⁴³ EFN's response to the hearing on the implementation of the Data Retention Directive, available in Norwegian at <http://efn.no/dld-hoeringsuttalelse2010.html>.

¹⁴⁴ See Stopp datalagringsdirektivet's homepage, at <http://stoppdld.no/om-initiativet/>.

¹⁴⁵ NOU 2009:1 *supra*, particularly Chapter 17.

¹⁴⁶ Norway has signed the ICCPR and its First Optional Protocol on 20 March 1968 and ratified them on 13 September 1972. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁴⁷ Signed 11 November 1950; ratified 15 January 1952; entered into force 3 September 1953, available together all the Conventions adopted within the CoE at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG>.

Personal Data (ETS No. 108) and has signed its Additional protocol (ETS No. 181).¹⁴⁸ It has also signed and ratified the CoE's Convention on Cybercrime.¹⁴⁹

Moreover, Norway is a member of the Organisation for Economic Cooperation and Development (OECD). It has adopted the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), together with the OECD Guidelines for Cryptography Policy (1997) and Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002).¹⁵⁰

* Updates to the Norwegian Report published in the 2010 edition of EPHR have been provided by: Christine Hafskjold, The Norwegian Board of Technology, Norway; Lee A. Bygrave, Tobias Mahler and Thomas Olsen, Norwegian Research Center for Computers and Law, University of Oslo, Norway.

¹⁴⁸ ETS No 108 signed 13 March 1981, ratified 20 February 1984, entered into force 1 October 1985; ETS No. 181 signed 8 November 2001,

¹⁴⁹ Signed 23 November 2001, ratified 30 June 2006; entered into force 1 October 2006.

¹⁵⁰ Available at http://www.oecd.org/departement/0,3355,en_2649_34255_1_1_1_1_1,00.html.

REPUBLIC OF POLAND

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Polish Constitution recognises the rights of privacy and data protection. Article 47 states, "Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life." Article 49 states, "The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute." Article 51 states, "(1) No one may be obliged, except on the basis of statute, to disclose information concerning his person. (2) Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law. (3) Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute. (4) Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute. (5) Principles and procedures for collection of and access to information shall be specified by statute."¹

The right to privacy is highly respected on constitutional grounds. It is reflected by Article 233(1) which includes the right to privacy as one of the inviolable rights that cannot be limited even by laws enacted in times of martial law and states of emergency. In case of violation of constitutional rights or freedoms the injured party has the right to the following remedies: the right of access to the court,² the right to complain to the Constitutional Tribunal,³ and the right to apply for assistance to the Commissioner for Citizens' Rights.⁴

As in other constitutional rights and freedoms, enjoyment of the right to privacy is subject to certain limitations. Article 31(3) stipulates three requirements for imposing such limitations: 1) it can be done only by statute, 2) when it is necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons, 3) such limitations shall not violate the essence of freedoms and rights.

¹ The Constitution of Poland of 2 April 1997, Journal of Laws of 1997 No. 78 item 483, English version available at <http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm>.

² *Id.*, Article 45.

³ *Id.*, Article 79.

⁴ *Id.*, Article 80.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Law on the Protection of Personal Data (LPPD) was approved in October 1997 and took effect in April 1998.⁵ The law is based on the European Union (EU) Data Protection Directive 1995/46/EC. Under the Law, personal information relating to identity may only be processed upon the fulfilment of at least one of the conditions the LPPD requires to be met for lawful personal data processing. Special rules are provided for the processing of sensitive data, which is defined as data relating to race, ethnic origin, religion or philosophical beliefs, political opinions, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions, sexual preferences, and convictions and other decisions issued in court or administrative proceedings. Everyone has the right to control the processing of his other personal data contained in the filing systems, and has the right to be informed whether such databases exist and who administers them. All queries should be answered within 30 days. Upon finding out that data is incorrect, inaccurate, outdated, or collected in a way that constitutes a violation of the Act, citizens have the right to request that the data be corrected, filled in, or withheld from processing.⁶ Personal information cannot generally be transferred outside of the European Economic Area unless the destination country has "comparable" protections. The law sets out criminal sanctions for violations. A 1998 regulation from the Minister of Internal Affairs and Administration set out standards for the security of information systems that contain personal information,⁷ but was replaced by the regulation of 2004.⁸

In August 2001, the Act was amended in order to bring it into full compliance with the EU Data Protection Directive.⁹ Among other changes, the amendment redefined the term "personal data"; introduced a new provision relating to final decisions issued solely on the basis of automated processing of personal data; introduced a new provision on data processing in relation to performance of a contract; adjusted the lawful processing provision; and inserted a scientific research clause. These amendments also included

⁵ Law on the Protection of Personal Data, Dz.U. nr 133, poz. 833, 29 October 1997. Unified text available in the Journal of Laws of 2002 No. 101, item 926 with later amendments. See also <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.PL>.

⁶ "The Info Boom's Murky Side," *Warsaw Voice*, 9 November 1997.

⁷ The Regulation of 3 June 1998, by the Minister of Internal Affairs and Administration as regards Establishing Basic Technical and Organisational Conditions Which Should Be Fulfilled by Devices and Information Systems Used for the Personal Data Processing, Journal of Laws 30 June 1998 No. 80 item 521.

⁸ Regulation of 29 April 2004, by the Minister of Internal Affairs and Administration as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing, Journal of Laws 2004 No. 100 item 1024.

⁹ Act of 25 August 2001, amending the Act on Personal Data Protection, Journal of Laws No. 100 item 1087.

regulations regarding the prior checking of sensitive data and the transfer of personal data to a third country, as well as further specifying the controller's duties. Enforcement of the Amendments to the Act on the Protection of Personal data began on 1 May 2004, the day of Poland's entrance into the European Union.¹⁰

In recent years additional changes to the LPPD were introduced in regards to the establishment of the Central Anticorruption Bureau¹¹ and the involvement of Poland in the Schengen Information System and the Visa Information System.¹² These legal amendments adversely affected the transparency of data processing.¹³ On 21 December 2007 the President of Poland introduced a proposal to supplement the existing and largely ineffective¹⁴ regime of criminal liability for infringements of personal data protection with administrative sanctions based on heavy fines. The bill proposes pecuniary sanctions (up to €100,000) to be imposed by the Inspector General on data controllers who did not act according to the Inspector's decisions. This proposal faced criticism from the business sector and the government as being "extremely unfavourable for data controllers and incompatible with the law on execution in administrative proceedings".¹⁵ Following lengthy debate, reservations raised by the government were accepted by the parliamentary commission, as reflected in its report of 20 May 2010.¹⁶ On 24 September

¹⁰ See http://www.giodo.gov.pl/259/id_art/195/j/en/. The text of the Amendment to the Act is available on the website at <http://orka.sejm.gov.pl/proc6.nsf/0/DEDD42548B204B7FC12577BA004A7CB7?OpenDocument>.

¹¹ Law of 9 June 2006 on the Central Anticorruption Bureau, Journal of Laws of 2006 No. 104 item 708.

¹² Law of 12 February 2010 amending the Law on the Participation of the Republic of Poland in the Schengen Information System and Visa Information System and the Law on the Protection of Personal Data, Journal of Laws, 17 March 2010 No. 41, item 233.

¹³ For instance, pursuant to legal provisions added to the LPPD (Article 43. 1.2b) Polish authorities were exempted from the obligation of registering data filing systems used for processing of personal data for the purposes of the Schengen Information System and the Visa Information System.

¹⁴ Out of 462 notifications on the commission of crime against personal data protection which were addressed by the Inspector General to the prosecution authorities (1999-2006) only in 58 cases (12.5 percent) an indictment was brought to the court, after. Explanatory statement to a draft amendment of the Law on Personal Data Protection (Print No. 488) presented by the President of the Republic of Poland on 21 December 2007, available in Polish at <http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/488>.

¹⁵ Stanowisko Rządu z 17 września 2008 r. w sprawie prezydenckiego projektu ustawy o zmianie ustawy o ochronie danych osobowych (druk nr 488) (Position of the Government of 17 September 2008 on the President's bill on amendments of the Law to the Protection of Personal Data, print No. 488), available at [http://orka.sejm.gov.pl/Druki6ka.nsf/0/0FBB35F2AF59F045C12574C900370519/\\$file/488-s.pdf](http://orka.sejm.gov.pl/Druki6ka.nsf/0/0FBB35F2AF59F045C12574C900370519/$file/488-s.pdf).

¹⁶ Sprawozdanie Podkomisji Nadzwyczajnej z 20 maja 2010 r. o przedstawionym przez Prezydenta RP projekcie ustawy o zmianie ustawy o ochronie danych osobowych (druk nr 488) (Report of the Extraordinary Subcommittee of 20 May 2010 on the President's bill on amendments to the Law on the Protection of Personal Data, print No. 488), at <http://www.ensi.net/odo/dopobrania/sprawozdanie20052010.pdf>.

2010, the bill was adopted by the *Sejm* and passed to the *Senat* for approval.¹⁷ The final version of the bill (with the amendments proposed by the *Senat*) was adopted on 29 October 2010 and signed by the President on 18 November 2010. Among other amendments to LPPD, the bill provides that data subjects will have the right to withdraw their consent at any time.

Sector-based laws

Protection of personal data is also subject to sector-based regulations, the most extensive of which is the Law of 18 July 2002 on Providing Services by Electronic Means (LPSEM).¹⁸ This law is based on two EU Directives¹⁹ but has not yet been fully implemented.²⁰ Chapter 4 of the LPSEM concerns the protection of personal data of users of electronic services, and explicitly includes an electronic address of the user as a part of the category of personal data. It also addresses the issue of spamming by adopting the opt-in principle, and regulates the liability of ISPs for hosting illegal content on websites to which they provide access. A 15 January 2010 judgement of the Appellate Court in Wrocław shows such liability may also apply if the ISP does not block access to a fake account set up on a social networking service, despite the injured person's requests to block or remove a profile with his or her personal data from a website.²¹

¹⁷ Ustawa z 24 września 2010 o zmianie ustawy o ochronie danych osobowych i niektórych innych ustaw (Law of 24 September 2010 amending the Law on Personal Data Protection and some other laws), at [http://orka.sejm.gov.pl/opinie6.nsf/nazwa/488_u/\\$file/488_u.pdf](http://orka.sejm.gov.pl/opinie6.nsf/nazwa/488_u/$file/488_u.pdf).

¹⁸ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. Nr 144, poz. 1204 ze zm. (The Law of 18 July 2002 on Providing Services by Electronic Means, Journal of Laws 2002 No. 144 item 1204 with amendments), in English at http://www.itu.int/osg/spu/spam/legislation/Ustawa%20SUDE-eng_ver.pdf.

¹⁹ Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Brussels, 8 June 2000, OJ L 178/1 of 17 July 2000; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Brussels, 12 July 2002, OJ L 201, 31 July 2002. In case of the latter instrument, the Law of 18 July 2002 was based on its draft.

²⁰ Paweł Litwiński, Świadczenie usług drogą elektroniczną (Providing of services by electronic means), Paweł Podrecki (ed.), Prawo Internetu (Law of the Internet) 222 (LexisNexis 2004).

²¹ Tomasz Rychlicki, Social networking sites, case IACa 1202/09, 3 March 2010, at <http://rychlicki.net/en/2010/03/03/3173/>.

The categories of personal information allowed for processing are specified in many legal acts. Among others, there are the Code of Labour,²² the Telecommunications Act,²³ the Law on the Police ²⁴ and the Law on Insurance Activities.²⁵

Article 161 of the Telecommunications Act allows providers of publicly available telecommunications services to process the following data concerning users who are natural persons: 1) surnames and first names; 2) parent's first names; 3) place and date of birth; 4) address of permanent residence; 5) personal number (PESEL) – in the case of a citizen of the Republic of Poland; 6) name, series, and number of documents confirming the identity, and in the case of a foreigner being a citizen of a country which is not a member of the European Union or the European Economic Area – a passport number or a residence card number; 7) data included in documents confirming the ability to perform an obligation towards a provider of publicly available telecommunications services resulting from an agreement for the provision of telecommunications services.

Another important contribution to privacy protection is the notion of "telecommunication secrecy." Article 159 of the Telecommunications Act covers content of communications, subscriber data, traffic data, location data and data on call attempts, including unsuccessful call attempts.²⁶ A breach of telecommunication secrecy is subject to criminal liability (Article 266(1) of the Penal Code) and administrative measures of pecuniary penalty (Article 209(24) of the Telecommunications Act).

Protection of personal data related to health status is also stipulated by the Law on the Medical Profession,²⁷ the Law on the Rights of Patients and the Ombudsman of Patient's

²² Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy, Dz.U.1998, Nr 21, poz. 94 ze zm. (Law of 26 June 1974 – the Code of Labour, Journal of Laws of 1998 No. 21 item 94, with amendments).

²³ Ustawa z dnia 16 lipca 2004 Prawo telekomunikacyjne, Dz.U.2004, Nr 171, poz. 1800 ze zm. (Act of 16 July 2004 on Telecommunication, Journal of Laws of 2004 No. 171 item 1800, with amendments). unofficial consolidated English translation at http://www.en.uke.gov.pl/_gALLERY/10/58/1058/telecommunications_law.pdf.

²⁴ Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 2002, Nr 7, poz.58 ze zm. (Law of 6 April 1990 on the Police, Journal of Laws of 2002 No. 7 item 58 with amendments), in English at http://www.policja.pl/portal/pol/90/4889/Polish_National_Police.html.

²⁵ Ustawa dnia 22 maja 2003 r. o działalności ubezpieczeniowej, Dz. U. 2003, Nr 124, poz. 1151 ze zm. (Law of 22 May 2003 on the Insurance Activity, Journal of Laws of 2003 No. 124 item 1151 with amendments).

²⁶ Article 159 of the Telecommunications Act, *supra*.

²⁷ Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza denty, Dz. U. z 2005 r. Nr 226, poz. 1943 (Law of 5 December 1996 on the Professions of Medical Doctor and Dentist, Journal of Laws 2005 No. 226 item 1943, with amendments).

Rights,²⁸ and in the Law on Health Care Units.²⁹ Among Polish regulations on the health care system, there is no specific regulation on genetic examination and access to genetic data.³⁰ The Law of 22 May 2003 on Insurance Activities (Article 22(6)), and related Regulation of the Ministry of Health of 2004 (paragraph 3.3)³¹ forbids the transfer of genetic data to insurance companies by medical institutions and other subjects in possession of such information (e.g., hospitals, health-care personnel).

DATA PROTECTION AUTHORITY

The Inspector General for the Protection of Personal Data (*Generalny Inspektor Ochrony Danych Osobowych*, GIODO) enforces the LPPD.³² Ewa Kulesza was appointed as the first Inspector General by the Polish Parliament in April 1998 and held the post through May 2006. Michał Serzycki acted as Inspector General for Personal Data Protection from 13 July 2006 to 13 July 2010. Wojciech Wiewiórowski was elected by the Parliament to the position of Inspector General in June 2010. According to the Data Protection Act he shall remain in office until 2014.³³

The Inspector General has six central duties: to ensure data is processed in compliance with the provisions on the protection of personal data; to consider complaints and issue administrative decisions; to comment on proposed new laws and regulations that impact upon data protection; to maintain a central registry of databases; to initiate and undertake activities to improve the protection of personal data; and to participate in the work of international organisations and institutions involved in personal data protection.

Amendments to the LPPD adopted on 29 October 2010 grant the Inspector General the right to formulate his or her position in relation to the protection of personal data, directed at any data controller. The Inspector General for Personal Data Protection is an independent authority and performs his or her duties assisted by the Bureau of the Inspector General (Bureau). The Bureau is regulated by the President of the Republic of

²⁸ Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Dz.U. 2009, Nr 151, poz.1217 ze zm.(Law of 6 November 2008 on the Rights of Patient and the Ombudsman of Patient's Rights, Journal of Laws 2009, No.151, item 1217 with amendments).

²⁹ Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej, Dz. U. z 2007 r. Nr 14, poz. 89, ze zm. (Law of 30 August 1991 on Health Care Units, Journal of Laws 2007 No.14 item 89, with amendments).

³⁰ Jacek. A. Piątkiewicz, National Regulations on Ethics and Research in Poland, European Commission, Brussels 2005, at http://ec.europa.eu/research/science-society/pdf/pl_eng_lr.pdf.

³¹ Rozporządzenie Ministra Zdrowia z dnia 23 marca 2004 r. w sprawie szczegółowego zakresu i trybu udzielania zakładom ubezpieczeń informacji o stanie zdrowia ubezpieczonych lub osób, na rzecz których ma zostać zawarta umowa ubezpieczenia, oraz sposobu ustalania wysokości opłat za udzielenie tych informacji, Dz. U. 2004, Nr 71, poz. 654 (Regulation of the Ministry of Health of 23 March 2004 on the Detailed Scope and Procedure of Communication to the Insurance Companies of Information on the State Health of the Insured Persons or Persons in Favour of Whom an Insurance Contract Will be Made, Journal of Laws 2004 No. 71 item 654).

³² GIODO' website (in English) <http://www.giodo.gov.pl/168/j/en/>.

³³ Curriculum vitae of the Inspector General Mr. Wojciech Wiewiórowski, at <http://www.giodo.gov.pl/453/j/en/>.

Poland.³⁴ The Bureau ensures that the tasks required of the Inspector General under the Act and other provisions are carried out.

Registration details must include the name and address of the data controller, the scope and purpose of the data processing, methods of collection and disclosure, and security measures. An example of the data filing system for registration by the Inspector General is shown in the Appendix to the Regulation of 29 April 2004. An Inspector has the right to access data, check data transfer and security systems, and to determine whether the information gathered is appropriate for its intended purpose.³⁵ The Inspector General's office monitors the activities of all central government, local government and private institutions, individuals and corporations.

In the years 2007-2009, the Bureau of the Inspector General received 2,831 complaints that were investigated by the employees of the Bureau. In 1,023 cases (36 percent) an administrative decision was issued.³⁶ Administrative proceedings initiated by individual complaints are subject to the requirements stipulated by the Code of Administrative Procedure or by the Act of 9 September 2004 on Stamp Duty. The Code of Administrative Procedure, which by the power of Article 22 of the LPPD is applicable to all proceedings conducted by the Inspector General unless the LPPD states otherwise, provides that any case should be investigated within a one-month period. In complicated cases this period may be prolonged for up to two months.

All proceedings are conducted solely in writing. The authority addresses the entities which according to the complainant have breached provisions of the LPPD with a request for an explanation and for any documents confirming their right to process the personal data of the complainant. Once the documentation has been collected, the evidence is analysed. If there is a recognised breach of provisions on personal data protection, the Inspector General orders, by means of administrative decision, restoration of the proper legal state.

The Inspector General for Personal Data Protection, pursuant to the provisions of the LPPD, may also react to any breach of the Act by initiating disciplinary proceedings or notification of commission of a crime. In the years 2007-2009, the Inspector General issued 76 notifications of commission of a crime.³⁷ In addition, the Complaints Department may, in case of individual complaints and in cases conducted *ex officio*, request that the Inspection Department inspect the premises of the data controller against whom the complaint has been lodged. The inspectors of the Bureau have carried out 126

³⁴ The Regulation of 3 November 2006 by the President of the Republic of Poland. As regards granting the statutes to the Bureau of the Inspector General for the Protection of Personal Data, Journal of Laws of 2006 No. 203 item 1494 available at http://www.giodo.gov.pl/144/id_art/354/j/en/.

³⁵ "A One-Woman Orchestra," *Warsaw Voice*, 21 June 1998.

³⁶ Bureau of the Inspector General Statistics page, at http://www.giodo.gov.pl/246/id_art/886/j/pl ; Annual reports of the Inspector General, available at http://www.giodo.gov.pl/541/id_art/2685/j/pl/.

³⁷ Annual reports of the Inspector General at http://www.giodo.gov.pl/541/id_art/2685/j/pl/.

inspections to date in 2010. In the years 2007-2009 the number of inspections amounted to 167, 201, and 220 respectively.³⁸ In the Polish personal data protection legal system it is the Inspector General that registers personal data files (also referred to as personal data filing systems) and not the controllers themselves. In the surveyed period (January 2008 to August 2010) the Inspector General issued 16,808 decisions on registration of personal data filing systems,, 1,015 decisions on denial of registration of data filing systems, 221 decisions on discontinuation of proceedings, and 654 decisions on striking of filing systems from the registry.³⁹

As of 10 February 2009, personal data filing systems shall be required to register with the Inspector General for Personal Data Protection using the new notification form. The introduction of a new simplified notification form is aimed at facilitating the data controller's proper compliance with their statutory obligation to notify the Inspector General of their data filing systems.⁴⁰

An electronic platform "e-GIODO" established in 2006 enables data controllers to apply for registration of their personal data filing system via the Internet.⁴¹ Since the introduction of this system, the number of applications has increased considerably, up 43 percent between 2005 (5,344) and 2009 (7,688).⁴²

On 1 May 2004, the Inspector General became a member of the Article 29 Working Party. Since 1 November 2004, Poland has also been a party to the Europol Convention and the Europol Joint Supervisory Body. Poland is a party to the Convention on the Use of Information Technology for Customs Purposes which came into force in Poland on 16 February 2006.⁴³ A bill to amend the LPPD has been proposed which increases the powers of the Inspector General.⁴⁴ According to the bill, the Inspector General will be given more options to ensure that data controllers obey the LPPD.⁴⁵

³⁸ Bureau of the Inspector General Statistics page, *supra*.

³⁹ *Id.*

⁴⁰ Inspector General for Personal Data Protection, Simplified notification of personal data filing systems, available at http://www.giodo.gov.pl/365/id_art/426/j/en.

⁴¹ Files registration at <http://www.giodo.gov.pl/148/j/en/>.

⁴² Bureau of the Inspector General Statistics page at http://www.giodo.gov.pl/246/id_art/1894/j/pl.

⁴³ Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, Brussels, 26 July 1995, Ratification Details. See <http://www.consilium.europa.eu/App/accords/Default.aspx?command=details&id=297&lang=EN&aid=1995110&doclang=EN>.

⁴⁴ Amendments to the Polish Data Protection Law, January 2008, at <http://iplawpoland.blogspot.com/2008/01/amendments-to-polish-data-protection.html>.

⁴⁵ *Id.*

The Inspector-General has also inspected and approved the social networking site "Nasza-klasa" for meeting all requirements provided by the LPPD.⁴⁶

An agreement between the Inspector General and the Direct Marketing Association has been reached which aims to ensure cooperation for improvement of protection of personal data and citizens' right to privacy. The Association has pledged to require marketing organisations to apply a Direct Marketing Code of Practice which defines notions of direct marketing, obligations of data controllers, and other provisions related to collection and use of personal data.⁴⁷

MAJOR PRIVACY & DATA PROTECTION CASE LAW

On 12 October 2004, the Supreme Administrative Court delivered a significant judgment concerning the transfer of personal data.⁴⁸ This judgment followed the cassation claim against the decision of the Regional Administrative Court examining the legality of the decision of the Inspector General for Personal Data Protection. The Court affirmed the illegality of the transfer of debtor's personal data (as a result of the transfer of receivables) to a debt collection company without prior approval from the debtor. The Inspector General has decided that any transfer of personal data must be preceded by an individual consent of the debtor. The fact that Polish law allows for the transfer of receivables does not constitute a sufficient justification for making personal data available to third parties without the approval of the debtor. It is also impermissible to reserve such a right contractually. Both the Regional and Supreme Administrative Courts have shared this view.

In a subsequent judgment dated 16 December 2004 the Supreme Administrative Court adopted a different standpoint. The Court decided that transfer of receivables can be considered as a legitimate interest of the data controller and the transfer of the subject's personal data is allowed without his or her consent. However, after long deliberation the Supreme Administrative Court (comprised of seven judges) in a final judgment dated 6 June 2005 revoked this view, and established that the processing or the transfer of personal data within the transfer of receivables does require the consent of the data subject. The lack of consent cannot be justified by a legitimate interest of the data controller.⁴⁹

In the last years, the administrative courts considered issues related to personal data protection over the Internet. A growing number of cases concern *nasza-klasa.pl* website – a popular Polish social networking service which enable classmates to be in touch and search for old friends. The judgments pronounced in these matters contribute, *inter alia*, to an interpretation of the notion of "personal data" in a network environment. On 18

⁴⁶ IWG Country Report – Poland, 43rd Meeting of the Working Group, March 2008.

⁴⁷ *Id.*

⁴⁸ Number of the judgment: OSK 769/04.

⁴⁹ Number of the judgment: sygn. I OPS 2/05.

November 2009 the Supreme Administrative Court ruled that a 30-year-old photograph of the complainant, listed with class year, name, and surname on *nasza-klasa.pl* constitutes personal data within the meaning of Article 6(2) of the LPPD.⁵⁰

In a judgment dated 3 February 2010, the Voivodeship Administrative Court in Warsaw (i.e., the court of the second instance), stated that an IP address constitutes personal data under Article 6(2) of the LPPD. The Court admitted that usually an IP address as such is not a sufficient basis for identification of an individual who uses it. However, in combination with other information, particularly those at the disposal of the requested party (an ISP), an IP address enables identification of its user without unreasonable cost or expenditure of time and manpower.⁵¹

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

A search may generally only be ordered in Poland by a court or by a public prosecutor. All searches require a reasonable suspicion that items which may be used as evidence or seized for another purpose are on the premises. Nevertheless in urgent cases (i.e., when there is a risk that the evidence may be lost or hidden in case of delay) it may be carried out with an order from a chief of a police unit or by showing of a police ID. In these situations, the police ask the court or the public prosecutor for authorisation afterwards. Unfortunately, evidence shows that most searches in Poland are carried out without any earlier application for the order.⁵²

There are two methods of interception of communications in Poland: procedural (ordered in the framework of criminal proceedings) and non-procedural (ordered out of criminal proceedings). The first is regulated in the Code of Criminal Procedure 1997.⁵³ The second is regulated in various acts, such as the Police Act 1990,⁵⁴ the Central Anticorruption Bureau Act 2006,⁵⁵ etc. Each act contains a list of crimes in relation to which interception

⁵⁰ Wyrok NSA z dnia 18 listopada 2009 (I OSK 667/09), at <http://orzeczenia.nsa.gov.pl/doc/B0351DAD7F> (in Polish); Tomasz Rychlicki, "Personal data protection, case I OSK 667/09", 13 February 2010, at <http://rychlicki.net/en/2010/02/13/2176/>.

⁵¹ Wyrok WSA w Warszawie z dnia 3 lutego 2010 r. (II SA/Wa 1598/09), at <http://orzeczenia.nsa.gov.pl/doc/AD6FF02867>; Tomasz Rychlicki, "IP address is personal data says Polish Court," at <http://rychlicki.net/en/2010/02/05/1985/>.

⁵² See Z. Uniszewski, *Przeszukanie. Problematyka kryminalistyczna* (Search. Forensic problems) 407 (Warszawa 2000).

⁵³ Journal of Laws No. 89 item 555.

⁵⁴ Journal of Laws No. 30 item 179.

⁵⁵ Journal of Laws No. 104 item 708.

is authorised. Under the Code of Criminal Procedure, there are no precise requirements as to the basis of authorisation. The Police Act allows for interception only if the evidence cannot be gathered by other methods.

The Government of Poland carries out a large number of wiretaps with limited oversight. Under the Code of Criminal Procedure, the use of wiretaps shall be authorised by the court after an appropriate motion by a public prosecutor. The Minister of Justice, in consultation with the Minister appropriate for the communication issues, the Minister of Defence and the Minister appropriate for the internal affairs, shall specify the technical requirements of wiretaps, how it shall be controlled, and how to carry out the wiretap.⁵⁶ The law specifies for which cases the interception of communications may be authorised. In exceptional cases, a public prosecutor may initiate a wiretap and then apply for authorisation to a court. The Police Act also permits the use of electronic surveillance for the prevention of crime as well as for investigative purposes. Non-procedural wiretapping is authorised by a court on a motion from a relevant agency and consent of the public prosecution service. In urgent cases the agencies may initiate wiretapping without authorisation and then apply to the court.

The government does not usually release statistics on the number of wiretaps applied for and authorised, tending to view this as a state secret. In 1997, reports on the number of wiretaps varied from 2,000 to 4,000.⁵⁷ The exact number of interceptions is not known, as this information is also deemed secret but it has been claimed recently that the number of interceptions could be as high as 20,000 per year.⁵⁸

A proposal for amendment of the Code of Criminal Procedure has been introduced to Parliament that ensures more control over information gathered in the course of wiretapping.⁵⁹ The proposal aims to increase the control of the court and public prosecutor over interception of communications, to oblige the General Prosecutor to keep them informed about the number of interceptions and to strengthen the control of the court over materials obtained by interceptions.

Various proposals have been put forward to expand law enforcement surveillance capabilities over the last few years. In July 2001, amendments to the Police Act gave police increased powers to monitor individuals in public places including through the use of video surveillance. The International Helsinki Committee noted in its 2002 report that

⁵⁶ The Regulation of 24 June 2003 by the Ministry of Justice.

⁵⁷ Some Remarks on Human Rights Protection in Poland (in connection with the fourth periodic report of Republic of Poland on implementation of the International Covenant on Civil and Political Rights), Helsinki Foundation for Human Rights,

⁵⁸ W. Czuchnowski, "Rosnie liczba podsłuchów w Polsce" ("The Number of Interceptions in Poland is Rising"), *Gazeta.pl*, at <http://wiadomosci.gazeta.pl/Wiadomosci/1,80273,3216546.html>.

⁵⁹ Rządowy projekt ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (The Government Proposal for Amendment of the Code of Criminal Procedure and some other Acts of Parliament), at <http://orka.sejm.gov.pl/proc6.nsf/opisy/2915.htm>.

these amendments "were dubious in terms of the right to privacy."⁶⁰ Creation of new agencies for combating crime and vesting in them the power to carry out interception remains an issue. One of the most controversial is Central Anticorruption Bureau (*Centralne Biuro Antykorupcyjne* or CBA) which was created in 2006⁶¹ to fight corruption in both public and private sectors. It is argued that the Bureau obtained authorisations for some interceptions illegally and was used for a "political fight".⁶²

Poland has given priority to the fight against organised crime. The Police Act was amended in August 2001 to give the police more operational powers (authorisation to check bank and insurance accounts of suspects). Considerable efforts have been made to equip police with the latest technological tools (a central automated system for identifying fingerprints has been extended to regional and local levels).⁶³

The Police Act⁶⁴ has been amended by the Telecommunications Act. The amendments focus on disclosing and processing of caller ID by the Police, and also concern network terminals and/or telecom devices used in the connection, data generated during the connection or attempts to connect to particular telecom devices or network terminals, and circumstances and type of connection. Currently they may be disclosed to and processed by the Police only in order to prevent or detect a crime. This data may be disclosed at a written request by the Police Commander in Chief and/or a Regional Commander, or at an oral request of a policeman having a written authorisation of the above-mentioned authorities. Telecom operators shall disclose to the policemen the data mentioned in the request of an appropriate Police unit. Materials obtained by the Police which contain information relevant to the criminal proceedings are transferred to the office of the prosecutor. Materials obtained by the Police which do not contain information significant to criminal proceedings shall be immediately destroyed by a specially formed committee, which shall also provide officially recorded evidence of the destruction. Data shall be disclosed to the Police at the cost of the telecommunications operator. Despite the opinions of the Police and state security services, operators are not obliged to register (identify) pre-paid users.

In April 2004 the Constitutional Tribunal (*Trybunał Konstytucyjny* - TK) found an act unconstitutional regarding the Internal Security and Intelligence Agencies which allowed

⁶⁰ International Helsinki Federation for Human Rights, "Human Rights in the OSCE Region: The Balkans, the Caucasus, Europe, Central Asia and North America," Report 2002 (events 2001), available at <http://web.archive.org/web/20030210183203/http://www.ihf-hr.org/reports/AR2002/country+links/Poland.htm>.

⁶¹ Central Anticorruption Bureau Act of 9 June 2006, Journal of Laws No. 104 item 708.

⁶² See B. Wróblewski, "Sztuczki podsłuchowe CBA" ("CBA Interception Tricks"), *Gazeta.pl*, at http://wyborcza.pl/1,75478,7657168,Sztuczki_podsłuchowe_CBA.html.

⁶³ "Poland Adoption of the Community Acquis," Summary of the Legislation available at http://web.archive.org/web/20100908131827/http://europa.eu/legislation_summaries/enlargement/2004_and_2007_enlargement/poland/e22106_en.htm (last updated 10 August 2005).

⁶⁴ The Police Act of 6 April 1990, Journal of Laws of 2007 No. 43 item 277 (consolidated text).

officers to observe and record events in public places. Public groups had opposed the act on numerous grounds, including that it violated the right to privacy.⁶⁵

Of equal importance is a judgment of the Constitutional Tribunal from December 2005⁶⁶ where some of the provisions of the Police Act concerning interception of communications were found unconstitutional. One such provision was the possibility of interception without a court order when one of the parties to the communication consented. The Tribunal ruled that consent of one party did not justify interference with the privacy of the other party, and therefore in such situations a court authorisation was still required.

National security legislation

No specific information has been provided under this section.

Data retention

Mandatory retention of telecommunication traffic and location data specifically for the purposes of the law enforcement and national security agencies has been required in Poland since 2003. Both the regulation of the Ministry of Infrastructure of 2003⁶⁷ and the Law on Telecommunication of 2004⁶⁸ provided for a 12-month retention period for "transmission and location data".

In December 2005 an amendment to the Law on Telecommunication introduced mandatory telephony data retention for two years, after which time the service provider has the choice of either destroying or anonymising the data. The original draft called for a 15-year retention period, and local investigators stated that they were unable to effectively prosecute corruption without telephony billing data from the last four years. This prompted criticism from NGO ISOC Poland as well as the Inspector General for the Protection of Personal Data. A retention period of 15 years is clearly out of step with the EU Data Protection Directive adopted in 2006, which calls for retention periods of between six months and two years.⁶⁹

⁶⁵ "Court Says Parts of Secret Services Law Unconstitutional," BBC Worldwide Monitoring, 20 April 2004 (source Polish Radio 1, Warsaw, 20 April 2004).

⁶⁶ Judgment of 12 December 2005, K 32/04, OTK ZU nr 11/A/2005.

⁶⁷ Rozporządzenie Ministra Infrastruktury z dnia 28 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, Dz. U. Nr 19, poz. 166, zob. (Regulation of the Ministry of Infrastructure of 28 January 2003 on the Performance by Telecommunication Operators Tasks Related to National Defence, State Security, Safety and Public Order, Journal of Laws No. 19, item 166), available in Polish at <http://www.abc.com.pl/serwis/du/2003/0166.htm>.

⁶⁸ The Law of 16 July 2004 on Telecommunication, Journal of Laws of 2004 No. 171 item 1800.

⁶⁹ Ninth Annual Report of the Article 29 Working Party on Data Protection, June 2006, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

The Government's legislative proposals to extend the retention period over two years in order to increase efficiency in combating crime and terrorism were rejected by the parliamentary commission as not compatible with the Directive 2006/24/EC.⁷⁰

The Directive has been transposed into the Polish legal system in 2009 in two steps. In April 2009 the obligation of telephone data retention was imposed on telecommunication operators and service providers pursuant to the amended Law on Telecommunication of 2004.⁷¹ Requirements for the retention of "communications data relating to Internet access, Internet telephony and Internet email" were postponed until 15 March 2009.⁷² Even so, respective regulations of the Minister of Infrastructure covering, *inter alia*, retention of Internet data were enacted on 28 December 2009.⁷³

The retention period is equal for both telephone and Internet traffic data and amounts to 24 months from the date of the communication. After this time, a telecom operator or provider is required to destroy transmission data unless otherwise provided by the law. Clauses included in Article 180(a) of the Telecommunications Act imply an undetermined period of storage of traffic data.

Access to retained data is restricted to the Police, national security agencies, and judicial authorities.⁷⁴ All authorities have the right to access traffic, subscriber and localisation data in the case of any crime, however trivial. There is no legal threshold for seriousness of a crime or independent oversight of the disclosure of data by telecom providers to the applicants. These flaws of the legal data retention program may account for a recently disclosed scandal in Poland concerning surveillance of ten journalists by the secret services, who allegedly used traffic and location data from the journalist's mobile phones starting in 2005 and continuing through 2007 in order to reveal their informants in

⁷⁰ Commission minutes of 19 July 2006, in Polish at <http://orka.sejm.gov.pl/Biuletyn.nsf/wgsknr5/INF-63>.

⁷¹ Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. 2009.85.716.

⁷² Poland, like most of the EU member states, chose to take advantage of Article 15 (3) of the Directive in this respect.

⁷³ Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, Dz. U. Nr 226. poz.1828. (Regulation of the Minister of Infrastructure of 28 December 2009 on a Detailed Specification of Data and Types of Operators of Public Telecommunications Networks or Providers of Publicly Available Telecommunications Services Obligated for Its Retention and Storage, Journal of Laws of 2009 No. 226 item 1828). The Regulation went into force on 1 January 2010.

⁷⁴ A list of competent authorities includes: the Police, Military Police, Military Counter-Intelligence Service, Fiscal Intelligence, Border Guard, Internal Security Agency, and Central Anticorruption Bureau. Courts and prosecutors are also authorised to get access to traffic, location and subscriber data.

politically motivated investigations.⁷⁵ Costs for the retention, storage, retrieval and security of this data are borne by telecom operators and providers.

National databases for law enforcement and security purposes

An exact number and profile of the databases storing personal information set up and run by the law enforcement and public security agencies is not known. Legal restraints stemming from official secrecy regulations make it difficult to find comprehensive and up to date information on the subject. For the same reason, exercise of the right of inspection the data is subject to serious restrictions which apply both to the Inspector General and the data subjects.

As a rule, criminal intelligence data shall be kept confidential, so its controllers are exempt from the obligation to register data filing systems that it contains (Article 43.1.1a of the LPPD). The Inspector General is entitled neither to have access nor to inspect the data filing systems held by the Internal Security Agency, Foreign Intelligence Agency, Central Anticorruption Bureau and Military Information Services (Article 43 section 2). Data subject's right of access is denied in this case as well.

Police databases are more open for inspection, however not to the extent proposed by the Council of Europe (CoE) recommendation.⁷⁶ The Law of 6 July 2001 on gathering, processing, and transfer of criminal information⁷⁷ (LCI) specifies in detail what is criminal information, who is empowered to process it and by what means. This legislation does not provide a balance between the law enforcement and the data subject's interests, and it contains a number of exceptions to data protection regulations in the interests of law enforcement authorities (Article 18(2) of the LCI). The data subject is entitled to obtain "extensive information" about the data filing system (e.g., its purpose, scope, and controller) used by the Police, but not about his or her own data that is processed by the Police. The mere fact that such processing takes place shall remain secret for the individual concerned. As Article 2 of the LCI states, "collection, processing and transfer of criminal information according to the rules specified in the present law shall take place without the knowledge of the data subjects". Nevertheless, the right to rectification of data is recognised under the LCI, so one may speculate as how to exercise this right in such circumstances. A role of the Inspector General is very limited in this context. According to Article 18(1) of the LCI the Inspector is empowered to exercise control over the gathering and processing of criminal information. As a supervisory authority, he/she is, however, unable to act as an appeal instance and control whether a refusal of the data controller to disclose one's own records is legitimate or not.

⁷⁵ "Journalists' Phones Monitored in Politically Inspired investigation?," *Thenews.pl*, 8 October 2010, at http://www.thenews.pl/national/artykul141157_journalists-phones-monitored-in-politically-inspired-investigation.html.

⁷⁶ Recommendation No. R (87) 15 of the Committee of Ministers to member states of the Council of Europe regulating the use of personal data in the police sector.

⁷⁷ Law of 6 July 2001 on gathering, processing, and transfer of criminal information. Unified text available in the Journal of Laws of 2010 No. 29 item 153.

The Law of 9 June 2006 on the Central Anticorruption Bureau (CBA) restricted the powers of the Inspector General. Simultaneously it also granted the CBA officers almost unlimited access to the citizens' personal data held in public sector databases. Article 22 of the CBA law, which *inter alia* allows for collection and processing of sensitive data (Article 27 of the LPPD), requires a written authorisation from the head of the Bureau to access a database in another state agency. The administrator of the database is obliged to provide CBA agents access to data which falls within the scope of the authorisation. On 24 September 2006 Prime Minister Jaroslaw Kaczynski issued a decree allowing the CBA to access the public sector databases online.⁷⁸ This regulation provided direct access to data through the database administrator, making individual requests for disclosure of specific data unnecessary. On 3 October 2007 the daily *Gazeta Wyborcza* wrote on its front page about an agreement made as a result of this decree granting the CBA direct access to data on 25 million citizens gathered by the public Social Insurance Company (*Zakład Ubezpieczeń Społecznych*)[].⁷⁹ On 9 November 2007 a group of deputies representing the *Democratic Left Alliance* party (*Sojusz Lewicy Demokratycznej*) applied to the Constitutional Tribunal with a motion to consider non-conformity to the Constitution of both the Law of 9 June 2006 on the Central Anticorruption Bureau and the regulations enacted by the Decree of 27 September 2006.

In a judgment dated 23 June 2009 the Constitutional Tribunal found several provisions of the CBA law unconstitutional. Article 22 was found unconstitutional insofar as it allows the CBA to collect and process sensitive data and use this information, acquired without the knowledge and consent of persons concerned, in conditions precluding any control over processing of such data. A reference was made in this context to an infringement of the right to privacy as stipulated by the Polish Constitution (Articles 47 and 51) the European Convention on Human Rights (Article 8) and the CoE Convention No. 108 (Articles 5-7). Additionally, the Prime Minister's Decree of 27 September 2006 was found unconstitutional as an infringement of Article 51(5) of the Constitution which provides for exclusively statutory regulation of procedural issues in data protection.⁸⁰

National and international data disclosure agreements

No specific information has been provided under this section.

⁷⁸ Rozporządzenie Prezesa Rady Ministrów z dnia 27 września 2006 r. w sprawie zakresu, warunków i trybu przekazywania Centralnemu Biuru Antykorupcyjnemu informacji przez organy, służby i instytucje państwowe, Dz. U. Nr 177, poz. 1310 (Decree of the Prime Minister of 27 September 2006 on the Scope, Requirements and Procedure of Transfer of Information to the Central Anticorruption Bureau by the State Agencies, Services and Institutions, Journal of Laws 2006 No. 177 item 1310).

⁷⁹ Konrad Niklewicz, Ewa Siedlecka, "CBA wchodzi do bazy ZUS," *Gazeta Wyborcza*, 03 October 2007, at <http://wyborcza.pl/1,76842,4545758.html> ; "CBA to Be Given Access to Detailed Information on 25 mln Poles," *The Warsaw Voice*, 6 October 2007, at <http://www.warsawvoice.pl/WVpage/pages/article.php/4957/news>.

⁸⁰ Number of the judgment: sygn K 54/07, available in Polish at <http://www.trybunal.gov.pl/OTK/otk.htm>.

Cybercrime

Cybercrime legislation is developing quickly in Poland. It originated with the Penal Code of 1997 which criminalised most computer-related infringements, composing “a minimum list” of the 1989 Council of Europe recommendation.⁸¹ The list of computer offences has expanded in size subsequent to the 2004 amendment of the Penal Code.⁸² This legal change was related to Poland’s entrance into the European Union and was aimed at harmonisation of Polish criminal legislation with the Council of Europe Convention on Cybercrime (CoC). Three new offences against confidentiality, integrity, and availability of computer data and systems were introduced to Chapter 33 of the Penal Code (“Offences against the Protection of Information”).⁸³ Additionally, the possession of child pornography was prohibited (Article 202).

The change to criminal law concerning cybercrime of 2008 was aimed at implementation of regulations contained in two EU Framework Decisions.⁸⁴ This goal was accomplished in the case of criminalisation of “hacking”(Article 267(2)) and so-called “virtual child pornography” (Article 202(5)) in the Penal Code. A newly established provision of “hacking” (Article 267(2)) implements literally Article 2 of the 2005 Framework Decision and penalises anyone who obtains access to the whole or any part of an information system without authorisation. An official explanation for this legislative change stressed the usefulness of being able to punish “pure access” as a legal weapon against distributors of spyware and other malicious software used for taking control of infected computers.⁸⁵

The most recent contribution to cybercrime regulations comes from 2009 and consists of the so-called grooming offence (Article 200(a)), recommended by the CoE Convention of Lanzarote,⁸⁶ and two penal provisions introduced to the Penal Code in response to high profile Internet-related incidents. In Article 191(a) the wilful “dissemination of pictures of a naked person or person in a course of sexual activity, without consent of the person concerned” has been criminalised. In Article 200(b) a controversial prohibition of “public promotion or approval of paedophile’s behaviours” was placed.

⁸¹ Computer-Related Crime. Recommendation No.R (89) on computer-related crime and final report of the European Committee, Strasbourg 1990.

⁸² The Penal Code Amendment of 18 March 2004, Journal of Laws 2004 No. 69 item 626.

⁸³ These were: “system interference” (Article 269(a)), “misuse of devices” (Article 269(b)), and “data interference” (Article 268(a)).

⁸⁴ Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography, OJ L 13/44, 2004;
Council Framework Decision 2005/222/JHA on attacks against information systems, OJ L 69/67, 2005.

⁸⁵ Reasoning of the draft amendment of the Penal Code of 28 October 2008.

⁸⁶ Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Lanzarote, 25 October 2007, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=&CL=ENG>.

The Council of Europe Convention on Cybercrime has not yet been ratified by Poland despite the many steps taken to implement its provisions. The ratification procedure commenced by the Ministry of Justice in May 2008 but is still pending due to implementation problems. According to a memorandum obtained from the Department of International Cooperation and European Law of the Ministry of Justice, the only inconsistency concerns regulations regarding child pornography.⁸⁷ Article 202 (4a) of the Penal Code sets a lower age limit for protection against pornographic exploitation than is required (as a minimum) under Article 9(3) of the Convention. There are however other, more significant gaps in the domestic law of Poland *vis-à-vis* the CoC.⁸⁸

Critical infrastructure

The concept of "critical infrastructure" emerged in Poland in the aftermath of 11 September 2001. A legal definition of this notion is included in Article 3 of the Law of Crisis Management of 2007.⁸⁹ This law also provides delegation for the establishment of the Government Centre for Security, the main government entity responsible for planning protection of national security against terrorism and other threats. The Government Centre for Security was established in 2008 pursuant to regulation enacted by the Prime Minister.⁹⁰ More information on the Centre's activity is available at its web page.⁹¹

⁸⁷ Ministerstwo Sprawiedliwości, Departament Współpracy Międzynarodowej i Prawa Europejskiego, Notatka w sprawie zgodności prawa polskiego z Konwencją Rady Europy o Cyberprzestępczości z dnia 12 sierpnia 2009 r., DWM V 025-5/08 (Memorandum of the Department of International Cooperation and European Law of the Ministry of Justice on the Consistency of Polish Law with the Council of Europe Convention on Cybercrime).

⁸⁸ Andrzej Adamski, Cybercrime Legislation in Poland, in Biruta Lewaszkiewicz-Petrykowska (ed.), Polish Reports on the XVIIIth International Congress of Comparative Law, Washington D.C., 25 July-1 August, 2010, (Łódź University Publisher 2010).

⁸⁹ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U.2007, Nr 89, poz. 590 ze zm. (Law on Crisis Management, Journal of Laws No. 89 item 590, with amendments).

⁹⁰ Rozporządzenie Prezesa Rady Ministrów z dnia 10 lipca 2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, Dz.U. 2008, Nr 128, poz. 821 (Regulation of the Prime Minister of 10 July 2008 on the Organisation of and Operating Mode of the Government Centre for Security, Journal of Laws 2008 No. 128 item 821).

⁹¹ Rządowe Centrum Bezpieczeństwa (the Government Centre for Security), at <http://rcb.gov.pl/>.

INTERNET & CONSUMER PRIVACY

E-commerce

Legal regulation of e-commerce in Poland comes from the early 2000s and is based on provisions of the amended Civil Code,⁹² consumer protection laws,⁹³ and laws on electronic services.⁹⁴ In 2008 the government announced an action programme for advancement of e-commerce and e-services in the years 2009-2010.⁹⁵ One of the goals of this programme is to improve the legal framework for the development of e-business. New anti-spamming provisions, better protection of consumer's personal data, clear tax regulations of Internet transactions and full implementation of EU Directives into the law on electronic services are thought to be of primary importance by government and legal experts.⁹⁶

Cybersecurity

Cybersecurity has become a topical issue for Polish authorities in the last years. On 1 February 2008 the Governmental Computer Security Incident Response Team (CERT.GOV.PL)⁹⁷ was formed within the framework of the Computer System Security Department at the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*).⁹⁸

⁹² Ustawa z dnia 23 kwietnia 1964 r. kodeks cywilny, Dz. U. Nr 16, poz. 93 ze zm. (Law of 23 April 1964 – the Civil Code, Journal of Laws 1964 No. 16 item 93, with amendments).

⁹³ Ustawa z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, Dz. U. 2000, Nr 22, poz. 271 ze zm. (Law of 2 March 2000 on the Protection of Certain Consumer Rights and on the Liability for Damage Caused by a Dangerous Product, Journal of Laws 2000 No. 22 item 271 with amendments), at http://konsument.gov.pl/files/act_on_protection.pdf.

⁹⁴ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. Nr 144, poz. 1204 ze zm. (The Law of 18 July 2002 on Providing Services by Electronic Means, Journal of Laws 2002 No. 144 item 1204, with amendments).

⁹⁵ Program działań na rzecz wspierania elektronicznego handlu i usług na lata 2009-2010, Ministerstwo Infrastruktury, Warszawa, grudzień 2008 r. (Action Programme for an Advancement of the E-commerce and E-services in the Years 2009-2010, Ministry of Infrastructure, Warsaw, December 2008), at <http://www.e-handel.org.pl/Programdzialannarzeczwspieraniaelektronicznegohand.pdf>.

⁹⁶ Protokół ze spotkania nt. Nowelizacji ustawy o świadczeniu usług drogą elektroniczną zorganizowanego przez Ministerstwo Spraw Wewnętrznych i Administracji w dniu 6 kwietnia 2009r. (Minutes of the meeting on the Amendment to the Law on Providing Services by Electronic Means organised by the Ministry of Interior Affairs and Administration, 6 April 2009).

⁹⁷ CERT.GOV.PL, at http://www.cert.gov.pl/portal/cee/38/77/About_us.html.

⁹⁸ Agencja Bezpieczeństwa Wewnętrznego (Internal Security Agency) is a governmental agency responsible for the internal security of the Republic of Poland, at http://www.abw.gov.pl/portal/en/17/14/Our_Mission.html.

On 9 March, 2009, the Governmental Program for the Protection of Cyberspace in Poland for 2009-2011 was adopted.⁹⁹ As a result of cooperation between CERT Polska¹⁰⁰ operating within the NASK organisation (*Naukowa i Akademicka Sieć Komputerowa*)¹⁰¹ and the Internal Security Agency, an early warning system (ARAKIS) reporting threats arising on the Internet has been developed.¹⁰² A modified version of this system – the ARAKIS-GOV¹⁰³ – was implemented in the .gov domain in order to support protection of government computer networks and information resources. Its system sensors are installed in over 60 offices of central and local administrations. Since the ARAKIS-GOV system became fully operational (mid-2009), 3,367 security incidents have been reported via this system.¹⁰⁴

Online behavioural marketing and search engine privacy

There are no specific regulations or research in Poland on behavioural marketing and search engine privacy over the Internet. To date, press and Internet publications on privacy threats related to these developments are scarce, however they may influence public awareness on both subjects.¹⁰⁵

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

On 1 January 2005, *Dyżurnet*, a hotline for reporting illegal content on the Internet, was put into operation in Poland.¹⁰⁶ Its mission is to remove any illegal web content that

⁹⁹ Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 -założenia, Warszawa , marzec 2009 (Governmental Program for the Protection of Cyberspace in Poland for 2009-2011 – guidelines, Warsaw, March 2009).

¹⁰⁰ CERT Polska, at <http://www.cert.pl/>, is Poland's first Computer Emergency Response Team, established in 1996.

¹⁰¹ NASK (Naukowa i Akademicka Sieć Komputerowa), at http://www.nask.pl/nask_en/.

¹⁰² ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems in order to detect new threats. It does not in any way monitor the content of the data exchanged by the secured institution with the Internet. It is possible due to the fact that system sensors are installed beyond the secured internal network of the institution, on the Internet side.

¹⁰³ ARAKIS-GOV, at http://www.cert.gov.pl/portal/cee/39/78/ARAKISGOV_system.html.

¹⁰⁴ Internal Security Agency – ABW, Annual Report 2009, Poland 2010, at http://www.abw.gov.pl/portal/en/16/577/Annual_report_2009.html.

¹⁰⁵ "W internecie nikt nie jest anonimowy, ale mamy prawo do prywatności, wydanie internetowe" ("No One is Anonymous Over the Internet, However, We Have the Right to Privacy"), *Gazeta Prawna* (Legal Newspaper Internet edition), 1 February 2010, at http://prawo.gazetaprawna.pl/artykuly/394495,w_internecie_nikt_nie_jest_anonimowy_ale_mamy_prawo_do_prywatnosci.html.

¹⁰⁶ Dyżurnet.pl is the team acting within the framework of the Research and Academic Computer Network (NASK), at <http://www.dyzurnet.pl/en>.

involves child abuse, threatens children's safety, or promotes xenophobia and/or racism. The team's activities are regulated by Polish law and are based on international cooperation with other members of the International Association of Internet Hotline Providers (INHOPE). During its five years of operation *Dyżurnet* has received thousands of reports from the Internet users, most of them related to child pornography (63 percent).¹⁰⁷

TERRITORIAL PRIVACY

Video surveillance

Under the Police Act, the Police may use video surveillance and audio recording in public places, when performing secret investigations, and in the course of protection of public order. Police may also use video surveillance during covert operations. Video surveillance is also used by municipalities and private persons, however there is no regulation concerning this kind of surveillance. There is debate over the use of CCTV by private persons and entities, especially in supermarkets, as some owners placed cameras in locations which enabled them to monitor persons in changing rooms.

Location privacy (GPS, mobile phones, location based services, etc.)

Location data is protected by Article 159 of the Telecommunications Act 2004. It may be revealed only in situations listed in the Law. Data processing is allowed under the condition that consent is obtained from the subject or the data is anonymised. Consent may be withdrawn. Location data must be presented to relevant authorities upon request.¹⁰⁸

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Travel privacy is protected by the LPPD. The use of biometrics in travel documents was regulated by the Passport Documents Act 2006.¹⁰⁹ According to the Act, documents may contain biometrics data related to the face and fingerprints. Far reaching regulations on transborder exchange of biometrics data are contained in the Prüm Treaty 2005 and related EU documents which have yet to be implemented in Poland.

NATIONAL ID & SMART CARDS

Controversy still surrounds the expanded national identification (ID) system. The Electronic Census System (*Powszechny Elektroniczny System Ewidencji Ludności* or PESEL), which has been in operation since the mid-1970s, is the biggest collection of personal data in Poland. Every identity card contains a PESEL number, which is a confirmation of the owner's date of birth and sex. The system is fully computerised. The

¹⁰⁷ Reports of *Dyżurnet.pl* activity, in English at http://www.dyzurnet.pl/en/about_us/download.html.

¹⁰⁸ Article 166 of Telecommunications Act 2004, *supra*.

¹⁰⁹ Journal of Laws No. 143 item 1027.

Government began issuing new ID cards in January 2001. In August 2006, the PESEL II Steering Committee was formed to develop a two-stage identification card which includes biometric data storage. At the end of 2009, Prime Minister Tusk announced that biometric ID will be included as of 2011.¹¹⁰

Physicians in Poland have protested against the latest use of the PESEL number in a new law requiring that all prescriptions must include the PESEL number of the patient in order to qualify for reimbursement. A new prescription will not be honoured by pharmacies unless the physician physically writes a PESEL number on it.¹¹¹

RFID tags

There are no specific regulations for RFID tags. The individual is protected by general data protection and privacy regulations.

BODILY PRIVACY

The Constitution protects bodily privacy from the perspective of protection of private life (Article 47) and inviolability of the person (Article 41(1)). Situations in which the government may interfere with bodily privacy are listed *inter alia* in the Code of Criminal Procedure. It allows for taking of blood, swabs, hair, etc. for investigative purposes (Article 74). These regulations are generally fragmentary and do not fully comply with the requirements of the Constitution and the European Convention on Human Rights. Many authors argue there is no express legal basis for compulsory examinations.¹¹²

Interference with bodily privacy may also take place with regards to prisoners and persons suspected of having infectious diseases.¹¹⁴

WORKPLACE PRIVACY

According to Article 11 of the Polish Labour Code, employers are obliged to respect the dignity and personal life of their workers.

Unfortunately, Polish law does not regulate monitoring at work. This causes many problems in practice and may result in uncontrolled monitoring and/or legal liability for

¹¹⁰ "Tusk: nowe dowody biometryczne za rok" ("Tusk: New Biometric ID in One Year), RMF 24, 30 December 2009, available at <http://www.rmfm24.pl/fakty/polska/news-tusk-nowe-dowody-biometryczne-za-rok,nId,79282>.

¹¹¹ Centrum Medyczne, Current Issues, 20 June 2007, available at <http://www.enel.pl/en/onas/aktualnosc.asp?id=65>.

¹¹² See Arkadiusz Lach, *Granice badań oskarżonego w celach dowodowych* (The Limits of the Investigative Tests of the Accused for Evidential Purposes) 170 and authors quoted (Torun 2010).

¹¹³ Article 118 of the Criminal Executive Code 1997.

¹¹⁴ Article 27 of the Infectious Diseases and Infections Act 2001.

the employer due to intrusion into employee's privacy. Employers are particularly uncertain as to which extent they may access to emails received or sent by workers.

Protection of workplace privacy is therefore based mainly on criminal law, civil law and data protection regulations.

In a judgment dated 1 December 2009,¹¹⁵ the High Administrative Court indicated that the relationship between employer and employee poses a difficulty with regards to employees consenting to monitoring by their employer. As a result the employer may process only the data listed in the Labour Code and other legal acts. In this particular case employees consented to the processing of fingerprints to track time worked. This was held to be unlawful by the court, as the Labour Code does not provide for processing of such data.

HEALTH & GENETIC PRIVACY

Medical records

Medical records in Poland are protected as sensitive data. According to the Health Protection Institutions Act 1991, medical institutions are obliged to protect the medical records of their clients (Article 18). Doctors, nurses, and childbirth assistants are obliged to secure information related to their patients¹¹⁶ unless there is a statutory exception to this rule. Special protection is given to medical records related to psychiatric health.¹¹⁷

The 1996 Act on the Profession of a Doctor and a Dentist imposes a duty of confidentiality in regards to patient information for medical professionals, subject to certain exceptions. The Constitutional Tribunal ruled in March 1998 that requiring doctors to identify the disease of the patient on sick leave certificates violated patients' right to privacy.

Genetic identification

DNA profiles are regarded as sensitive data in Poland, therefore its processing must take place in line with the requirements of the LPPD. The Police Act regulates the processing of DNA profiles for investigative purposes.

Polish law forbids genetic testing for insurance purposes.¹¹⁸ One unsolved problem in Poland is paternity testing. DNA checks without express consent of the persons involved take place and this may have a significant negative effect on the subject's privacy.

¹¹⁵ Case number I OSK 249/09.

¹¹⁶ See Article 40 of the Act on Profession of a Doctor and a Dentist 1996 and Article 21 of the Nurse and Childbirth Assistant Act 1996.

¹¹⁷ See Articles 50-52 of the Psychiatric Health Protection Act 1994.

¹¹⁸ Article 21 (1) Insurance Act 2003, Journal of Laws of 2010 No. 11 item 66.

FINANCIAL PRIVACY

Under the Banking Act of 1997,¹¹⁹ a bank, its staff and other persons involved in the performance of banking operations shall be bound by the obligation of banking secrecy, which shall apply to all information concerning a banking operation, where such information is obtained during negotiations, conclusion and performance of an agreement under which the bank performs such operation (Article 104(1)). Numerous exceptions from the rule are provided by the act (Articles 104-106(d)). Broad exemptions are granted to authorities such as the Police, public prosecutors, and courts. Law enforcement shows a tendency to broaden these exceptions, especially to allow identification of unknown perpetrators.

In April 2000, the Constitutional Tribunal dismissed a challenge to the rights of Polish tax authorities to request confidential information about any individual's bank accounts, bonds and securities. The court held that these powers were important in the fight against bribery and money laundering.¹²⁰ Banks are obliged to inform the authorities in the event of suspicion that its services are being used for terrorist purposes, money laundering or for other crimes (Articles 106 and 106(a) of the Banking Act 1997).

Besides bank information, other kinds of financial information are protected by general regulations (LPPD) and sector regulations, for example insurance law.

E-GOVERNMENT & PRIVACY

E-government in Poland is still underdeveloped. Electronic voting or voting by mail has not yet been introduced. The Information of Subjects Performing Public Tasks Act 2005¹²¹ was changed on 12 February 2010.¹²² According to its Article 4, the Act does not interfere with the LPPD.

OPEN GOVERNMENT

The Parliament approved the Act on Access to Public Information in September 2001, and it went into effect in January 2002. The Act creates a presumption of access to information held by all public entities, private entities who exercise public tasks, trade unions, and political parties. These entities are also required to publish material online. There are exemptions for official or state secrets, confidential information, personal privacy, and business secrets. Appeals are made through the courts. In July 2003, the Polish Access to Public Information Bill came into force, requiring thousands of public institutions such as local government, political parties and schools to put public

¹¹⁹ English version available at <http://www.nbp.pl/homen.aspx?f=en/aktyprawne/prawo.html>.

¹²⁰ "Constitutional Tribunal Allows Treasury to Screen Bank Accounts," *Polish News Bulletin*, 12 April 2000.

¹²¹ Journal of Laws No. 64 item 656.

¹²² Act on Changing the Informatisation of Subjects Performing Public Tasks Act and certain other Acts 2010, Journal of Laws No. 40 item 230.

information on websites.¹²³ The Public Data Bulletin, a system of Internet sites, serves to collect these informational sites in one place.¹²⁴

Poland enacted the Classified Information Protection Act in January 1999 as a condition to entering North Atlantic Treaty Organisation (NATO).¹²⁵ This act has been replaced by the new Classified Information Protection Act adopted on 5 August 2010.¹²⁶ The act covers classified information or information collected by government agencies whose disclosure "might damage interests of the state, public interests, or lawfully protected interests of citizens or of an organisation." There have also been efforts to deal with the files of former employees of the communist era secret police. A law creating a National Remembrance Institute (*Instytut Pamięci Narodowej* or IPN) to allow victims of this secret police agency access to records was approved by the Parliament in October 1998. The files were opened to the public in February 2001.¹²⁷ The Screening Act of 1997 created a special commission to examine the records of government officials who might have collaborated with the secret police. The Commission began work in November 1998. Presently the screening procedure is regulated by Disclosure of Information on the Documents of Security Agencies from 1944 to 1990 and the Content of the Documents.¹²⁸ Under the LPPD, individuals have the right to access and correct records that contain personal information about them from both public and private entities.

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

The Polish Constitution sets out the necessary foundations for the existence of NGOs in Articles 12 and 58. The two basic types of non-governmental organisations in Poland are associations and foundations, regulated respectively by the Law on Associations¹²⁹ and the Law on Foundations.¹³⁰

The Polish history of relations between the government and civil society groups is quite brief. Development of civil society did not begin until 1989. As a result, even though

¹²³ Journal of Laws No. 112 item 1198.

¹²⁴ See <http://www.bip.gov.pl/> (in Polish).

¹²⁵ The Classified Information Protection Act of 22 January 1999, available in English at <http://www.lexadin.nl/wlg/legis/nofr/eur/lxwepol.htm>.

¹²⁶ Journal of Law No. 182 item 1228.

¹²⁷ See David Banisar, "Freedom of Information and Access to Government Records Around the World," At 125, available at http://www.freedominfo.org/documents/global_survey2006.pdf.

¹²⁸ Journal of Laws No. 165 item 1171.

¹²⁹ Act of 4 April 1989 The Law of Associations, Journal of Laws No. 79 item 855, 2001 (with changes).

¹³⁰ Act of 6 April 1984 The Law of Foundations, Journal of Laws No. 46 item 203, 1991 (with changes).

Poland is now an EU Member State, there have not been any significant developments in this area. Civil society is still weak and its influence on policy making is relatively small.¹³¹

Legal grounds for the cooperation between public authorities and NGOs are established in the Act on Public Benefit and Volunteer Work.¹³² This act provides a framework for such cooperation and imposes an obligation on public administration to cooperate with NGOs in public tasks. This obligation concerns cooperation not only with "public benefit organisations" but also all with other NGOs involved in the area of public tasks.

Recent efforts to train and organise NGOs have resulted in better cooperation and communication. The NGO web portal, NGO.pl, consists of an NGO database, forum and links to funding and partnership opportunities.¹³³

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Poland has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol that establishes an individual complaint mechanism.¹³⁴

Poland is a member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. In May 2002, Poland ratified the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).¹³⁵ In November 2001, it signed, but has not ratified, the CoE Cybercrime Convention (ETS No. 185).¹³⁶

In 2006, the European Court of Human Rights found that the monitoring and censorship of an inmate's correspondence violates Article 8 of the European Convention on Human Rights. According to the Court's decision, the opening of a letter from a lawyer is permissible if prison authorities have reasonable cause to believe that it contains an illicit item and suitable guarantees are provided. However, no compelling reasons were found to exist for the opening of letters as a matter of course. The Court reiterated, "it is important to respect the confidentiality of its correspondence since it may concern allegations against prison authorities or prison officials. The opening of letters... undoubtedly gives rise to the possibility that they will be read and may conceivably, on

¹³¹ UN Country Program document for Poland (2004-2005), DP/DCP/POL/1, 5 August 2003.

¹³² Act of 24 April 2003 on Public Benefit and Volunteer Work.

¹³³ <http://english.ngo.pl/>.

¹³⁴ Poland has signed the ICCPR on 2 March 1967 and ratified it on 18 March 1977. It acceded to its First Optional Protocol on 7 November 1991. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹³⁵ Signed 21 April 1999; ratified 23 May 2002; entered into force 1 September 2002.

¹³⁶ Signed 23 November 2001.

occasion, also create the risk of reprisals by prison staff against the prisoner concerned."¹³⁷

Poland is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In November 2001, Poland ratified the United Nations Convention of 2000 against Transnational Organised Crime (the Palermo convention¹³⁸).

On 1 May 2004, Poland joined the European Union and is obliged to respect EU privacy guidelines.

* Updates to the Polish Report published in the 2010 edition of EPHR have been provided by: Andrzej Adamski and Arkadiusz Lach, Nicolas Copernicus University, Poland; Arwid Mednis, Wierzbowski & Wspolnicy, Poland; Katarzyna Szymielewicz, Panoptykon Foundation, Poland.

¹³⁷ European Court of Human Rights, Application No. 20841/02, 6 December 2005, *Drozdowski v. Poland*, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=DROZDOWSKI&sessionid=58714472&skin=hudoc-en>. See also *Janus v Poland*, Application 8713/03, 21 July 2009, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=8&portal=hbkm&action=html&highlight=Poland%20%7C%20drozdowski&sessionid=59445131&skin=hudoc-en>.

¹³⁸ See <http://europa.eu.int/scadplus/leg/en/lvb/l33088.htm>.

REPUBLIC OF PORTUGAL¹

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Portuguese Constitution has extensive provisions on protecting privacy, secrecy of communications and data protection.²

Article 26 provides "everyone shall possess the right to a personal identity, to the development of their personality, to civil capacity, to citizenship, to a good name and reputation, to their likeness, to speak out, to protect the privacy of their personal and family life, and to legal protection against any form of discrimination; the law shall lay down effective guarantees against the procurement and misuse of information concerning persons and families and its use contrary to human dignity; the law shall guarantee the personal dignity and genetic identity of the human person, particularly in the creation, development and use of technologies and in scientific experimentation; deprivation of citizenship and restrictions on civil capacity may only occur in such cases and under such terms as may be provided for by law, and shall not be based on political motives."³

Article 34 provides the inviolability of "personal homes and the secrecy of correspondence and other means of private communication"; "entry into a citizen's home" only by competent judicial authority and after complying with due process requirements; and a bar on non-consensual entry of a person's home at night unless in pursuit of a criminal, or with judicial authorisation as laid down by law. The article also prohibits public authorities from interfering with correspondence, telecommunications or other means of communication unless as provided by law in relation to criminal proceedings.⁴

In 1997, Article 35 of the Constitution was amended to give citizens a right to data protection. The Article provides that "every citizen shall possess the right to access to all computerised data that concern him, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law; the law shall define the concept of personal data, together with the terms and conditions applicable to its automated treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative body; computers shall not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious beliefs, private life or ethnic

¹ The EPHR 2010 "Portugal" report has been updated in July 2010 by João Luís Traça, Miranda Correia Amendoira & Associados, Portugal.

² Constitution of the Portuguese Republic, available at http://app.parlamento.pt/site_antigo/ingles/cons_leg/Constitution_VII_revisao_definitive.pdf.

³ *Id.* at Article 26.

⁴ *Id.* at Article 34.

origins, save with the express consent of the data subject, with authorisation provided for by law and with guarantees of non-discrimination, or for the purpose of processing statistical data that cannot be individually identified; third-party access to personal data shall be prohibited, save in exceptional cases provided for by law; the allocation of a single national number to any citizen shall be prohibited; everyone shall be guaranteed free access to public-use computer networks, and the law shall define both the rules that shall apply to cross-border data flows and the appropriate means for protecting personal data and such other data as may justifiably be safeguarded in the national interest; personal data contained in manual files shall enjoy the same protection as that provided for in the previous paragraphs, as laid down by law."⁵

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The 1998 Act on the Protection of Personal Data adopts the European Union (EU) Data Protection Directive requirements into Portuguese law.⁶ It limits the collection, use and dissemination of personal information in manual or electronic form. It also applies to video surveillance or "other forms of capture, processing and dissemination of sound and images." It replaces the 1991 Act on the Protection of Personal Data with Regard to Automatic Processing.⁷

Sector-based laws

On 18 August 2004, the Parliament enacted Law No. 41/2004,⁸ which implemented the European Directive on Privacy and Electronic Communications (2002/58/EC) without incorporating the Directive's Article 13 on unsolicited communications. That article had already been implemented in Law No. 7/2004,⁹ which also implemented the European Directive on Electronic Commerce (2000/31/EC). Law No. 41/2004 also repealed Law No. 69/98,¹⁰ which implemented the European Union Telecommunications Privacy Directive (1997/66/EC).

⁵ *Id.* at Article 35.

⁶ Act No. 67/98 of 26 October 1998. Act on the Protection of Personal Data (transposing into the Portuguese legal system Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), available at <http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM>.

⁷ Law No. 10/1991. Lei da Protecção de Dados Pessoais face à Informática, amended by Law No. 28/94 of 29 August 1994, Aprova medidas de reforço da protecção de dados pessoais.

⁸ Law No. 41/2004, available at <http://www.anacom.pt/template20.jsp?categoryId=125319&contentId=221691>.

⁹ Law No. 7/2004, of 18 August 2004, available at <http://www.anacom.pt/template20.jsp?categoryId=125300&contentId=221668>.

¹⁰ Law No. 69/98 of 28 October 1998, available at http://www.cnpd.pt/bin/legis/nacional/lei_6998.htm.

DATA PROTECTION AUTHORITY

The National Data Protection Commission (*Comissão Nacional de Protecção de Dados*, or CNPD) is charged with controlling and enforcing the laws on the protection of personal data.¹¹ The Commission functioned as part of the National Parliament until 2004. In 2004, it became an independent agency that is directly responsible to the Parliament.¹² Its functions are to register existing databases containing private data, authorise, and control such databases, issue directives, and oversee the Schengen Information System (SIS). The number of investigations and inspections conducted has remained fairly stable in the past six years, fluctuating between a low of 183 in 2004 and a high of 223 in 2001. There were 207 investigations and inspections conducted in 2006. Inspections fell somewhat in 2006 when CNPD, in cooperation with law enforcement, asked those authorities to inspect video surveillance systems. The number of complaints received by the Commission has also remained somewhat steady: 173 in 2003, 156 in 2004, 183 in 2005, 177 in 2006, and an increase to 212 in 2008.¹³

The number of referrals for criminal prosecution to the Public Prosecution Service is very low due to the existence of a fine system for the transgressions. There was one referral in 2001, two in 2002, one in 2003, and none from 2004 through 2006. The Commission applied 47 fines in 2006, totalling 75,000 EUR, but in 2008, there was a substantial increase in the fines applied: 151 fines, totalling approximately €366,000.¹⁴ The Commission authorised 2,146 databases in 2006, compared with 2,440 in 2004 and 1,858 in 2005.¹⁵ It issued opinions on obtaining subscriber information from telecommunications providers, access to marketing databases by the Criminal Investigation Police, denied access by the Information and Security Service to the information system of the Aliens and Frontiers Department, approved transborder data flows to the United States when the receiving company promised to protect the personal data collected pursuant to European data protection legal standards,¹⁶ The Commission also recently prohibited Google's Street View from gathering photographs of Portuguese

¹¹ Comissão Nacional de Protecção de Dados <http://www.cnpd.pt/>.

¹² Law No. 43/2004 of 18 August 2004, available at <http://www.dre.pt/pdfgratis/2004/08/194A00.PDF#page=21>.

¹³ Comissão Nacional de Protecção de Dados, Relatório de Actividades (summary of activities), 2008, available at http://www.cnpd.pt/bin/relatorios/anos/RELATORIO_2008.pdf.

¹⁴ *Id.* at 3.

¹⁵ Email from Clara Guerra, International Relations, CNPD. Portugal, to Guilherme Roschke, Electronic Privacy Information Center, 19 July 2007 (on file with EPIC).

¹⁶ Comissão Nacional De Protecção De Dados, Decisões da Comissão (CNPd's decisions), available at <http://www.cnpd.pt/bin/decisooes/decisooes.asp>.

streets for its databases due to concerns about the company's ability to guarantee the anonymity of Portuguese citizens and of their vehicles.¹⁷

In January 2008, the CNPD launched "Project DADUS" by establishing a website aimed at schools. The project allows teachers to access educational content through a data protection programme.¹⁸ It is aimed at creating awareness among students between the ages of ten and 15 about issues relating to privacy and data protection. Teachers and their classes are granted access to interactive themed "units" with activities and talking points.¹⁹ The Project covers a wide range of subjects, including an introduction to data protection, as well as modules on social networking and video surveillance.²⁰

In 2008, the CNPD hosted the Iberian-American Meeting on Data Protection which approved Directives for the Harmonisation of Data Protection in the Iberian-American Community and the Lisbon Declaration. The Lisbon Declaration highlighted the recent developments in some countries for the adoption of data protection and stressed the importance of safeguarding the fundamental right to data protection in international transborder flows of personal data.²¹

MAJOR PRIVACY & DATA PROTECTION CASE LAW

There is no major privacy or data protection case law to report in the last two years.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The Penal Code has provisions against unlawful surveillance and interference with privacy.²² Evidence obtained by any violation of privacy, including that of the home, correspondence, or telecommunications, without the consent of the affected party is null

¹⁷ "Google assegura que serviço Street View é legal", *Expresso*, 4 August 2010, available at <http://auiou.expresso.pt/google-assegura-que-servico-street-view-e-legal=f597681>.

¹⁸ Article 29 Data Protection Working Party, 12th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2008, 16 June 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/12th_annual_report_en.pdf.

¹⁹ See http://dadus.cnpd.pt/content_pages/view/4.

²⁰ See <http://dadus.cnpd.pt/unidades/indice>.

²¹ Article 29 Working Party on Data Protection, 11th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2007, 24 June 2008, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf.

²² Penal Code, Chapter VII, §§ 190-98, available at http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=109&tabela=leis.

and void.²³ An inquiry was opened in October 1994 on illegal surveillance of politicians after microphones were discovered in the offices of a state prosecutor and several ministers.²⁴ The Portuguese government ordered cellular telephone companies to assist with surveillance in October 1996.²⁵ There are also specific laws on the SIS,²⁶ cybercrime,²⁷ and counselling centres.²⁸

National Security Legislation

Law 67/98 on the Protection of Personal Data expressly applies to any processing of personal data for the purposes of public and state security.²⁹

Data Retention

In July 2008, a law requiring communication providers to store customer data for a period of one year was enacted.³⁰ It is aimed at preventing serious crime through mandating the retention of data relating to communications made by telephone, text message, media message or email, where such data is likely to identify those communications' source, destination, time, and type.³¹ The data includes customer information, which includes personally identifying information as well as a user's location.³² The law requires those handling communications data to be authorised and registered by the CNPD.³³

²³ Code of Penal Procedure, Article 126, paragraph 3, available at http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=199&tabela=leis.

²⁴ "Bug Found in Portuguese State Prosecutor's Office," Reuters European Business Report, 27 April 1994.

²⁵ "Portugal to Tap Mobile Phones in Drugs War," Reuters World Service, 9 October 1996.

²⁶ Law No. 2/94 of 19 February 1994 (Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen), available at http://www.cnpd.pt/bin/text/legis/nacional/lei_294.htm.

²⁷ Law No. 109/2009 of 15 September 2009 (Sobre a Lei do Cibercrime) (Law on Cybercrime), available at <http://dre.pt/pdf1sdip/2009/09/17900/0631906325.pdf>.

²⁸ This law creates a duty of confidentiality for counseling centers, Article 15, Law No. 3/84 (Educação sexual e planeamento familiar).

²⁹ Law 67/98, op. cit., at Art. 4 (7).

³⁰ Law No. 32/2008 (Transpõe a Directiva da Retenção de Dados, relativa à conservação de dados das comunicações electrónicas), July 2008, available at http://www.cnpd.pt/bin/legis/nacional/Lei32-2008_retencao_dados.pdf.

³¹ *Id.* at Article 4.

³² Brett Allan King, "Portugal Cabinet Urges One Year Retention of Communication Provider Customer Data," BNA Privacy and Security Law Report, 24 September 2008, available at <http://www.bna.com>.

³³ *Id.*

National Databases for Law Enforcement and Security Purposes

Decree Law 309/2007 was promulgated in an effort to fight fraud. It aims at regulating the linking of governmental databases and the government's methods for sharing data. The new law allows government bodies to access third party databases to aid their activities.³⁴

National and International Data Disclosure Agreements

There are no national nor international data disclosure agreements to report.

Cybercrime

Portuguese Law 109/2009 on Cybercrime was implemented in order to regulate and punish cybercrime, including perpetrators who unlawfully access others' IT system or deletes, modifies, or suppresses data stored electronically in an IT system.³⁵ The penalties imposed by this legislation are not, however, contingent on the violation of any rights to the protection of personal data. Notwithstanding, the statute does impose procedural safeguards aimed at protecting personal data, namely by requiring judges to deliberate on whether data or documentation likely to reveal personal data apprehended in the course of an investigation ought to be allowed as evidence,³⁶ and by requiring national authorities to act in conformance with the 1998 Law on the Protection of Personal Data when they cooperate with competent foreign law enforcement bodies.³⁷

Critical Infrastructure

There is nothing to report with respect to critical infrastructure.

INTERNET & CONSUMER PRIVACY

E-commerce

In January 2004, the Decree-Law No. 7/2004 for information society services³⁸ started to regulate, among other things, unsolicited communications for marketing purposes providing direct measures of protection against the invasion of privacy. The Decree-Law transposes EU Directive 2000/31 and, at Article 22, prohibits the sending of unsolicited communications for the purposes of marketing unless the parties to whom they are sent ask request that no further such communications be sent to them.³⁹

³⁴ Decree Law No. 309/2007, available at <http://www.dre.pt/pdf1sdip/2007/09/17300/0633606340.PDF>.

³⁵ See <http://www.dre.pt/pdf1s/2009/09/17900/0631906325.pdf>.

³⁶ *Id.*, at Art. 16(3).

³⁷ *Id.*, at Art. 20.

³⁸ Available at <http://www.anacom.pt/text/render.jsp?contentId=976170> (English version). Decreto-Lei No. 7/2004 of 7 January 2004, D.R. No. 5 (Série I-A), 7 January 2004, available at <http://www.anacom.pt/render.jsp?contentId=952094&channel=text> (official version in Portuguese).

³⁹ *Id.*

In September 2005, the CNPD published general principles related to electronic communications for political marketing. The principles clarified that opt-in rules apply not only to commercial marketing, but also to the electronic messages of a civil or political nature.⁴⁰

In March 2009, the Decree Law No. 62/2009 modified Decree-Law No. 7/2004 by requiring that the Directorate-General of the Consumer (DGC) update a list of people nationwide who wish not to receive general commercial communications. Organisations that promote the sending of commercial messages for direct marketing purposes are required to check the list, updated quarterly by the DGC and available upon request. The practice of sending communications materials electronically to people on the lists is prohibited.⁴¹

Cybersecurity

The protection of online personal data against deliberate attempts at accessing the IT systems of others is covered by Law 109/2009 on Cybercrime. Further, Law 41/2004 imposes duties on any company offering network or electronic communications services to take adequate steps to guarantee an adequate level of cybersecurity,⁴² and ensure that the electronic communications that they offer are inviolable.⁴³

Online Behavioural Marketing and Search Engine Privacy

There is nothing to report with respect to online behavioural marketing and search engine privacy.

Online Social Networks and Virtual Communities

There is nothing to report with respect to online social networks and virtual communities.

Online Youth Safety

There is nothing to report with respect to online youth safety.

⁴⁰ CNPD, "Princípios Gerais Aplicáveis ao Marketing Político no Âmbito das Comunicações Electrónicas," September 2005, available at http://www.cnpd.pt/bin/orientacoes/marketing_politico.htm and http://ec.europa.eu/justice_home/fsj/privacy/docs/policy_papers/Portugal/marketing_politico.pdf.

⁴¹ Decree-Law No. 62/2009 of 10 March 2009, D.R. number 48 (Series I) of 10 March 2009, available at <http://www.anacom.pt/render.jsp?contentId=978476&channel=text> (English version). Decreto-Lei No. 62/2009, of 10 March 2009, D.R. n.º 48 (Série I), 10 March 2009, available at <http://www.anacom.pt/render.jsp?contentId=956777&channel=text> (official version in Portuguese).

⁴² Law 41/2004 of 18 August 2004, Article. 3(1) and 3(2), available at <http://www.cnpd.pt/bin/legis/juris/decisoos/Lei41-2004.pdf>.

⁴³ *Id.* at Article 4(1).

TERRITORIAL PRIVACY

Video surveillance

Law 207/2005⁴⁴ sets the means of any electronic (including video) surveillance for road safety used by law enforcement agencies.⁴⁵ The system is limited to specific and determined purposes: catching traffic infractions, traffic control, locating stolen or illegal vehicles, and use as evidence of a crime.⁴⁶ The installation of the surveillance methods should be directed, as much as possible, to capture images of vehicles.⁴⁷ Information from the system may be released for didactic and statistical purposes, as long as no individuals or vehicles are identifiable.⁴⁸ The CNPD published a clarification in response to many inquiries concerning the surveillance.⁴⁹ The clarification states that according to the law these systems do not need CNPD approval. The equipment should be registered with the CNPD, and the make, model, and serial number of the surveillance equipment used is published on the CNPD website.

In 2006, Law 51/2006 on the use of video surveillance to monitor traffic as well as other incidents entered into force.⁵⁰ That law grants permission to "Estradas de Portugal" (Roads of Portugal) to install roadway video surveillance equipment in the interests of road safety. All such installation is subjected, however, to the terms of Act No. 67/98, particularly the requirement of prior notification to the CNPD.

In August 2007, Portugal published a new law punishing improper handling of visual data with fines up to EUR 10,000 and directed captured images to be deleted if the threat did not actually materialise.⁵¹

In October 2008, three Portuguese cities were authorised to be equipped with CCTV cameras.⁵²

⁴⁴ Ministério da Administração Interna, Decreto-Lei No. 207/2005, 29 November 2005, available at <http://www.dre.pt/pdfgratis/2005/11/229A00.pdf>.

⁴⁵ Law No. 207/2005 of 29 November 2005, available at <http://www.cnpd.pt/bin/legis/nacional/DL207-2005-RADARES.pdf>.

⁴⁶ *Id.* at Article 10.

⁴⁷ *Id.* at Article 3.

⁴⁸ *Id.* at Article 18.

⁴⁹ CNPD, "Sistemas de Vigilância Electrónica Rodoviária Utilizados Pelas Forças de Segurança: Esclarecimento da CNPD," 16 May 2006, available at <http://www.cnpd.pt/bin/relacoes/comunicados/16-05-06.HTM>.

⁵⁰ Article 29 Working Party on Data Protection, Tenth Annual Report, June 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/10th_annual_report_en.pdf.

⁵¹ Law 33/2007, available at <http://www.cnpd.pt/bin/legis/nacional/Lei33-2007-vvg-taxis.pdf>.

⁵² Oporto, Portimão and Fátima. "Big Brother Will Be Watching You," The Portugal News Online, 25 October 2008 <http://theportugalnews.com/>.

On 14 July 2008, the CNPD issued an opinion on the use of video surveillance and set down conditions, including: using the system at night if possible, not recording sound, and preventing private houses from being recorded.⁵³

Location Privacy (GPS, Mobile Phones, Location Based Services, etc.)

Article 7 of Law 41/2004 requires any company in the course of providing electronic communication services that process information about a data subject's location, to process that data anonymously.⁵⁴ The data processor must also inform the data subject of the types of location data that will be processed, how long the data will be kept, and for what purposes the data is being processed.⁵⁵

Travel Privacy (Travel Identification Documents, Biometrics, etc.) and Border Surveillance

A new vehicle identification system was introduced that requires all information about a vehicle to be stored on a chip-equipped driver's license.⁵⁶ The government has addressed how such a system may impact privacy rights.⁵⁷

NATIONAL ID & SMART CARDS

Law No. 7/2007 established a national identification card,⁵⁸ or *Cartão de cidadão* ("Citizen Card"), which contains personal information about each citizen and is mandatory for all citizens. The use of the card has become widespread with thus far over 3.5 million card bearers.⁵⁹ Details on the face of the card include parentage, date of birth, nationality, photograph, and the individual's civil, tax, health insurance, and social security numbers.⁶⁰ The various numbers cannot be cross-referenced or interconnected other than in ways permitted by the data protection authority.⁶¹ The law also expressly

⁵³ Available at <http://www.cnpd.pt/bin/decisoos/2008/htm/par/par27-08.pdf>.

⁵⁴ Article 7 (1) of Decree-Law No. 41/2004, 18 August 2004, available at <http://www.cnpd.pt/bin/legis/juris/decisoos/Lei41-2004.pdf>.

⁵⁵ *Id.*, at Article 7(4).

⁵⁶ Decree-Law No. 112/2009, 18 May 2009, available at <http://dre.pt/pdf1sdip/2009/05/09500/0310703118.pdf>.

⁵⁷ Decree-Law No. 112/2009, 18 May 2009, available at <http://dre.pt/pdf1sdip/2009/05/09500/0310703118.pdf>.

⁵⁸ Law No. 7/2007, of 5 February 2007, creating a citizen's card and regulating its use and emission, available at <http://www.cnpd.pt/bin/legis/nacional/Lei7-2007-cartao-cidadao.pdf>; see also http://www.cnpd.pt/bin/legis/leis_nacional.htm.

⁵⁹ At http://www.cartao decidadao.pt/index.php?option=com_content&task=view&id=196&Itemid=103&lang=pt.

⁶⁰ Article 7, Law No. 7/2007 of 5 February 2007, available at <http://www.cnpd.pt/bin/legis/nacional/Lei7-2007-cartao-cidadao.pdf>.

⁶¹ Article 16, Law No. 7/2007 of 5 February 2007, *supra*.

prohibits retention of the card, including by photocopy, unless authorised by law.⁶² The card contains an integrated circuit which stores one's residential address, a fingerprint, digital authentication and digital signature certificates, space for further data elements as well as space for personal data of the choice of the individual.⁶³ The law prohibits the physical detention, as well as photocopying, of the card without the consent of the card owner, except as otherwise prescribed by law.⁶⁴ The biometric fingerprint may only be accessed upon the citizen's consent, and only the police and justice officials may otherwise compel a citizen to identify him or herself via the biometric fingerprint.⁶⁵ The card has a document number, comprising the civil identity number plus extra digits, but the number is unique to the document – if the document is re-issued, the new document must have a different number.⁶⁶ The digital certificates on the card are accessible only by the use of a PIN and are revocable, but must be replaced when revoked.⁶⁷ A citizen is entitled to know what is contained in the card – including in electronic storage and in the files created during the issuance of the card – and has the right to correct information, suppress improperly collected information, and insert omitted information.⁶⁸

RFID tags

In 2004, the CNPD published guidelines on the usage of Radio Frequency Identification (RFID) technology,⁶⁹ biometrics,⁷⁰ and surveillance systems.⁷¹ These guidelines establish the need for the registration of the databases connected to these systems, and determine the criteria for the use of such systems to comply with data protection principles. The data controller must not only comply with the terms of Law 67/98 on Personal Data Protection, but must also clearly label the RFID-capable product and issue a warning to its user whenever the RFID system is remotely activated.

⁶² Article 5(1) Law No. 7/2007 of 5 February 2007, *supra*.

⁶³ Article 8, Law No. 7/2007 of 5 February 2007, available at <http://www.cnpd.pt/bin/legis/nacional/Lei7-2007-cartao-cidadao.pdf>.

⁶⁴ Article 5(3), Law No. 7/2007 of 5 February 2007, *supra*.

⁶⁵ Article 14, Law No. 7/2007 of 5 February 2007, *supra*.

⁶⁶ Article 17, Law No. 7/2007 of 5 February 2007, *supra*.

⁶⁷ Article 18, Law No. 7/2007 of 5 February 2007, *supra*.

⁶⁸ Article 39, Law No. 7/2007 of 5 February 2007, *supra*.

⁶⁹ Comissão Nacional para a Protecção de Dados, "Identificação por radiofrequência," 13 January 2004, available at <http://www.cnpd.pt/bin/decisoes/2004/hm/del/del009-04.htm>.

⁷⁰ Comissão Nacional para a Protecção de Dados, "Principles for the use of biometric data in controlling access and monitoring hours worked," 26 February 2004, available at <http://www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm>.

⁷¹ Comissão Nacional para a Protecção de Dados, "Princípios sobre o tratamento de videovigilância," 19 April 2004, available at <http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm>.

BODILY PRIVACY

The CNPD has issued guidelines on the use of biometrics in the workplace.⁷² These guidelines state that collecting biometric data for the purpose of monitoring a worker's productivity does not constitute *per se* a violation of the worker's bodily privacy,⁷³ but the data subject may object to such processing of his or her data where there are "compelling legitimate grounds relating to his particular situation," as per the terms of Article 12, Act No. 67/98 of 26 October 1998. Collection of biometric data may not be carried out in a manner so intrusive that it violates the data subject's constitutional rights to personal identity, private life, and bodily integrity.⁷⁴ Whether these rights have been violated depends on the purpose for which the data is to be used, which must be proportionate and non-discriminatory.⁷⁵

WORKPLACE PRIVACY

In 2003, the CNPD published "Guidelines on Privacy in the Workplace."⁷⁶ These guidelines establish that information and contents of phone calls, emails, and Internet access for the private use of a worker is protected as private data and must be respected as such by the employer, although the employer is still free to restrict such personal use of office facilities by the employee by using generic means of monitoring, and avoiding as far as possible any individual monitoring of personal data.

In 2007, the CNPD prohibited the reporting of worker absenteeism due to strike action.⁷⁷ The Director-General of Administration and Public Works (DGAEP) collects aggregate data on workers on strike and publishes the aggregate data on the Internet. The Director-General of taxation began to require that the identification numbers of workers on strike be submitted within 48 hours, via a software system, so that income could be properly allocated. The CNPD found that the automatic and independent treatment of strike data called into question the legality of this decision. Article 35 of the Constitution, as well as Art. 7 of Act No. 67/98, prohibit computer treatment of political convictions, and the CNPD determined that strike participation is a political conviction. Therefore, absence due to strike action should be reported normally along with other absences as opposed to receiving discriminatory treatment which singles out strike participation.

⁷² Comissão Nacional para a Proteção de Dados, "Principles for the use of biometric data in controlling access and monitoring hours worked," 26 February 2004, *supra*.

⁷³ *Id.*, at paragraph 28.

⁷⁴ *Id.*, at paragraph 44.

⁷⁵ *Id.*, at paragraphs 49-52.

⁷⁶ Comissão Nacional para a Protecção de Dados, "Princípios sobre a Privacidade no Local de Trabalho," 29 October 2002, available at <http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm>.

⁷⁷ CNPD, Deliberação No. 225/2007 of 30 May 2007, available at <http://www.cnpd.pt/bin/decisoies/2007/htm/del/del225-07.HTM>.

In January 2009, Law 7/2009 was passed to limit the rights of employers with respect to their employees' biometric and other personal data.⁷⁸ In essence, the law prohibits employers from examining employees' private emails that pass through the employer's computer network.⁷⁹ Furthermore, employees cannot be asked to provide information regarding their personal life and whether they are pregnant, except when the provision of such information relates to the employees' capability to perform their jobs.⁸⁰ Any use of employees' biometric data must first be notified to the CNPD prior to processing such information.⁸¹

HEALTH & GENETIC PRIVACY

Medical records

In January 2005, the Health Ministry published a regulation⁸² adding HIV and AIDS to the list of diseases requiring compulsory notification by any doctor to the Epidemic Surveillance Centre of the National Health Institute. The stated objective is to identify the epidemic pattern of the disease. The form in question included all the data needed to identify a specific individual, including the person's full name. A later regulation⁸³ provided for the reduction of the personal information to be collected, after negotiations with the National Data Protection Commission.

Genetic Identification

Law 12/2005 regulates the collection and use of health and genetic information.⁸⁴ It defines genetic information as health information of hereditary characteristics of one or more people, and includes information collected from family histories that can, by itself, declare the genetic make-up of a person.⁸⁵ Medical information should be kept confidential and secure, may only be used by the medical system in accordance with express written consent, and should be kept separate from other personal information in

⁷⁸ Law No. 7/2009 of 12 February 2009, amended by Law No. 105/2009 of 14 September 2009, available at http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=1047&tabela=leis.

⁷⁹ "Surveillance: New Employee Privacy Law in Portugal," Real Time Community: IT Compliance, 17 February 2009, at http://www.realtime-itcompliance.com/laws_regulations/2009/02/surveillance_new_employee_priv.htm.

⁸⁰ Article 17, Law No. 7/2009 of 12 February 2009, amended by Law No. 105/2009 of 14 September 2009.

⁸¹ Article 18, Law No. 7/2009 of 12 February 2009, *op. cit.*

⁸² Regulation No. 103/2005 of 25 January 2005, available at <http://www.dre.pt/pdfgratis/2005/01/017B00.PDF#page=39>.

⁸³ Regulation No. 258/2005 of 16 March 2005, available at <http://www.dre.pt/pdfgratis/2005/03/053B00.PDF#page=71>.

⁸⁴ Law No. 12/2005 of 26 January 2005 on Personal Genetic and Health Information, available at <http://www.cada.pt/uploads/c28ce883-8bb0-4aa4.pdf>.

⁸⁵ *Id.* at Article 6.

databases by means of tiered access controls.⁸⁶ Genetic information not of immediate impact on health (i.e., recessive genes, questions of identity, pre-symptomatic or pre-natal) is not considered medical information and should be kept separate from medical files, and inaccessible by doctors in the case of healthy persons.⁸⁷ Genetic tests for disease in healthy individuals can only be performed with informed written consent and after counselling. The law also regulates the usage of genetic tests, prohibiting their use in denying health and life insurance or increasing premiums.⁸⁸ Employers may not request genetic tests, even with the consent of employees, but they may require such tests either where the particular workplace may pose a health risk to workers with specific diseases or genetic susceptibilities – in which case such tests may never be used to the worker's detriment – or where there is a very serious risk to public health that is relevant to the worker's health, in which case the testing must be undertaken by an agency or body that is independent of the employer.⁸⁹ Neither adoption services nor future adoptive parents may request tests or use information from tests already performed in adoption cases.⁹⁰

A law was published to regulate a national DNA database for criminal investigations and, upon the data subject's consent, for civil identification as well.⁹¹

FINANCIAL PRIVACY

In September 2009, the CNPD adopted Resolution No. 765/2009, containing the principles governing the processing of personal data for the purpose of internal communication acts of irregular financial management (ethics hotlines).⁹² It regulates the rights of people accused of committing financial irregularities in so-called "whistleblowing" situations, particularly the accused person's rights to access, correct, and delete data relating to her that is being processed as a result of such allegations. Such data must be collected in a way that is proportionate to the data subject's rights, despite the existence of a public interest in promoting corporate transparency and responsibility.⁹³ While the data subject must have access to the data and be able to correct it where it is

⁸⁶ *Id.* at Article 4.

⁸⁷ *Id.* at Article 6.

⁸⁸ *Id.* at Article 12.

⁸⁹ *Id.* at Article 13.

⁹⁰ *Id.* at Article 14.

⁹¹ Article 29 Data Protection Working Party, 11th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2007, 24 June 2008, *supra*.

⁹² CNPD emite orientações para "Linhas de ética", 21 Sept. 2009, available at http://www.cnpd.pt/bin/orientacoes/DEL765-2009_LINHAS_ETICA.pdf.

⁹³ *Id.* at 7.

incomplete or incorrect, she has no right whatsoever to find out the identity of the accuser.⁹⁴

E-GOVERNMENT & PRIVACY

In November 2005, the CNPD released a deliberation on privacy and electronic voting.⁹⁵ The CNPD based its recommendations on its evaluation of the 2004 and 2005 elections. The evaluation stresses the principles of transparency, security, and integrity. Specifically, the CNPD recommended that: electronic voting be publicly debated and the public be informed by political and technological leaders about electronic voting; that software be open source and capable of being audited before and after voting; that electronic voting be used to complement, not replace, traditional methods; that voter-verified paper trails be used; that separate machines hold voter information and vote collection databases – the former being preferably done on paper; and that the communication of voting information be encrypted and not use the public Internet or telephone network.

OPEN GOVERNMENT

Law No. 46/07 of 24 August 2007 (*Regula o Acesso aos Documentos Administrativos* or Law on the Regulation of, and Access to, Administrative Documents) provides for access to government records in any form by any person.⁹⁶ Documents can, however, be withheld for "internal or external security," secrecy of justice, and personal privacy.⁹⁷ Documents with personally identifiable information can only be accessed by the subject of that information or third parties with "direct, personal, and legitimate" interest.⁹⁸ Access to environmental information is regulated by Law No. 19/2006, which implements EC Directive 2003/4/CE.⁹⁹

The access to government documents is overseen by the Commission for Access to Administrative Documents (CADA), an independent parliamentary agency. The CADA can examine complaints, provide opinions on access, and decide on classification of systems. CADA's decisions are not binding, so if an agency continues to deny access,

⁹⁴ *Id.* at 11-13.

⁹⁵ CNPD, "A Privacidade dos Eleitores no Voto Electrónico," 14 November 2005, available at http://www.cnpd.pt/bin/orientacoes/Delib_voto_electronico.pdf.

⁹⁶ Law No. 46/2007 of 24 August 2007, available at <http://www.cada.pt/modules/news/article.php?storyid=86>. (Portuguese version available at http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=931&tabela=leis&ficha=1&pagina=1).

⁹⁷ *Id.* at Article 6 (1), Law No. 46/2007 of 24 August 2007, available at <http://www.cada.pt/modules/news/article.php?storyid=86>.

⁹⁸ *Id.* at Article 6 (5), Law No. 46/2007 of 24 August 2007, *supra*.

⁹⁹ Law No. 19/2006 of 19 June 2006, regulating access to information on the environment, available at <http://www.cada.pt/uploads/7f000001-a20b-9451.pdf>.

further appeal can be made to an administrative court. CADA processed 330 complaints in 2004, 306 in 2005, 310 in 2006, and 361 in 2007.¹⁰⁰

OTHER RECENT FACTUAL DEVELOPMENTS

There is nothing to report under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

There is nothing to report with respect to this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

The European Court of Human Rights had 262 cases pending against Portugal by the end of 2009 and had issued a total of 17 judgments. These cases involved alleged violations of rights unrelated to personal data protection.¹⁰¹ In 2001, the European Court of Human Rights has found Portugal to be in breach of Article 8 of the European Convention on Human Rights in the case of *Antunes Rocha v Portugal*, where a governmental security investigation into the personal life of a NATO employee was found to have been a violation of the employee's right to respect for her private life.¹⁰² This case was, however, based on facts that had occurred prior to the implementation of a wide range of legislation guaranteeing the protection of personal data, such as the 1998 Act on the Protection of Personal Data.

On 10 December 1948 the General Assembly of the United Nations, of which Portugal is a member, adopted and proclaimed the Universal Declaration of Human Rights.¹⁰³ Portugal ratified the International Covenant on Civil and Political Rights on 15 June 1978.¹⁰⁴

Portugal is a member of the Council of Europe (CoE). It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁰⁵ It has also signed and ratified the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) (Convention No.

¹⁰⁰ Last statistics available at <http://www.cada.pt/modules/smartsection/item.php?itemid=121>.

¹⁰¹ European Court of Human Rights, Annual Report 2007, at 140, available at http://www.echr.coe.int/NR/rdonlyres/C25277F5-BCAE-4401-BC9B-F58D015E4D54/0/Annual_Report_2009_Final.pdf.

¹⁰² *Antunes Rocha v Portugal*, No. 64330/01, 31 May 2005, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=antunes%20%20rocha%20%2064330/01&sessionid=63534646&skin=hudoc-en>.

¹⁰³ Available at <http://www.un.org/Overview/rights.html>.

¹⁰⁴ International Covenant on Civil and Political Rights, 16 December 1966 available at <http://www.cirp.org/library/ethics/UN-covenant/>.

¹⁰⁵ Signed 22 September 1976; ratified 9 November 1978; entered into force 9 November 1978.

108),¹⁰⁶ and, in November 2001, signed the CoE Convention on Cybercrime (ETS No. 185) but has not ratified it.¹⁰⁷ In January, 2007, Portugal also ratified the Additional Protocol to Convention No. 108 regarding supervisory authorities and transborder data flows, which entered into force on 1 May 2007.¹⁰⁸ Portugal is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

¹⁰⁶ Signed 28 January 1981; ratified 2 September 1993; entered into force 1 January 1994.

¹⁰⁷ Signed 23 November 2001.

¹⁰⁸ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181, available at <http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?PO=POR&MA=999&CM=3&CL=ENG>).

ROMANIA

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Romanian Constitution¹ adopted in 1991 recognises under Title II (Fundamental Rights, Freedoms, and Duties) the rights of privacy, inviolability of domicile, and freedom of conscience and expression. Article 26 of the Constitution states, "(1) Public authorities shall respect and protect the intimate, family and private life. (2) Any natural person has the right to freely dispose of himself unless by this he causes an infringement upon the rights and freedoms of others, on public order or morals." Article 27 states, "(1) The domicile and the residence are inviolable. No one may enter or remain in the domicile or residence of a person without consent. (2) Derogation from provisions under paragraph (1) is permissible by law, in the following circumstances: for carrying into execution a warrant for arrest or a court sentence; to remove any danger against the life, physical integrity, or assets of a person; to defend national security or public order; to prevent the spread of an epidemic. (3) Searches may be ordered only by a magistrate and carried out exclusively under observance of the legal procedure. (4) Searches at night time shall be prohibited, except in cases of *flagrante delicto*." Article 28 states, "Secrecy of the letters, telegrams, and other postal communications, of telephone conversations, and of any other legal means of communication is inviolable." According to Article 30, "(6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of person, and the right to one's own image."

The Romanian Constitutional Court had two important decisions taken in 2009 and 2010 regarding the interpretation of the right to privacy, as enshrined by the Constitution. The first is Decision No. 1258 of 8 October 2009² that considered unconstitutional the national implementation of the Data Retention Directive.³

¹ Available in English at http://www.cdep.ro/pls/dic/act_show?ida=1&idl=2&tit=2#t2c2s0a26.

² Curtea Constitutională a României, Decision No. 1258 of 8 October 2009 on the objection of unconstitutionality of the provisions of Law No. 298/2008 on the retention of data generated or processed by the providers of publicly available electronic communications services or public communications networks, which also amends Law No. 506/2004 on the processing of personal data and privacy protection in the electronic communications sector, Official Monitor No. 798, 23 November 2009, available in Romanian at http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf, An unofficial English translation of the Decision is available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf. The content of Decision 1258 is discussed *infra* in the text.

³ Law No. 298/2008 regarding the Retention of the Data Generated or Processed by the Public Electronic Communications Service Providers or Public Network Providers, as well as the modification of Law No. 506/2004 regarding the Personal Data Processing and Protection of Private Life in the Field of Electronic Communication Area, published in the Official Monitor No. 780, 21 November 2008, available in Romanian at <http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-2982008-privind-pastrarea-datelor-de-trafic-informational.html>.

The second decision is the Constitutional Court ruling 415 of 14 April 2010⁴ regarding the unconstitutionality of the law establishing the National Agency of Integrity⁵ that obliged all the interest and income declarations of certain public servants to be published on the Internet. In this case, the Court considered that "the obligation stipulated by the law to publish the declarations of assets and interests on the Web pages of the entities where the persons, according to the legal provisions, have to submit them, as well as their transmission to the Agency to be published on its website, breach the right to respect and protection of private life ensured by Article 26 of the Fundamental Law as well as by article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, by the unjustified exposure, in an objective and sensible way, on the Internet page, of the data related to the assets and interests of people who, according to the law, have the obligation to submit declarations of assets and interests."

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

In November 2001, the Parliament enacted Law No. 676/2001 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector⁶ and Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data.⁷ These laws follow very closely the European Union Telecommunications Privacy (1997/66/EC) and Data Protection (1995/46/EC) Directives respectively. Romania joined the European Union on 1 January 2007.⁸

Law No. 676/2001 provides for specific conditions under which privacy is protected with respect to the processing of personal data in the telecommunications sector. In 2004, Law No. 676/2001 was, practically speaking, replaced by Law No. 506/2004,⁹ which closely follows Directive 2002/58/EC of the European Parliament and the Council on personal

⁴ Official Monitor No. 294, 5 May 2010, Decision available in Romanian at <http://www.legestart.ro/Decizia-415-2010-referitoare-exceptia-neconstitutionalitate-dispozitiilor-cap-I-Dispozitii-generale-art-1-9-ale-art-11-lit-e-f-g-ale-art-12-alin-2-ale-art-13-ale-art-1-%28MzUyMjMw%29.htm>.

⁵ Law No. 144/2007 for setting-up, organizing, and functioning of National Agency for Integrity - Official Monitor No. 359, 25 May 2007, text available in Romanian at http://www.dreptonline.ro/legislatie/lege_agentie_nationala_integritate_144_2007.php.

⁶ Official Monitor No. 800, 14 December 2001, available at <http://www.riti-internews.ro/lg676.htm>.

⁷ Official Monitor No. 790, 12 December 2001, available at <http://www.avp.ro/leg677en.html>.

⁸ See http://europa.eu/abc/european_countries/eu_members/romania/index_en.htm.

⁹ Law No. 506/2004, Official Monitor No. 1101, 25 November 2004, Romanian text available at <http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-privind-prelucrarea-datelor-cu-caracter-personal-si-protectia-vietii-private-in-sectorul-comunicatiilor-electronice.html>. An English summary is available at <http://www.glin.gov/view.action?glinID=119653>.

data processing and privacy protection in the electronic communications sector. This directive repealed and replaced Directive 1997/66/EC.¹⁰

Law No. 506/2004 divides the task of enforcing the personal data protection laws between two institutions: the National Regulatory Authority for Communication (later renamed the National Authority for Management and Regulations in Communications – Romania, or ANCOM¹¹) for issues related to electronic communications and the People's Advocate Office (later renamed the Data Protection Authority, or ANSPDCP), which handles issues related to privacy. In this sense, ANCOM has competence in relation to: security measures for electronic communication; non-compliance with invoice issuing conditions; infringement of the obligations regarding the presentation and restriction of calling; and connected line identification.

Law No. 677/2001 applies to the processing of personal data, that is carried out totally or partially through automatic means, as well as to the processing of personal data through other means that are part of, or destined for, an evidence system.

A new civil code was approved in July 2010 by the Romanian Parliament.¹² The Code has not come into force, and it is unclear when this will happen – the Parliament needs to issue a new law to establish it. The code's new text includes provisions relating to private life and a series of articles stating the respect to private life, the right to dignity, the interdiction against public use of images, voice recordings, manuscripts, correspondence, or other personal documents without the owner's consent (except in cases where the use is legally allowed by the law because the material is of justified public interest). The new text also defines that a breach of someone's private life (Article 74 – "Breaches of private life") includes: capturing or using a person's image or voice in a private space without the person's consent; broadcasting images representing private space interiors without the consent of the legal occupant; placing private life under observation by any means, except for the express cases provided by the law; broadcasting news, debates, inquiries, or written and audio-visual coverage of a person's private, personal or family life, without the person's consent; broadcasting materials including images of a person under treatment in medical assistance units as well as personal data related to health, diagnosis, prognosis, treatment, or other circumstances and facts related to the disease including autopsy results, without the consent of the person involved or, in case of the person's death, of that of his family or authorised persons; using, with malice, the name, image, voice, or likeness of another person; broadcasting or using correspondence, manuscripts, or other

¹⁰ Directive 2002/58/EC, Official Journal of the European Community L. 201, 31 July 2002.

¹¹ See <http://ancom.org.ro/index.aspx>.

¹² Official Monitor No. 511, 24 July 2009, text available in Romanian at http://www.avocatnet.ro/content/articles/id_16209/Noul-Cod-civil-2009-publicat-in-Monitorul-Oficial-Text-integral.html.

personal documents including data relating to the domicile, residence, or phone numbers of a person or his (her) family members, without the person's consent.¹³

Some of these provisions were criticised by several mass-media organisations¹⁴ as limiting freedom of expression, especially where there is a public interest for a specific case. The government's reply was to present a proposal in 2009 to add another, rather vague article to the draft. This would make all the above-mentioned privacy provisions concerning inapplicable if interfering with the right were "allowed by the law or international conventions and agreements regarding human rights to which Romania is part". It also says: "Exercising the constitutional rights and freedoms in good faith and by observing the international conventions and agreements Romania is part of, is not an infringement of the rights provided for by this section."

The civil code has not yet come into force. It may enter into force on 1 October 2011 if the law establishing this date, as suggested by the Ministry of Justice, is adopted by Parliament.¹⁵

Sector-based laws

In 2002, the National Audiovisual Council¹⁶ issued regulations regarding privacy and television and radio programs in Decision No. 80 of 13 August 2002, Regarding the Protection of Human Dignity and the Right to Protect One's Own Image. These established a few privacy principles. Article 6 states, "(1) Any person has a right to privacy, privacy of his family, his residence and correspondence. (2) The broadcasting of news, debates, inquiries, or audio-visual reports on a person's private and family life is prohibited without that person's approval." According to Article 7, "It is forbidden to broadcast images of a person in his or her own home or any other private place without that person's approval; (2) It is forbidden to broadcast images of a private property, filmed from the inside, without its owner's approval."¹⁷

¹³ See Bogdan Manolea, Privacy in the New Draft Civil Code, 18 March 2009, at <http://legi-internet.ro/blogs/index.php/2009/03/18/viata-privata-in-noul-proiect-de-cod-civ>.

¹⁴ See Activewatch, Libertatea Presei în România 2009 (2009 Freedom of Press in Romania) Annual report,, 3 May 2010 available at <http://www.activewatch.ro/uploads/FreeEx%20Publicatii%20Raport%20Freeex%20%203%20mai%202010.pdf>; Annual report Hotnews.ro, "UPDATE: CJI, AMP, COM, CRP, AJR si MediaSind protesteaza fata de prevederile noului Cod Civil referitoare la presa: Guvernul dovedeste 'opacitate' si comite 'abuzuri'" ("UPDATE CJI, AMP, COM, CRP, AJR and MediaSind are protesting against the provisions of the new civil code: The Government proves to be 'opaque' and makes 'abuses'."), 16 March 2009, available at http://economie.hotnews.ro/stiri-media_publicitate-5496874-update-cji-amp-com-crp-ajr-mediasind-protesteaza-fata-prevederile-noului-cod-civil-referitoare-presa-guvernul-dovedeste-opacitate-comite-abuzuri.htm.

¹⁵ Draft laws from the Ministry of Justice available at Hotnews.ro's website, at <http://www.hotnews.ro/stiri-esential-7543964-predoiu-noul-cod-civil-noul-cod-penal-vor-intra-vigoare-1-octombrie-2011.htm>.

¹⁶ See <http://www.cna.ro/-English-.html>.

¹⁷ Mariana Stoican, "Measures to Protect Human Dignity and Personal Image Rights," Radio Romania International, 2002, available at <http://merlin.obs.coe.int/iris/2002/10/article21.en.html>.

In 2009 the Parliament adopted a new Penal code¹⁸ that includes a new crime called "Breaching privacy". Article 226 states: "(1) The harm unlawfully brought to private life by photographing, capturing, or recording images, listening in by technical means or audio recording a person within a home, a room, or an out-building related to it, or a private conversation, is punished with imprisonment from six months to a year or a fine. (2) Revealing, broadcasting, presenting, or transmitting unlawfully the sounds, conversations, or images covered by paragraph (1), to another person or to the public, is punished with imprisonment from three months to two years or a fine. (3) The criminal case starts at the complaint of the harmed person."¹⁹

DATA PROTECTION AUTHORITY

The new authority for protecting personal data, the National Authority for the Supervision of Personal Data Processing (ANSPDCP), was created by Law No. 102/2005,²⁰ which replaced the previous supervisory authority (called "The People's Advocate").²¹ The law regulates the transfer of the database from the People's Advocate Office to the ANSPDCP. Due to the delay in creating the ANSPDCP, the Romanian Government issued Emergency Ordinance No. 131/2005, which delayed the authority's creation date until 31 December 2005.²² The new authority's internal regulations were adopted on 2 November 2005.²³ The ANSPDCP opened in February 2006, and the new institution began to provide advice and help with respect to infringements of the personal data legislation.²⁴ Starting with 21 January 2008, the authority of ANSPDCP was extended²⁵ to include monitoring the implementation of Law No. 298/2008 on data retention.

The budgetary cuts of 2009 have significantly affected the activity of the Authority. The budget allocated for the year 2009 was insufficient to provide payment for the 50 people the ANSPDCP was supposed to hire. In fact, by August 2009, only 35 positions had been

¹⁸ Law No. 286/2009 regarding the Penal Code, Official Monitor No 510, 24 July 2009. Full text available in Romanian at <http://www.avocatnet.ro/UserFiles/articleFiles/noul-cod-penal-2009-text-integral.html>.

¹⁹ The term "unlawfully" used in the text corresponds to the Romanian word "fara drept" which literally translated is "without right". This latter expression means that there may be some cases when interferences with the right to privacy is done in accordance with the law – for example in case of a penal investigation with a judge approval.

²⁰ Official Monitor No. 391, 9 May 2005, available in Romanian at http://www.legi-internet.ro/index.php/Legea_privind_infiintarea_org/82/0/.

²¹ See <http://www.avp.ro/indexen.html>.

²² Official Monitor No. 883, 3 October 2005, available at http://legi-internet.ro/blogs/index.php?title=autoritatea_naa_355_ionala_de_supraveghe&more=1&c=1&tb=1&pb=1.

²³ Published in the Official Monitor No. 1004 of November 11 2005, available at <http://legi-internet.ro/blogs/index.php?p=348&more=1&c=1&tb=1&pb=1#more348>.

²⁴ See <http://www.ceecprivacy.org/main.php?s=2&k=romania>.

²⁵ See http://www.dataprotection.ro/index.jsp?page=Comunicat_presa_extindere_atributii&lang=ro.

filled.²⁶ The budget for 2009 did not allow the Authority to do any investigations outside Bucharest.²⁷

Since June 2006, four decisions have been issued by the ANSPDCP regarding the application of the personal data legislation. These decisions establish standard notification forms (modified in 2008),²⁸ categories of sensitive personal data processing operations,²⁹ notification exemptions,³⁰ and situations in which the simplified notification form for personal data processing may be used.³¹ In 2007, the ANSPDCP issued several orders. One order, for example, implemented the online registry of controllers; another abolished the notification fee.³² In 2007 the ANSPDCP also issued a decision regulating the transfer of personal data to third countries.³³ In 2008 and 2009 the ANSPDCP continued to regulate the personal data processing notification regime³⁴ by issuing a decision concerning the standard notification form and the procedure for the authorisation of health-related data processing.³⁵ The decision also mandates that, in the absence of the subject's express written consent, an operator must first obtain authorisation from ANSPDCP before processing such data.

In 2008, the ANSPDCP applied sanctions against a legal firm for unlawful processing of personal data (they didn't respect an individual's right to be informed that his/her data are being processed) and against a financial private company for not having observed a client's right of intervention.

²⁶ Bogdan Manolea, Romania National Report – EDRI , December 2009, available at <http://www.ldh-france.org/IMG/pdf/ETUDE-ROUMANIE-EN.pdf>.

²⁷ ANSPDCP 2009 Annual Report, available in Romanian at <http://www.dataprotection.ro/servlet/ViewDocument?id=623>.

²⁸ Decision No. 95/2008, Official Monitor No. 876, 24 December 2008.

²⁹ Decision No. 89/2006, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=184027#>.

³⁰ Decision No. 90/2006, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=184028>.

³¹ Decision No. 91/2006, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=184029>.

³² The abolishment was made by Government Emergency Ordinance No. 36/2007 – Official Monitor No. 335, 17 May 2007. See http://legi-internet.ro/blogs/index.php?title=doua_vesti_bune_de_la_anspdc&more=1&c=1&tb=1&pb=1.

³³ See Decision No. 28/2007, available at http://www.dataprotection.ro/images/PDF/decizie_282007_en.pdf.

³⁴ See http://m.cdep.ro/pls/legis/legis_pck.http_act?ida=84675.

³⁵ Decision No. 101/2008, Official Monitor Part I, No. 4, 19 January 2009.

In 2009, ANSPDCP³⁶ fined two mobile phone companies for sending SMS to their subscribers despite the fact that the subscribers had not opted to receive them³⁷ as well as a financial company that sent unsolicited SMS messages to a former client.³⁸ A private company was fined for having used video cameras to monitor access to public/private areas without having previously notified the authority. Furthermore, the company was fined for having used the images for other purposes than just surveillance.³⁹

The Authority has made it clear several times that the practice, common to several commercial companies, of asking for the client's CNP (Personal numerical code – a unique identifier for each physical person) on invoices is not supported by any legislation. The legislation covering the content of invoices⁴⁰ does not imagine the introduction of the CNP on the invoice. And, according to the ANSPDCP, there are no provisions requiring the CNP for any other tax.⁴¹

The ANSPDCP also fined a local company that provided Internet Street View services because it did not notify the Authority or blur the collected personal data (faces, car numbers, etc.).⁴²

In 2010, another telecommunications company was fined for having disclosed its subscribers' personal data to an insurance company without first asking for their consent.⁴³

The ANSPDCP issued a decision in 2009 that established a framework for the processing of health-related personal data.⁴⁴ In 2010, the Authority sanctioned Health Insurance House in Brasov county for posting its list of debtors on its website, some 30,000 local

³⁶ See ANSPDCP 2009 Annual report, *supra*.

³⁷ See "Romanian Authority Fines Vodafone for Spamming," Trading Markets, 2 March 2009, available at <http://www.tradingmarkets.com/.site/news/Stock%20News/2201164/> and http://www.dataprotection.ro/index.jsp?page=Comunicat_presa_investigatie_Orange&lang=en.

³⁸ See http://www.dataprotection.ro/index.jsp?page=Comunicat_presa_investigatie_la_Garantibank_International_N.V._Sucursala_Romania_SA&lang=en.

³⁹ See http://www.dataprotection.ro/index.jsp?page=Comunicat_de_presa_referitor_la_investigatia_efectuata_la_SC_Petrom_SA&lang=en.

⁴⁰ Art. 155(5) of Title VI of the Fiscal Code transposing Art. 226 of Directive 112/2006/EC.

⁴¹ See Bogdan Manolea, "CNP-ul nu trebuie cerut de magazinele online," ("E-commerce businesses may not ask for the CNP"), 4 September 2009, at <http://legi-internet.ro/blogs/index.php/2009/09/04/cnp-nu-trebuie-cerut-magazinele-online>, See also the ANSPDCP 2008 Annual report at <http://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro> and 2009 Annual report, *supra*.

⁴² See ANSPDCP 2009 Annual report, *supra* at 27-28.

⁴³ See http://www.dataprotection.ro/index.jsp?page=stire_10052010&lang=ro.

⁴⁴ Decision No. 101/2008, which entered into force on 1 January 2009, is described in English in Tuca Zbarcea Asociatii, "Legal Bulletin January 2009," at 6-7, available at http://brconline.eu/library/Legal-Bulletin-Tuca_Zbarcea_&_Asociatii-January-2009.pdf.

individuals along with their personal data (name, address, the number of their contracts).⁴⁵

The Authority may be asked for its opinion on normative acts. For example, in 2008 it was consulted for 17 normative acts. However, such requests are not obligatory for an institution/body, and such opinions are not published on the ANSPDCP's website or in any official newspaper, not even *Monitorul Oficial*.

Between 2006 and 2009, the Authority carried out a series of activities in to elevate personal data protection awareness, most of them directed at the local public authorities. These awareness activities also included a joint conference with the Romanian Banks' Association regarding personal data protection and processing within the financial and banking sectors.⁴⁶ The ANSPDCP has also been involved in awareness activities, usually in partnership with the public sector (Prefects' offices in several counties, Police Inspectorates), the private sector (professional associations in real estate, notaries public, Chambers of Commerce), and the educational sector (universities in Sibiu and Tg. Jiu).⁴⁷

The ANSPDCP has also organised the "Open Doors Event" and several other events on the occasion of the European Data Protection Day (28 January).

According to a 2008 EU report on the citizens' perception regarding the protection of their personal data, Romanian citizens were poorly informed and educated about data protection issues.⁴⁸ Only 42 percent of Romanians were concerned about giving their personal data online, about 36 percent answered they did not know whether legislation in the domain was enough to solve online personal data issues, 47 percent had no idea they had the right of access to their personal data retained by others and 79 percent did not know of the existence of the Romanian data protection authority.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

At the beginning of 2010, the Bucharest Tribunal confirmed the decision of a local Bucharest court imposing upon the town hall of one of the Bucharest districts damages of €10,000 damages to a an individual whose personal data had been posted on the town hall's website identifying him as someone who had the right to free local transport. The website showed not only individuals' names, but also addresses, identification numbers, details of certain social cases, and details of medical conditions such as HIV infection.⁴⁹

⁴⁵ ANSPDCP, press release of 7 July 2010, available in Romanian at http://www.dataprotection.ro/?page=stire_03072010&lang=ro.

⁴⁶ See ANSPDCP, Buletin Informativ trim. II, at 2, at <http://www.dataprotection.ro/servlet/ViewDocument?id=391>.

⁴⁷ See *supra* <http://www.ceecprivacy.org/main.php?s=2&k=romania>.

⁴⁸ See http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

⁴⁹ See "Romania: Moral damages for publishing personal data online," EDRI-gram No. 8.4, 24 February 2010, at <http://www.edri.org/edriagram/number8.4/romanian-case-moral-damages-personal-data>.

In 2009, the Bucharest Tribunal ruled that two publications⁵⁰ had to pay moral and material damages to an actress for having infringed her right to private life and image by posting incorrect, unverified information about her in their publications. The decision was not final, however, and the publications decided to appeal.

Also in 2009, a famous couple obtained an interim judicial restraining order against a local tabloid, requiring it to take down photos taken by paparazzi during their holiday in France and prohibiting it from publishing photos of the couple during their private moments.⁵¹

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Intercepting telephone calls, opening correspondence, and other similar actions are regulated by Criminal Procedure Code and Law No. 51/1991 on National Security in Romania.⁵²

The Criminal Procedure Code was modified several times. A new section (V¹) on the use of audio and video recordings for interception purposes was introduced. The section establishes the conditions under which video and audio recordings may be made, including the interception of telephone calls. Therefore, according to Article 91¹ of the Criminal Procedure Code, recordings on magnetic tape can be used as evidence if the following conditions are complied with: there are reasons to believe that a crime has been, or is about to be, committed; the criminal deed related to which the recording is made is a crime investigated *ex-officio*; the recording is useful in finding out the truth; and the authority that carries out the wiretap has been properly authorised to do so. The authority competent to issue such an authorisation is the President of the Court who would be competent to judge the case or another judge appointed by the President. The authorisation to wiretap is given for a period of up to 30 days and can only be extended for subsequent 30 days periods, and may not exceed a maximum period of 120 days. The law also compels law enforcement authorities to report specific information about their wiretapping: the authorisation given by the judge, the numbers of the telephones among

⁵⁰ "Daniela Nane ar putea primi 150.000 de euro de la Spy și Gardianul" ("Daniela Nane Could Receive 150.000 Euros from Spy and Gardianul"), MediaFax.ro, at <http://www.mediafax.ro/life-inedit/daniela-nane-ar-putea-primi-150-000-de-euro-de-la-spy-si-gardianul-4136452>.

⁵¹ Diana Popescu, "Andreea Marin și Ștefan Bănică i-au bătut pe paparazzii care i-au filmat pe plajă" ("Andreea Marin and Ștefan Bănică Have Won against the Paparazzi that Filmed Them on the Beach"), Gandul.ro, 3 March 2009, at <http://www.gandul.info/media-advertising/andreea-marin-si-stefan-banica-i-au-batut-pe-paparazzii-care-i-au-filmata-pe-plaja-4016732> and Activewatch, *Libertatea Presei în România 2009*, *supra* at 26.

⁵² Nicolae Volonciu, *Penal Procedure Treatise*, 509-514 (Ed. Padeia 1999).

which the calls take place, the names of the people carrying out the conversations, if known, the date and time at which each communication took place; and the item number of the roll or tape on which the recording is made.

The new Criminal Procedure Code adopted in 2010 will change these rules.⁵³ It is not clear yet when it will enter into force, but no sooner than one year after its adoption. Article 138 of the new code establishes the special techniques of surveillance which are detailed in Articles 139-153. These include: interception of conversations and communications; access to a computer system; video, audio, or photographic surveillance; locating and tracking through technical means; obtaining lists of telephone calls; retaining, submitting, or searching postal correspondence; requiring and obtaining, according to the law, data relating to financial transactions as well as a person's financial data; the identity of the subscriber, owner, or user of a telecommunication system or of an access point to a computer. Basically, these special techniques need to be approved by a judge (specifically a judge of rights and liberties) at the request of a prosecutor for a maximum period of 30 days if certain conditions are met. One of these conditions is to investigate a crime listed in the Criminal Procedure Code or one that may be punishable by imprisonment for a minimum of seven years. In emergencies, the prosecutor can also authorise these special techniques for a period of 48 hours, after which the measures need to be approved by a judge. If the judge does not approve the techniques, then all the recorded data must be destroyed.

Chapter V of the new Criminal Procedure Code, which includes Articles 154-155, will regulate the data conservation, partly replacing some provisions ("Procedural Provisions regarding Cybercrime") of the Law No. 161/2003 on Anti-Corruption. The same conditions as those above will apply; the one difference is that the period for using these special techniques is extended to a maximum of 90 days.

Law No. 51/1991 on National Security in Romania allows the interception of calls in cases of crimes against the state and terrorism acts, but only as a result of a mandate issued⁵⁴ by the Romanian Supreme Court (High Court of Cassation and Justice)

At the beginning of 2005, several cases appeared in the press with regard to the Romanian secret service intercepting the phone calls of journalists and other public figures. On 27 January 2005, the Chief of the Romanian Secret Service (SRI), Ioan Timofte, explained⁵⁵ that the phone calls of a number of Romanian and foreign journalists in Romania were intercepted for several months. The reason was that they were suspected of sabotage and crimes against Romanian National security. The Romanian Press Club and the Board of the Foreign Press in Romania Association

⁵³ Law No. 135/2010 on the Penal procedure Code, Official Monitor No. 486, 15 July, 2010.

⁵⁴ For further details, see Adrian Petre, Catalin Grigoras – Audio and Audio-video recordings, at 11-14 (Ch Beck, 2010).

⁵⁵ Dan Bucura, Gabriela Stefan, "There are paid and recruited journalists by foreign information services," *Adevarul*, 27 January 2005.

protested⁵⁶ and demanded that SRI publicly announce the names of the monitored journalists. SRI refused, claiming that it cannot reveal information that may affect national security. The Defence Commissions in the Romanian Parliament, after hearing the testimony of the people involved, have concluded that the interceptions were legal.⁵⁷ Another case involved the Anticorruption Prosecutor (PNA) from the Mures County (Andreea Ciuca, ex-president of the Mures Tribunal), who monitored the phones of more than 70 local journalists, local and national press headquarters, and lawyers for more than 13 months from 24 April 2003 to 25 May 2004.⁵⁸ No information or explanation was offered by PNA.

According to the former director of a Romanian Secret Service unit, the cost of wiretapping one telephone line is €150 to €200 per hour⁵⁹ including all interception and transcription costs. According to President Traian Basescu, approximately 6,370 telephones were wiretapped in 2005. Figures provided by the human rights organisation Helsinki Committee (APADOR-CH) show that, in 2002, a telephone line was wiretapped for an average of 220 days. Journalists from the newspaper *Adevarul* estimated that every intercept generates about 30 minutes of recorded conversation per day.⁶⁰ If the average per day were to climb to 60 minutes, total government spending on wiretaps would double, reaching an amount higher than the annual budget for any Ministry in Romania. For example, in 2005, the Romanian Ministry of Culture had a budget of €235 million.

During the period from 1991 to 2003, the conversations of more than 20,000 persons were intercepted under judicial orders. Another 14,000 interception mandates were issued between 1991 and 2002 at the request of national security bodies. Out of the 5,500 watched persons, only 620 were sent to court and just 238 were found guilty.

In February 2006 public concern about illegal interception led the Parliamentary Commission that supervises the Romanian Secret Service's (SRI) activities to open a supervisory procedure to inspect the SRI wiretapping centres.⁶¹

⁵⁶ "SRI Does Not Publicize the Names of the Surveilled Journalists," Hotnews.ro, 1 February 2005, available in Romanian at http://www.hotnews.ro/articol_14162-SRI-nu-face-publice-numele-ziaristilor-urmariti.htm.

⁵⁷ Ion M. Ionita, "Virgil Ardelean Pretends That the Intention to Intercept Journalists Calls Started from a Provocation," *Adevarul*, 27 January 2005.

⁵⁸ Adina Anghelescu, Razvan Savaliuc, "PNA has illegally intercepted the journalists phones," *Ziua*, 3 February 2005.

⁵⁹ "Extremely High Romanian Wiretapping Costs," EDRI-gram, Number 4.4, 1 March 2006, available at <http://www.edri.org/edriagram/number4.4/romania>. More info in Romanian at http://legi-internet.ro/blogs/index.php?title=cine_si_cit_ne_asculta&more=1&c=1&tb=1&pb=1.

⁶⁰ See <http://web.archive.org/web/20061206195718/http://www.adevarulonline.ro/arhiva/2006/Februarie/1343/174646.html>.

⁶¹ See <http://web.archive.org/web/20070608095723/http://www.ziua.ro/display.php?id=194466&data=2006-02-24>.

In another case, also begun in February 2006, a judge of the Bucharest Tribunal ordered the SRI to produce all of the authorisations obtained for intercepting the phone calls of Romanian businessman Dinu Patriciu and other employees of the Rompetrol company.⁶² The judge eventually convicted SRI of breaching the right to privacy of correspondence and Article 8 of the European Convention of Human Rights. The court required SRI to pay moral damages of RON50,000 because of the very long period in which his phones were tapped – a year and three months, with no real motives. Both the SRI and Patriciu appealed, and in May 2009, the Bucharest Court of Appeal upheld the Tribunal's decision.

The case has now reached the Supreme Court of Justice, which will have the final word. The trial started there in November 2009.⁶³

National security legislation

In response to international terrorism events, Romania has adopted specific legislation that directly attempts to combat terrorism. Law No. 508/2004⁶⁴ establishes the conditions in which the Investigating Division on Terrorism and Organised Crime, a new unit created within the Prosecutor's Office from the Supreme Court of Justice, will operate. The unit has the authority to investigate crimes related to terrorism.

A law on combating and preventing terrorism was passed in November 2004 (Law No. 535/2004⁶⁵), changing the previous normative acts⁶⁶ that were in force since 2001. The law allows the surveillance or interception of electronic communications, as well as investigation of computer systems, where there are activities that might be considered threats to national security. The surveillance activities need to be approved by the General Prosecutor within the Supreme Court of Justice and authorised by the Supreme Court's judges. The warrant for interception or investigation cannot exceed six months.

Data retention

Some provisions related to the recording of traffic data were introduced by the Law on Anti-Corruption No. 161/2003⁶⁷ in order to prevent and combat cybercrime. Under this

⁶² See <http://www.hotnews.ro/stiri-esential-5401491-dinu-patriciu-obtinut-castig-cauza-procesul-intentat-sri.htm>; see also http://www.atac-online.ro/la-zi_/sri---in-boxa-acuzatilor_2514.

⁶³ See <http://www.jurnalul.ro/special/anchete/convorbirile-lui-patriciu-cele-mai-scumpe-pentru-statul-roman-print-562191.html>.

⁶⁴ Official Monitor No. 1089, 23 November 2004.

⁶⁵ Official Monitor No. 1161, 8 December 2004, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=123373>.

⁶⁶ Emergency Ordinance No. 141/2001 on Punishing Terrorist Acts, Official Monitor No. 691, 31 October 2001, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=76738>.

⁶⁷ Official Monitor No. 279, 21 April 2003, available at <http://www.legi-internet.ro/english/romanian-itc-legislation-and-articles/criminalitate-informatica/romanian-cybercrime-law.html>.

law, applicable only to emergencies and properly motivated cases, law enforcement can expeditiously obtain the preservation of computer or traffic data if they could be destroyed or altered, and if there are good reasons to believe that a criminal offence by means of computer systems is being, or is about to be, committed, and for the purpose of gathering evidence or identifying the wrongdoers. During the criminal investigation, the preservation is undertaken by the prosecutor pursuant to an appropriate order and at the request of the investigative body or *ex-officio*, and during trial, by a court settlement. This order is valid for no longer than 90 days, and can be extended only once for a period not longer than 30 days. Earlier versions of the law would have required ISPs to retain internet traffic data for six months, but this provision was not included in the final law.⁶⁸

In 2008, Romania adopted Law No. 298/2008, which mandates that telephone and Internet providers must retain certain data about their customers for six months and make this information available to investigators who have received court permission to access it.⁶⁹ For telephone operators, the relevant data include incoming and outgoing telephone numbers, subscriber's address, location of called number, and call time and duration.⁷⁰ For email and e-call providers, the relevant data include where the email is sent from; the time and date of Internet access; and the subscriber's IP address, physical address, and name.⁷¹ The retained information does not include content or websites visited.⁷² Several civil society groups called on the Ombudsman to "notify the Constitutional Court about the infringement of constitutional rights" posed by the law,⁷³ but the Ombudsman did not consider that the law was unconstitutional and thus did not proceed with the notification.

The law was widely and strongly opposed and, as a result of a case introduced by a Romanian NGO, on 8 October 2009, the Constitutional Court decided that the law was unconstitutional⁷⁴ because "even if indirectly" it breached Article 28 of the Romanian

⁶⁸ New Cybercrime Legislation in Romania," EDRI-gram No. 9, 21 May 2003, available at <http://www.edri.org/edri-gram/number9/cybercrime-law-romania>.

⁶⁹ Official Monitor No. 780, 21 November 2008. An English summary of the law, as well as a link to the full text in Romanian, is available at <http://www.glin.gov/view.action?glinID=217494>; see also "Telephony Operators Compelled to Store Calls Data, for 6 Months," AGERPRES, 20 January 2009, available at <http://www.doingbusiness.ro/en/business-news/9969/telephony-operators-compelled-to-store-calls-data-for-6-months>; "Romania Adopts Data Retention Law," EDRI-gram, Number 6.22, 19 November 2008, available at <http://www.edri.org/edri-gram/number6.22/data-retention-adopted-romania>.

⁷⁰ AGERPRES, *supra*.

⁷¹ *Id.*

⁷² *Id.*

⁷³ Appeal to the Ombudsman filed by Asociatia Pro Democratia (APD), Active Watch - The Media Monitoring Agency (AMP), the Association for the Defence of Human Rights in Romania – the Helsinki Committee (APADOR-CH), the Center for Legal Resources (CRJ), the Centre for Independent Journalism (CJI), and the Assistance Centre for Nongovernmental Organizations (CENTRAS), 5 February 2009, available at <http://www.apador.org/en/index.htm>.

⁷⁴ *Id.*

Constitution stipulating the secrecy of correspondence and Articles 25, 26, and 30 relating to the freedom of movement, privacy, and freedom of expression respectively.⁷⁵

The Court stressed that under the new law "the physical and legal persons, mass users of the public electronic communication services or networks, are permanent subjects to... intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays." The Court also explained that the proportionality principle was not respected: "The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008, is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, but rather the legal obligation with a continuous character, generally applicable, of data retention. This operation equally addresses all the law's subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes."

The Constitutional Court also noted that the traffic data is personal data: "even though Law No. 298/2008 refers to data with a predominantly technical character, these are retained with the scope of providing information regarding a person and his private life".

National databases for law enforcement and security purposes

In 2008, Parliament approved legislation that permits DNA evidence related to 30 different crimes to be collected and stored in a database operated by the Forensic Institute – General Police Inspectorate.⁷⁶ Stored data can only be deleted on the court's or prosecutor's decision, raising the spectre of indefinitely stored information in the event that the court or prosecutor simply forgets to delete it.⁷⁷ It is unclear, though, how the data was obtained before the law was in force. In practice, the Institute of Legal Medicine (IML) did conduct DNA tests and hold DNA samples. Secondary legislation still needs to be produced by the Ministry of Internal Affairs and the Ministry of Justice. According to the initial law, this needed to be ready by 14 November 2008. It is also not clear how

⁷⁵ See <http://www.edri.org/edri-gram/number7.20/romania-data-retention-law-unconstitutional>; Bogdan Manolea, "Legea pastrarii datelor de trafic considerata neconstitutionala - evenimentele majore ale anului 2009" ("Law on Traffic Data Retention Considered Unconstitutional – Major Events in 2009"), 11 January 2010, at <http://legi-internet.ro/blogs/index.php/2010/01/11/leaga-pastrarii-traffic-neconstitutionala>.

⁷⁶ Law No. 76/2008, regarding the National System of Genetic Data (SNDGJ) – entered in force on 14 October 2008, Official Monitor 289, 14 April 2008, available in Romanian at http://www.cdep.ro/proiecte/2008/000/10/8/leg_pl018_08.pdf; see also Bogdan Manolea, "Romania: Is Really Privacy a Topic in the Public Debate?", EDRI-gram No. 7.2, 28 January 2009, available at <http://www.edri.org/edri-gram/number7.2/romania-privacy-in-public-debate>. See also EDRI analysis – to be available soon at <http://www.edri.org>.

⁷⁷ See Manolea, "Romania: Is Really Privacy a Topic in the Public Debate?" *supra*.

access to the database will be made. This, too, should be explained in the (still unwritten) secondary legislation. The Romanian Data Protection Authority hasn't yet been consulted.

National and international data disclosure agreements

No specific information has been reported under this section.

Cybercrime

Law No. 64/2004 was adopted to ratify the Cybercrime Convention, which was signed by Romania on 23 November 2001.⁷⁸ Many provisions of this Convention, especially the definitions of the crimes, were incorporated into Title III (on Preventing and Fighting Cybercrime) of the Anti-Corruption Law No. 161/2003.⁷⁹ Additional laws deal with privacy issues, such as the Patient's Rights Law⁸⁰ or the Law on Combating and Preventing the Traffic of Human Beings.⁸¹

Critical infrastructure

No specific information has been reported under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

In 2002, Law No. 365/2002 on Electronic Commerce⁸² adopted the opt-in principle for unsolicited commercial emails ("spam").⁸³ Law No. 506/2004 also regulates spam, and transposes 2002/58/EC into the Romanian legal system. The law states that the use of electronic mail for the purposes of direct marketing without the prior explicit consent of the user will be sanctioned with a fine between RON5,000 (approx. €1,250) and RON100,000 (approx. €25,000). For companies with a turnover exceeding RON5 million, the fine could amount to as much as 2 percent of revenues. Other provisions regulate the subscribers' right to choose not to be included in printed or electronic directories and to consent to the use of their personal data in the directory. Companies that infringe this right are subject to a fine of between RON30,000 (approx. €7,500) and RON100,000 (approx. €25,000). Law No. 506/2004 further stipulates that the provider of a publicly available electronic communications service must take appropriate measures to

⁷⁸ Official Monitor No. 343, 20 April 2004, available in Romanian at <http://www.legi-internet.ro/ratifycybercrime.htm>.

⁷⁹ Official Monitor No. 279, 21 April 2003, *supra*.

⁸⁰ Law No. 46/2003, Chapter IV, Official Monitor No. 51, 29 January 2003, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=85080>.

⁸¹ Law No. 678/2001, Article 26, Paragraph 2, Official Monitor No. 783, 11 December 2001, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=78346>.

⁸² Official Monitor No. 483, 5 July 2002, available at <http://www.legi-internet.ro/en/e-commerce.htm>.

⁸³ Art. 6(1) provides that "commercial communications through the electronic mail are forbidden, except for the case when the recipient expressed his/her agreement to receive such communications."

safeguard the security of its services, and to inform subscribers and users about any risk of a security breach.⁸⁴

The ANSPDCP has acted to implement the above-mentioned legislation and succeeded in levying three fines in 2008 for unsolicited commercial messages sent by SMS and email and four fines in 2009 for SMS.⁸⁵

ANCOM, the communications authority, with competence in the domain until March 2009, applied fines to 13 legal personal and two natural persons for "spam" as well as two fines for private companies that refused to send the requested information regarding the transmission of unsolicited commercial messages. In 2009, the communications authority levied 14 such fines, five for spam and nine for not providing requested data. Starting in March 2009, the competence in the domain was passed on to the Ministry of Communications and Information Society (MCSI).⁸⁶ Since then, no fines have been issued for this infringement.

Cybersecurity

In recent years there have been several security breaches involving Romanian websites that resulted in the public disclosure of personal data on the Internet. One of the most notorious related to a major online job-search company that processed the data of over 1.3 million users. Because of a software bug, the data (including users' passwords) of more than 10,000 people were publicly disclosed.⁸⁷

Law No. 451/2004 concerning time-stamping has been added to the Romanian portfolio of laws regulating electronic signatures.⁸⁸ A time stamp shows when an electronic document was created or signed. The time stamp registration must be maintained for at least ten years.

Time stamps are usually used to verify an electronic signature, the validity of the electronic signature certificate in the Internet auctions, and authenticate copyright when there is a requirement for a certain date for the copyrighted materials. The law also regulates the liability of time stamp services providers, who are responsible for losses suffered by customers as a result of their failure to comply with the provisions of the law.

⁸⁴ Law No. 506/2004, *supra*.

⁸⁵ See *supra* in the text.

⁸⁶ See Bogdan Manolea, "Sanctionarea spamului: o utopie?!", ("Sanctioning Spam – an Utopia?!"), 16 September 2009, at <http://legi-internet.ro/blogs/index.php/2009/09/16/sanctionarea-spam-utopie>.

⁸⁷ See <http://www.hackersblog.org/2009/02/02/ejobsro-si-pestele-1300000-de-conturi-cu-date-personale/> (in Romanian).

⁸⁸ Official Monitor No. 1021, 5 November 2004, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=122121>.

Providers are required to contract a liability insurance policy or obtain a warranty certificate from a financial institution. The Law entered into force on 5 December 2004.⁸⁹

Online behavioural marketing and search engine privacy

No specific information has been reported under this section.

Online social networks and virtual communities

No specific information has been reported under this section.

Online youth safety

Only a few online safety programmes for youth are available in Romanian, most of them developed by the project *Sigur.info*,⁹⁰ the national contact point for youth awareness on Internet safety that was developed by Save the Children Romania, Focus Romania, and other partners. Similarly, only a few documents on this topic have been issued by electronic communications operators.

TERRITORIAL PRIVACY

Video surveillance

In Romania, the implementation and use of CCTV in public places (especially in schools with unclear privacy settings or purposes⁹¹) is spreading fast due to the fact that Romanian legislation on the matter is quite unclear. According to Law No. 333/2003, CCTV may only be installed by authorised security companies.⁹² Draft secondary legislation that was published by the Romanian Data Protection Authority in order to regulate CCT has been withdrawn from their website with no further explanation.

Location privacy (GPS, mobile phones, location based services, etc.)

The 2009 annual report of the Romanian DPA notes that during that year the Authority investigated a Romanian company offering Street View services (the report does not give the company's name). This company has been fined an unspecified amount for not blurring the personal data in the application (such as the faces of the persons) and for improper information on data protection. The website contested the fine in court, but lost.⁹³

⁸⁹ See Pachiu and Associates, "Information Technology: Law Regarding Temporal Marks," Legal Update, November 2004, at 6, available at <http://www.pachiu.com/pdf/63.pdf>.

⁹⁰ See <http://www.sigur.info>.

⁹¹ See comments in Romanian at <http://forum.portal.edu.ro/index.php?showtopic=63570&st=0&>.

⁹² Law No. 333/2003 regarding the security of valuables, goods, locations and protection of persons, Official Monitor No. 525, 22 August 2003.

⁹³ ANSPDCP 2009 Annual Rapport, *supra* at 27 and 41.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

In 2006, the Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, was transposed into Romanian law. The transposition law⁹⁴ was never adopted until the end of 2008, when an Emergency Governmental Ordinance⁹⁵ was adopted by the Government, repealing the law of 2006. Based on this ordinance, Romania started a pilot project in Ilfov county and began issuing passports with biometric data for all citizens over six years old on 1 January 2009 (the first ones were issued on 30 January).⁹⁶

As revealed by an Inspection Report of the Romanian Data Protection Authority, the present implementation in the pilot project is infringing the Law on Data Protection. Thus, there are no procedures that explain how the biometric data can be gathered. The Passport Authority did not provide the ANSPDCP with any information. What is clear is that there is no special consent required, even though the data collected is sensitive. The Ilfov authorities gathered ten fingerprints and could not prove which two fingerprints were stored in the passport's chip. The General Passport Division (GPD) could not explain why it needed to keep the data for 30 days and why it had kept all the applications since the beginning of the year. GPD didn't have enough security measures implemented (username, password, access card for each user). There were no access logs. All the major problems presented above were rectified by the Authorities after an inspection by the ANSPDCP.⁹⁷

Civil society and religious groups, organised as the "Coalition Against the Police State," organised a protest and an online petition that got more than 15,000 signatures.⁹⁸ The protesters were particularly concerned that the government made this decision in the absence of any public debate about its social, economic, and religious impact.⁹⁹ On February 18, the Romanian Appeal Court rejected a legal challenge brought by NGOs, and on March 3, the Legal Commission of the Senate issued a favourable opinion of the

⁹⁴ Law No. 279/2006 privind personalizarea centralizată a pașapoartelor cu date biometrice (Law No. 279/2006 on the Centralised Personalisation of the Passports with Biometric Data), Official Monitor No. 596, 11 July, 2006.

⁹⁵ Government Emergency Ordinance No. 94/2008 pentru stabilirea unor măsuri privind punerea în circulație a pașapoartelor electronice, precum și producerea altor documente de călătorie (No. 94/2008 for Establishing some Measures regarding the Putting into Circulation of the Electronic Passports, as well as Producing other Travel Documents), Official Monitor No. 485, 30 June 2008, later modified – insignificantly – by Government Emergency Ordinance No. 87/2009, Official Monitor No. 452 1 July 2009.

⁹⁶ *Id.*

⁹⁷ ANSPDCP, Report of 14 April 2009 leaked to the Internet, available in Romanian at <http://victor-roncea.blogspot.com/2009/05/raport-secret-de-pe-masa-lui-geoana.html>.

⁹⁸ "Romania: Protests Against Biometric Passports," EDRI-gram No. 7.3, 11 February 2009, available at <http://www.edri.org/edri-gram/number7.3/romania-biometric-passports-protests>.

⁹⁹ *Id.*

ordinance.¹⁰⁰ By the middle of 2009, the Parliament approved the Emergency ordinance without any modifications.¹⁰¹ By the end of 2009 the system was implemented in almost all the other counties in Romania.

In recent years, the Bucharest transport authority (*Regia Autonomă de Transport Bucurestior* RATB) has implemented a series of smart cards for travellers that include an RFID chip.¹⁰² There is relatively little information about which data are collected and how they are processed (the website does not even have any kind of "Privacy Policy"). Initially, the cards were only nominal with the name and Personal Numerical Code (CNP) written on it. Now there are two types of cards; one nominal (with the name and first seven digits of the CNP on them) and the other without any name. It is unclear at this point if this is a purely anonymous system. RATB has announced that from the beginning of 2010 the old paper tickets would no longer be available, but so far they have not been withdrawn.

NATIONAL ID & SMART CARDS

No specific information has been reported under this section.

RFID tags

No specific information has been reported under this section.

BODILY PRIVACY

Article 5 paragraph 3 of the Law No. 76/2008,¹⁰³ which concerns the judicial decision on the forced taking of biological data from a suspect who refuses to supply it voluntarily, has been challenged in the Constitutional Court. The Constitutional Court rejected the motion, considering that "the person in question, has the right to decide upon the necessity of drawing biological samples from a certain category of people, that is the suspects. [...] The current scope is entirely in agreement with the requirements imposed by Art. 8 paragraph 2 of the Convention for the protection of human rights and fundamental freedoms and by Art. 53 of the Constitution, the involvement of the authority in the intimate and private life being justified".¹⁰⁴

¹⁰⁰ *Id.*

¹⁰¹ Law No. 249/2009 for privind aprobarea Ordonanței de urgență a Guvernului nr. 94/2008 pentru stabilirea unor măsuri privind punerea în circulație a pașapoartelor electronice, precum și producerea altor documente de călătorie (Law No. 249/2009 for Approving Government Emergency Ordinance 94/2008 for Establishing some Measures Regarding the Putting into Circulation of the Electronic Passports, as well as Producing other Travel Documents – see *supra*), Official Monitor No. 462, 3 July 2009.

¹⁰² Official info in Romanian at <http://card.ratb.ro/>.

¹⁰³ Law No. 76/2008, regarding the National System of Genetic Data, *supra*.

¹⁰⁴ Decision 485, 2 April 2009 to Reject the Exception of Unconstitutionality of Art. 5 Paragraph 3 of the Law 76/2008, Official Monitor No 289, 4 May 2009, available in Romanian at <http://www.ccr.ro/cauta/DocumentOpen.aspx?Guid=0accee7c-c031-4c64-aa4d-3050235f8cde&type=D&action=open>.

WORKPLACE PRIVACY

No specific information has been reported under this section.

HEALTH & GENETIC PRIVACY

Medical records

No specific information has been reported under this section.

Genetic identification

No specific information has been reported under this section.

FINANCIAL PRIVACY

No specific information has been reported under this section.

E-GOVERNMENT & PRIVACY

The e-government portal was launched in September 2003.¹⁰⁵ Users can register for interactive and transactional services. Links to all central and local government departments are also included. There are nine fully online interactive services and 687 administrative forms that can be downloaded, filled in, signed, and electronically submitted to the appropriate authority. Moreover, a Unique Form Service system gathers together nine e-services for businesses. The number of available services and forms is continuously being extended. The e-services are designed for large contributors and provide unified access for e-government services.¹⁰⁶

In order for the portal front-office to be a single point of access to e-government services, the National Electronic System (NES) has been developed in parallel to serve as the portal's infrastructure. NES routes requests to a back-end system using XML-based web services. All Romanian institutions are legally required to provide access to their online services through the portal and NES. NES works as a data interchange hub that ensures interoperability with back-end systems across government. A citizen or business has access to the portal, signs on, and fills in and submits a form directed through the NES to the relevant government agency. Moreover, the NES provides a central authentication service allowing users to access all services using a digital certificate.¹⁰⁷

OPEN GOVERNMENT

The Law regarding Free Access to Information of Public Interest was approved in October 2001.¹⁰⁸ The law allows any person to ask for information from public

¹⁰⁵ See <http://www.e-guvernare.ro/>.

¹⁰⁶ ePractice, eGovernment Factsheet – Romania – national Infrastructure (June 2010), available at <http://www.epractice.eu/en/document/288409>.

¹⁰⁷ *Id.*

¹⁰⁸ Law No. 544/2001.

authorities and state companies. The authorities must respond in a maximum of 30 days. There are exemptions for national security, public safety and order, deliberations of authorities, and personal data. Those whose requests have been denied can appeal to the agency concerned or to a court. The Law was amended twice in 2006. The amendments bring "any authority or public institution which uses or manages public financial resources, any state company (*régie autonome*), and any national company, as well as any commercial society under the authority of a central or local public authority and of which the Romanian state or a territorial-administrative unit is a single or major "shareholder" within the scope of the Law, and also makes procurement contracts publicly accessible.¹⁰⁹

The 1999 Law on the Access to the Personal File and the Disclosure of the *Securitate* as a Political Police¹¹⁰ allowed Romanian citizens to access their *Securitate* (secret police) files. It also allowed public access to the files of those aspiring to public office. The law set up the National Council for the Search of Security Archives (CNSAS)¹¹¹ to administer the *Securitate* archives. The law was amended in 2005 and 2006,¹¹² and was declared unconstitutional by the Romanian Constitutional Court in 2008.¹¹³ The CNSAS continues its activities, however, under Governmental Emergency Ordinance No. 24/2008,¹¹⁴ which was passed less than two months after the Romanian Constitutional Court's decision.¹¹⁵

The Law on Protecting Classified Information was enacted in April 2002 at the behest of the North Atlantic Treaty Organisation.¹¹⁶ Its drafters used an expansive view of classification that will limit access to records under the access to information law. The law was strongly criticised by the Opposition and by civil society.¹¹⁷

¹⁰⁹ Law No. 371/2006, Official Monitor No. 837, 11 October 2006; Law No. 380/2006, Official Monitor No. 846, 13 October 2008. Law No. 371/2006, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=185933>. See also Law No. 80/2006, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=185987>.

¹¹⁰ Law No. 187/1999, Official Monitor No. 603, 9 December 1999, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=69500>.

¹¹¹ See <http://www.cnsas.ro/>.

¹¹² Governmental Emergency Ordinance No. 149/2005, Official Monitor No. 1008, 14 November 2005; Governmental Emergency Ordinance No. 16/2006, Official Monitor No. 182, 27 February 2006.

¹¹³ Decision No. 51/2008.

¹¹⁴ Official Monitor No. 182, 10 March 2008.

¹¹⁵ See <http://www.cnsas.ro/>.

¹¹⁶ Law No. 182/2002, Official Monitor No. 248, 12 April 2002, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=81973>.

¹¹⁷ See The Association for the Defence of Human Rights in Romania – The Helsinki Committee (APADOR-CH). The Limits to Information in Romanian Legislation, *supra*.

In 2008, the Bucharest Court of Appeal partially annulled an order by the Prime Minister¹¹⁸ that classified the minutes of all government meetings as state secrets.¹¹⁹ The court ruled that this decision violated Law No. 182/2002 (protection of classified information) and Law No. 544/2001 (free access to public information), and that only passages that implicate national security matters could be withheld.¹²⁰

Specific work done by NGOs – especially the Institute for Public Policies (IPP)¹²¹ and Activewatch¹²² – note that real access to public information is a major problem in Romania: "The legislation in force is not consistently, efficiently, and unitarily put into practice. The reflex attitude of clerks is to treat as secret the information that refers to the administration of the public money and assets. The restricting methods include delaying or ignoring requests or exaggerated costs. On the other hand, citizens, journalists, and non-governmental organisations do not know their legal rights, or the ones who know them do not exercise them because of the constant discouragement by the public clerks."

The IPP's reports of 2009 also show that "only 40 percent of Romania's citizens have heard of the existence of the law on the free access to public interest information" and only 20 percent have ever used the provisions of this law.

The IPP shows that the town halls "do not have the information organised so as to promptly make it public". Furthermore, the information that should be published online is not to be found on the Internet sites and "it is still extremely difficult and costly to get the public data on the local services". Some town halls simply ignore requests and even court cases and court decisions: "neither the law, nor the respect for the citizen seem to matter for certain town halls, as is the case of the one for district five of Bucureşti".

A general tendency is the decrease of court cases introduced in response to the refusal of providing access to information but, at the same time, the number of cases for the non-observance of answering terms and incomplete answers has increased.

OTHER RECENT FACTUAL DEVELOPMENTS

A series of media scandals made the front pages of newspapers in 2009 and 2010 that had as "informatic support" recordings or transcripts of private conversations (face-to-face or phone conversations).

¹¹⁸ Decision No. 261/2007.

¹¹⁹ APADOR-CH, Press Release Regarding Declassification of Government Meeting Minutes, 18 November 2008, *supra*.

¹²⁰ *Id.*

¹²¹ See IPP reports – "A performing public administration means quality services for the citizens", IPP, July 2009; "Public interest information, a right not a favour" IPP, October 2009; "Transparency of the public acquisition process in the local administration in Romania: challenges, obstacles, learnt lessons", IPP, April 2009, all available at <http://www.ipp.ro>.

¹²² See Activewatch, *Libertatea Presei în România 2009*, *supra*.

On 10 November 2009, the daily *Curentul* published the transcript (and posted the recording on its website) of a conversation between two reputed journalists, Sorin Rosca-Stanescu and Bogdan Chireac, on the one hand, and the head of the National Agency for Integrity, Catalin Macovei, on the other. In the conversation, the two journalists exerted pressure on Mr. Macovei to give them access to information regarding highly-placed politicians (such as, for example, bank account numbers).¹²³

On 10 December 2009, Senator Catalin Voicu (Social-Democrat) was invited for questioning by the Anti-Corruption National Department (*Directia Nationala Anti-Coruptie* or DNA). He was later arrested and investigated for corruption and trafficking in influence. The main accusations were based on phone calls between him and various other individuals. The transcripts of the incriminating conversations were leaked to the media and widely published/broadcast.¹²⁴

On 3 March 2010, Antonie Solomon, the mayor of Craiova (south-eastern Romanian, a city of 200,000 inhabitants) was arrested for alleged bribery based on several discussions between him and the owner of a football club that were intercepted while the latter was under surveillance for corruption.¹²⁵

On 21 June of the same year, the TV owner and journalist Dan Diaconescu was invited to DNA for questioning. He was later detained and arrested for 29 days under accusations of blackmail and threats against a local mayor. The accusations against him were also based on taped conversations between one of his employees and the mayor.¹²⁶ Diaconescu appealed and is currently being investigated at liberty. His employee is still in preventive arrest.

¹²³ Dana Iliescu, "Roșca Stănescu și Bogdan Chiriac - șantaj la șeful ANI" ("Sorin Rosca Stanescu and Bogdan Chireac – Blackmailing the NAI Head"), in *Curentul*, 10 November 2009, available at <http://www.curentul.ro/2009/index.php/2009111036663/Actualitate/Rosca-Stanescu-si-Bogdan-Chiriac-santaj-la-seful-ANI.html>.

¹²⁴ Attila Biro, "Reteaua, metodele si clientii lui Catalin Voicu. Ce discuta oamenii de afaceri cu politicienii si judecatorii cand vor sa ingroape dosare" ("The Network, the Methods and the Clients of Catalin Voicu. What the Businessmen talk with Politicians and Judges when They Want to Bury a File"), *Hotnews*, 18 March 2010 available at <http://www.hotnews.ro/stiri-esential-7046536-reteaua-metodele-clientii-lui-catalin-voicu-discuta-oamenii-afaceri>.

¹²⁵ Valentine Tudor, "Solomon, încătușat" ("Solomon Hand-cuffed"), *Gazeta de Sud*, 3 March 2010, available at <http://www.gds.ro/Actualitate/2010-03-03/Solomon,+incatusat&hl=solomon%20incatusat&tip=toate>.

¹²⁶ R.M., "Cum motiveaza judecatorii decizia arestarii lui Dan Diaconescu: Lasarea realizatorului TV in libertate reprezinta un pericol public. Primarul a fost haituit sistematic de inculpate" ("How the judges motivate their decision to arrest Dan Diaconescu: He is a public menace. The accused repeatedly harassed the mayor"), *Hotnews*, 24 June 2010, available at <http://www.hotnews.ro/stiri-esential-7474196-update-cum-motiveaza-judecatorii-decizia-arestarii-lui-dan-diaconescu-lasarea-realizatorului-libertate-reprezinta-pericol-public-primarul-fost-haituit-sistematic-inculpati.htm>.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

There have been limited campaigns by the private sector or civil society in the field of data protection. Most of the human rights associations have dealt with cases infringing privacy, but none has insisted on a special campaign in this domain.¹²⁷

The beginning of 2009 was more active. The new data retention law in place and the launch of the biometric passport, inflamed a part of public opinion that was very actively and aggressively against the new provisions, especially biometric passports. Mainly, the opposition is due to their religious beliefs; they incorporated themselves into civil organisations that were dealing also with these aspects of privacy.¹²⁸

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Romania has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol, which establishes an individual complaint mechanism.¹²⁹

Romania is a member of the Council of Europe and signed and ratified the Convention for the Protection of Human Rights and Fundamental Freedoms.¹³⁰ In 2001, Law No. 682/2001 was enacted to ratify the Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹³¹ The Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, was adopted in Strasbourg on 18 November 2001 and Romania ratified it by Law No. 55/2005.¹³² Romania also signed the Council of Europe Cybercrime Convention on 23 November 2001, and ratified it by adopting Law No. 64/2004.¹³³

Romania has been a member of the European Union since 2007.

¹²⁷ Bogdan Manolea, Romania National Report, *supra*.

¹²⁸ "Romania: Protests Against Biometric Passports," *supra*.

¹²⁹ Romania signed the ICCPR on 27 June 1978 and ratified it on 9 December 1974; Romania acceded to the First Optional Protocol to ICCPR on 20 July 1993. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹³⁰ See <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=23/09/2010&CL=ENG>.

¹³¹ Official Monitor No. 830, 21 December 2001. full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=77624>.

¹³² Official Monitor No. 244, 23 March 2005, full text in Romanian and English summary available at <http://www.glin.gov/view.action?glinID=147990>; see also e-mail from Virgil Cristian Cristea, *supra*.

¹³³ Official Monitor No. 343, 20 April 2004, available in Romanian at <http://www.legi-internet.ro/ratifycybercrime.htm>, English summary available at <http://www.glin.gov/view.action?glinID=137491>.

*Updates to the Romanian Report published in the 2010 edition of EPHR have been provided by: Ioana Avadani, Centrul pentru Jurnalism Independent, Romania; Bogdan Manolea, Association for Technology and Internet - APTI, Romania.

SLOVAK REPUBLIC

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Slovakia's 1992 Constitution provides for privacy, data protection, and secrecy of communications. Article 16 states, "(1) The inviolability of the person and its privacy is guaranteed. It can be limited only in cases defined by law." Article 19 states, "(1) Everyone has the right to the preservation of his human dignity, personal honour and good reputation, and the protection of his name. (2) Everyone has the right to protection against unwarranted interference in his private and family life. (3) Everyone has the right to protection against the unwarranted collection, publication, or other illicit use of his personal data." Article 22 states, "(1) The privacy of correspondence and secrecy of mailed messages and other written documents and the protection of personal data are guaranteed. (2) One must not violate the privacy of correspondence and the secrecy of other written documents and records, whether they are kept in private or sent by mail or in another way, with the exception of cases to be set out in a law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means."¹

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Personal Data Protection Act No. 428/2002 Coll. (PDPA) repealed the Act No. 52/1998 Coll. on Protection of Personal Data in Filing systems.² The PDPA brings Slovak data protection into line with the European Parliament and Council Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.³

Amendments to the PDPA over the years have brought Slovakia's data protection scheme into compliance with the EU Directive. The PDPA limits the collection, disclosure, and use of personal information by government agencies and private enterprises either in electronic or manual form. In addition to establishing the Office for Personal Data Protection of the Slovak Republic (OPDP), the amendments provided data subjects with the right to obtain a copy of their data from the controller.⁴ The last material amendment of the PDPA was carried out in 2005 by Act No. 90/2005 Coll.

¹ Act No. 460 of 1 September 1992, Constitution of the Slovak Republic (1 September 1992), available at in English <http://www.slovakia.org/sk-constitution.htm>.

² Act No. 428/2002 Coll. on Protection of Personal Data (PDPA), as amended by Act No. 602/2003 Coll., Act No. 576/2004 Coll., Act No. 90/2005 Coll. and Act No. 583/2008 Coll., available in English at http://www.dataprotection.gov.sk/buxus/docs/act_428_2002_01_09.pdf.

³ OJ L 281, 23 November 1995, at 31–50, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

⁴ *Id.*

The PDPA imposes duties of access, accuracy and correction, security, and confidentiality on the data processor. Processing information on race, ethnicity, political opinions, religion, philosophical beliefs, trade union membership, health, and sexuality is forbidden. Special protections are provided for sensitive data, defined as: (i) data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life and conviction"; (ii) identifier of general application, i.e., personal birth number; (iii) biometric data; (iv) data on physical identity; and (v) data on violations of criminal law, civil law, misdemeanours, and their enforcement.⁵

Information systems must be registered with the OPDP unless certain exemptions apply, such as oversight carried out over the information system by responsible personal data protection officials appointed by the controller.⁶ Moreover, the law imposes new duties on controllers, who are meant to ensure better protection of personal data and to put in place safeguards to mitigate the risk of processing infringing personal data.

Currently, the OPDP is preparing a further amendment to the PDPA which would reflect, in particular, the adoption of the Council Framework Decision 2008/977/JHA of 27 November 2008 on personal data protection processed within the framework of the police and judicial cooperation in criminal matters. The draft amendment will be submitted to the Slovak government in October 2010.⁷

Sector-based regulations

In addition to the provisions established by the PDPA, other Slovak laws specify norms for data processing in particular sectors like healthcare as well as in the employment and banking sectors. These laws represent an extension of the fundamental rules laid down in the PDPA.

In the areas of processing, providing, and making available a patient's medical documentation, a complex sector-based regulation is laid down in the 2004 Act No. 576/2004 Coll. on Healthcare as amended.

Workplace privacy was introduced in September 2007 by way of an amendment to the Labour Code. Unfortunately, the regulation was formulated only as a set of principles and rather succinctly, allowing a variety of interpretations. Court decisions in workplace privacy matters are yet to come.

Privacy in telecommunications and Internet communications follows from the general principles laid down in the PDPA, and is further specified in the Act No. 610/2003 Coll.

⁵ *Id.*

⁶ *Id.*

⁷ 13th Annual Report of the Article 29 Working Party on Data Protection, July 2010. With the exception of the cited document (not yet available on-line), all the Annual reports of Art. 29 WP are available at http://ec.europa.eu/justice/policies/privacy/workinggroup/annual_reports_en.htm.

on Electronic Communications,⁸ in particular with regard to data which constitute telecommunications secrets, *inter alia*, localisation and operational data. The Act on Electronic Communications also defines the limits for direct marketing.

DATA PROTECTION AUTHORITY

The 2002 Act created the OPDP, headed by the President, to supervise and enforce the Act. The OPDP and its President replaced the Commissioner and his Inspection Unit of Personal Data Protection. The President, currently Mr. Gyula Veszeli, is elected by the National Council for a five-year term and may be re-elected for at most two consecutive terms. The OPDP's budgetary independence was formally strengthened by a minor amendment to the PDPA, effective as of January 2009, which transferred responsibility for the OPDP's budgetary programme from the Government Office of the Slovak Republic to the General Treasury Administration.⁹

The OPDP monitors the implementation of the law, reviews registered systems, inspects the processing of personal data in information systems, receives and handles complaints concerning the violation of personal data protection in information systems, initiates corrective actions whenever a breach of legal obligations is discovered, and participates in the preparation of generally binding regulations in the field of personal data. In 2007 and 2008, legislation provided the OPDP with more than 67 principal annotations to legislative acts concerning issues of personal data protection.¹⁰ The OPDP is required to file a biannual report on the status of data protection with the National Council.¹¹

The activities of the OPDP's Inspection Unit are mainly focused on examining the filing systems of controllers and processors, as well as handling notifications of data subjects and other individuals claiming to have had their rights directly affected. In specific situations, the PDPA permits the OPDP to publish or issue binding statements (measures) as well as to impose sanctions, including fines for violating provisions of the Act.

By August 2010, the OPDP had registered 40,900 appointment notifications of personal data protection officials responsible for internal enforcement. The OPDP also maintains a register of 230 regular filing systems and 60 filing systems which are subject to a special registration requirement (e.g., because they contain biometric data).¹²

In 2009 the Office issued eight approvals for the cross-border flow of personal data to countries which do not provide an adequate level of data protection (three approvals were

⁸ Act No. 610/2003 Coll. on Electronic Communications, available at http://www.telecom.gov.sk/index/open_file.php?file=telekom/legsr/Act_on_electronic_communications__consolidated_text__final.pdf&lang=en.

⁹ 12th Annual Report of Article 29 Working Party on Data Protection, June 2009.

¹⁰ OPDP's Report on Status of Personal Data Protection 2007 – 2008, June 2009.

¹¹ Act No. 428/2002 Coll. on Protection of Personal Data (PDPA), *supra*.

¹² Email from Mr. Kudoláni of OPDP, 13 August 2010.

issued in 2008); the subject of these flows was mainly personal data concerning employees and clients of international corporations.¹³

In 2009 the OPDP initiated 272 proceedings compared to 252 in 2008. The OPDP's Inspection Unit, acting in conjunction with the complaint investigation subdivision, conducted 107 inspections and issued 72 "submissions to explanations" to be carried out by the controllers and processors of filing systems. Altogether, 161 "orders" were issued for the removal of deficiencies that were discovered by these inspections. This represents an increase of 120 percent compared to 2008.¹⁴

The OPDP received several complaints about fraud, faked contracts, and identity theft resulting in credit/debit card fraud. Many banks and private sector entities are instituting biometric authentication/verification in order to combat some of these abuses. However, consent to use biometric data is only required under the PDPA if said data falls under the PDPA's definition of personal data. There are no biometric-specific rules on collecting, using, or disclosing this data.¹⁵

The OPDP also organises numerous seminars and consultation sessions concerning the recent amendments to the PDPA, and has also presented several lectures and launched a new website. The OPDP is also active in organising public discussions such as the press discussion that took place on 28 January 2010, "Can we protect personal data for the sake of our privacy and safety of our children?"¹⁶

The OPDP also conducted a survey of data protection awareness. According to the last survey, carried out in February 2009 and conducted through the Opinion Research Institute of the Statistical Office of the Slovak Republic, the awareness of all categories of citizens' personal data protection rights increased by 5 percent between February 2007 and February 2009, and – all together – rose by 36 percent between November 1999 and February 2009. The poll showed that the biggest concern of most of the respondents was the misuse of their national ID number, followed by health-related data, and data on personal assets.¹⁷

The OPDP cooperates closely with the data protection authorities in other Central and Eastern European countries. In December 2001, the Data Protection Commissioners from the Czech Republic, Hungary, Lithuania, Slovakia, Estonia, Latvia, and Poland signed a joint declaration agreeing to provide closer cooperation and assistance. The Commissioners agreed to meet twice a year in the future so as to provide each other with

¹³ 13th Annual Report of Article 29 Working Party on Data Protection, *supra*.

¹⁴ *Id.*

¹⁵ 9th Annual Report of Article 29 Working Party on Data Protection, June 2006.

¹⁶ Press release, 28 January 2010, available in Slovak at http://www.dataprotection.gov.sk/buxus/docs/Tlacova_sprava_28012010.pdf.

¹⁷ OPDP's Report on Status of Personal Data Protection 2007 – 2008, *supra*.

regular updates and overviews of developments in their countries, and to establish a common website for more effective communication.¹⁸

The OPDP is active in developing and maintaining contacts within the partnerships with Central and Eastern European personal data protection authorities, e.g., by means of the annual Central and Eastern European Commissioners Conference.

The OPDP also maintains active bilateral cooperation, in particular with its sector partners in the Czech Republic, Poland, and Romania. A thorough exchange of the best practices on mass media policies, awareness raising, and opportunities for cooperation with the Office of Personal Data Protection of the Czech Republic took place in Bratislava in October 2009.¹⁹

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In situations that are not regulated by detailed provisions of the Acts,²⁰ the public administration has the discretion to interpret and apply general legal terms such as "privacy" or "honour" in conformity with the Constitution, and thus may consider that the right to privacy is in certain cases constrained by the right to information. The obligation of the public administration to consider Constitutional principles²¹ was recognised by the Slovak Constitutional Court in the ruling II. ÚS 44/00, which held that making a film record of policemen performing their official duties is not an invasion of their right to privacy and should be allowed.²²

Another serious problem arises when information about official duties (performed within public administrative bodies or institutions' public functions) is considered personal data. This information is often withheld. For instance, the Ministry of Foreign Affairs refused to provide information about the names and functions of its employees in order, it said, to protect their personal data. Two legal actions have been brought against the Ministry in the regional court in Bratislava in this connection, but neither has been decided yet.²³ At the end of 2004, the Cabinet approved rewards for high state officials. However, when journalists asked the Cabinet to disclose the amounts of these rewards, or specific sums

¹⁸ Website of Central and Eastern Europe Data Protection Authorities <http://www.ceeprivacy.org>.

¹⁹ 13th Annual Report of the Article 29 Working Party on Data Protection, *supra*.

²⁰ In instances where general legal terms such as "privacy" or "honor" are applied – for example, under Section 11 of the Slovak Civil Code "A natural person has a right to the protection of his personality, honor, dignity, privacy, name, and personal expressions."

²¹ For example, the principle stated in Article 152 paragraph 4 of the Constitution, according to which all laws shall be interpreted and applied in conformity with the Constitution.

²² Slovak Constitutional Court, judgment II. ÚS 44/00, in Slovak at http://www.concourt.sk/Zbierka/2001/10_01s.pdf.

²³ These are pending cases and have not yet been decided; ref Nos. 1S 64/05 and 2S 94/05.

and persons' names, the Cabinet responded that this information could not be disclosed on data protection grounds.²⁴

In 2005, the OPDP issued an order requiring the state administrative authority to terminate the disclosure of national identification numbers ("birth numbers") on the website of the Official Journal. The authority was also instructed to remove previously published birth numbers from its website. However, the authority filed a petition with a court, requesting the reversal of the OPDP's decision. The court dismissed the claim, arguing that the decision was based on appropriate grounds, and was in line with the competence granted to the OPDP by law. The law explicitly prohibits the disclosure of an "identifier of a general application", such as birth numbers.²⁵ In a similar case in 2006 involving the publication of birth numbers, the OPDP ordered that all birth numbers be removed from the website of the Commercial Bulletin or made unreadable. The Ministry of Justice of the Slovak Republic challenged this decision in court. The court dismissed the Ministry's claim and confirmed the OPDP's order at the end of January 2008.²⁶

In another case, a natural person sued the OPDP for not issuing legal sanctions against a newspaper publishing company that enabled the publication of the plaintiff's personal data on its website without the person's knowledge (the website allowed anyone to publish their opinions). The petitioner claimed that an unknown person had posted his personal data, including his name, surname, and address, on the website, and therefore claimed that his rights as stipulated in the Act had been violated. However, the petitioner himself had previously repeatedly published his personal data on other websites. In November 2004, the regional court ruled that the OPDP's procedure was in line with the Act. The petitioner appealed against the judgment and in May 2007, the Supreme Court fully confirmed the regional court's verdict.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

According to the Code of Criminal Procedure, the police are required to obtain permission from a court before undertaking any telephone tapping or mail surveillance in criminal investigations.²⁷ These activities should only be used in cases of extraordinarily serious premeditated crimes or crimes involving international treaty obligations. If it is not possible to obtain a warrant in advance and the matter is urgent, the warrant may be

²⁴ PRAVDA, 10 December 2004, available in Slovak at http://spravy.pravda.sk/sk_domace.asp?r=sk_domace&c=A041209_183102_sk_domace_p02.

²⁵ 12th Annual Report of the Article 29 Working Party on Data Protection, *supra*.

²⁶ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra*.

²⁷ Code of Criminal Procedure, Articles 115 and 116.

issued by a prosecutor. However, it must be approved by a court within 24 hours of its issuance.

Further protection outside of criminal investigations is provided by Act No. 166/2003 Coll. on Protection against Unlawful Use of Information and Technical Means (Wiretapping Protection Act). This Act defines the technical means that can be employed by specific public authorities (Police Department, Slovak Intelligence Service, Military Intelligence, Railway Police Department, Department of Corrections and Judicial Police, and the Customs Administration) in order to collect information and determines how the collected information should be used. Apart from the Slovak Intelligence Service, which is itself allowed to use both the information and the technical means to obtain it, the Police Department provides these services for the other public authorities. The municipal authorities, private security services, or other natural or legal persons may not use the information and/or the technical means to obtain it themselves. These means may only be used by Police Department, Slovak Intelligence Service, Military Intelligence, Railway Police Department, Department of Corrections and Judicial Police, and the Customs Administration if it is necessary in order to protect national security or national defence, prevent or detect crime, or to protect the rights and freedoms of others. A warrant to use the information and technical means is required and is valid for six months (it may be extended repeatedly by another six months). Only the Police Department is permitted to use the information and technical means in urgent cases without a warrant; however, a court must be notified within one hour and a request for a warrant within six hours from the commencement of using the means. If the warrant is not issued within 12 hours, or if the court dismisses the request, the use of the means must cease and any data that has been obtained cannot be used and must be destroyed.²⁸

In 2006, the Constitutional Court heard the case of an individual who claimed it was illegal to tap his telephone calls on the basis of two court-issued warrants that had been obtained for this purpose (one was issued on the basis of the Criminal Procedural Code; the second on the basis of the Wiretapping Protection Act).²⁹ He claimed that the warrants were issued without sufficient evidence to justify interference with his right to privacy (at the time when the warrants were issued the individual's file contained only a resolution to initiate an investigation). This view was confirmed by the Constitutional Court. Moreover, although the law stipulates the obligation to substantiate wiretapping warrants, the Constitutional Court found that the warrants in question merely contained a formalistic substantiation quoting the wording of the relevant acts. According to the Court's ruling, "no doubt can exist that a warrant must be justified in any case" and "for review of the warrant's legitimacy it is necessary that the warrant is substantiated by

²⁸ Act No. 166/2003 Coll. (Wiretapping Protection Act), Art. 4, in Slovak at <http://www.mosr.sk/data/files/628.pdf?PHPSESSID=63594e4a>.

²⁹ Constitutional Court of the Slovak Republic, June 2006, I. ÚS 274/05, in Slovak at http://www.concourt.sk/Zbierka/2006/06_31s.pdf.

relevant and specific argumentation as to by what facts the statutory requirements for such interference of the right to privacy were fulfilled."³⁰

In 2001, allegations were made that members of the Hungarian Coalition Party (*Strana maďarskej koalície* or SMK) and Social democracy (*Sociálnademokracia* or SMER) were being monitored and their telephones tapped.³¹ Active monitoring of the Church of Scientology by the Ministry of the Interior was also reported.³² Under the Criminal Procedural Code, police require a judicial search warrant in order to enter a private home and the court may only issue one with good cause. Police are required to present the warrant before conducting the search or within 24 hours. There are ongoing reports of Roma homes being entered without warrants.³³

Legal protection of privacy is stipulated also in the Civil Code. Article 11 states, "everyone has the right to the preservation of his personality, mainly of life and health, personal honour, and human dignity as well as privacy, name, and exhibitions of personal nature." There are also computer-related offences linked to the protection of a person (unjustified treatment of personal data).³⁴ The Slovak Constitutional Court ruled in March 1998 that the law allowing public prosecutors to demand to see the files or private correspondence of political parties, private citizens, trade union organisations, and churches, even when not necessary for prosecution, was unconstitutional. Chairman of the Court Milan Cic, said this was "not only not usual, but opens the door to widespread violation of peoples' basic rights and their right to privacy."³⁵ Moreover, there are sector-specific privacy provisions to protect an individual's medical, financial, and tax records.³⁶

National security legislation

No specific information has been provided under this section.

Data retention

The legal basis for retention of telecommunications traffic data as required by Directive 2006/24/EC (Data Retention Directive) was laid down in the form of the 2007

³⁰ *Id.*

³¹ US State Department Human Rights Report 2001 – Slovakia, available at <http://www.state.gov/g/drl/rls/hrrpt/2001/eur/8338.htm>.

³² *Id.*

³³ US State Department Human Rights Report 2006 – Slovakia, available at <http://www.state.gov/g/drl/rls/hrrpt/2006/78838.htm>.

³⁴ European Commission, Agenda 2000 "Commission Opinion on Slovakia's Application for Membership of the European Union, Doc 97/20", 15 July 1997.

³⁵ "Court Rules Law on Public Prosecutors Unconstitutional," CTK National News Wire, 4 March 1998.

³⁶ Act No. 576/2004 Coll. on Health Care; Act No. 21/1992 on Banks (later cancelled and replaced by Act No. 483/2001 on Banks); Act No. 511/1992 on Tax Fee Administration; see Christopher Millard and Mark Ford, "Data Protection Laws of the World," (Clifford Chance, Sweet & Maxwell 2000).

amendment to the Act on Electronic Communications. The retention period concerning operational data, localisation data, and traffic data on communicating parties has been set at six months with regard to Internet communications data, and at 12 months for other types of communication.

The purpose of data retention is specified in the Act No. 610/2003 Coll. on Electronic Communications and is aimed at investigating, detecting, and prosecuting crimes related to terrorism, illicit trafficking, organised crime, and threats to the disclosure of classified information and crimes committed by dangerous groups.

National databases for law enforcement and security purposes

On 21 December 2007, the Slovak Republic joined the Schengen area, which allows the free movement of persons within the internal boundaries of the countries participating in the 1985 Schengen Agreement and the Schengen Convention implementing the Schengen Agreement.³⁷ Both international treaties form part of the European Union *acquis communautaire*.

The Schengen Convention established the Schengen Information System (SIS) to maintain public policy and public security, including national security, in the territories of the Schengen Convention parties and use information communicated via this system to apply the provisions of the Schengen Convention relating to the movement of persons in those territories. Data on persons included in alerts sent through the system shall only include the following specific information: (a) surname and forenames, plus any aliases (possibly entered separately); (b) any specific, objective physical characteristics that are not subject to change; (c) the first letter of the second forename; (d) date and place of birth; (e) sex; (f) nationality; (g) whether the persons concerned are armed; (h) whether the persons concerned are violent; (i) reason for the alert; (j) action to be taken.³⁸

Sensitive information, i.e., information concerning racial origin, political, religious, or other beliefs, health, and sexual activities may not be entered.

Integrating the competent Slovak state authorities into the SIS required a number of legislative amendments and adjustments. Amendments to the Act on the Police Department and of a Decree of the Ministry of the Interior adopted in 2007 designated the Ministry of the Interior as the controller of the national part of the SIS (N-SIS) which is connected to the central system (C-SIS). The second-generation Schengen Information System (SIS II) will replace the current system, providing enhanced functionalities. It is

³⁷ Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

³⁸ *Id.*

currently undergoing extensive testing in close cooperation with European Union (EU) countries and associated countries participating in the Schengen area.³⁹

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

As a result of the cooperation among non-governmental public and private actors, project *www.zodpovedne.sk* ("responsibly") was launched in August 2007 with the aim of raising awareness of how to use the Internet and mobile communications responsibly and prevent related crimes. The project was co-funded by the European Commission within the "Safer Internet Plus" programme. It dealt with risks related to the use of the Internet and mobile communications for paedophilia, pornography, victimisation, racism, xenophobia, violence, grooming, disclosure of personal data, and fraud.⁴⁰

Critical infrastructure

Currently, Slovakia has no law governing the protection of critical infrastructure. In 2007, the Government adopted a document entitled: "The Concept of Critical Infrastructure in the Slovak Republic and of its Protection and Defence".⁴¹ Based on the same concept, the "National Programme of Protection and Defence of Critical Infrastructure" was adopted in 2008.⁴² However, both documents only provide a general outline of the critical infrastructure protection strategy in Slovakia and do not encompass a detailed description of proposed measures. Moreover, the documents do not in any way address the issue of safeguarding individuals' privacy in connection with protection measures.

INTERNET & CONSUMER PRIVACY

E-commerce

Unsolicited commercial emails (so-called "spam" emails) fall within the scope of Act No. 147/2001 Coll. on Advertising and, in particular the Act No. 610/2003 Coll. on Electronic Communications, adopted in 2003.⁴³ In February 2006, the latter was supplemented with

³⁹ For more information see http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/114544_en.htm.

⁴⁰ Miroslav Drobný, "O projekte" ("About the Project"), in Slovak at http://www.zodpovedne.sk/kapitola4.php?cl=zodpovedne_sk.

⁴¹ Available in Slovak at the Ministry of Interior's website, at <http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691>.

⁴² Available in Slovak at the Ministry of Interior website, at <http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10692>.

⁴³ Act No. 610/2003 Coll. on Electronic Communications, *supra*.

new provisions regulating cookies and unsolicited communications in order to fully implement EU Directive 2002/58/EC.⁴⁴

The regulation is based on the "opt-in" principle, with an exception, granted in compliance with Article 13 of the Directive on privacy and electronic communications,⁴⁵ for direct marketing by a legal or natural person based upon the use of electronic contact details of its customers obtained within the context of a previous sale of its own similar products or services. The customers must be given the opportunity to object, free of charge and in a simple manner, to such use of electronic contact details at any time. The Act on Electronic Communications prohibits sending commercial emails that conceal the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease.⁴⁶

According to the Act on Electronic Communications, a violation of the provisions concerning direct marketing in respect of unsolicited commercial emails may be sanctioned by the Telecommunications Regulatory Authority of the Slovak Republic with a fine of up to €33,000.

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

As part of the above mentioned project, *www.zodpovedne.sk*, two websites were created: *www.stopline.sk*, which is aimed at reporting illegal content and activities on the Internet with particular emphasis on the protection of children and youth; and *www.pomoc.sk* ("help"), which is an integrated helpline (it offers consultations via telephone, chat, and email) providing counselling via Internet, mobile communications, and new technologies. Moreover, a weekly TV show, *Cookie.sk*, was featured on public television as a part of the project. While the TV show was aimed primarily at youth, children were addressed by a series of cartoons and a related website, *ovce.sk* ("sheep"). Besides that, textbooks and workbooks for primary and secondary schools were distributed and the project was

⁴⁴ Act No. 117/2006 Coll., effective April 2006, available in Slovak at <http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=19238&FileName=06-z117&Rocnik=2006>.

⁴⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002, at 37-47, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>.

⁴⁶ Act No. 610/2003 Coll. on Electronic Communications, *supra*.

promoted via posters, leaflets, brochures, radio broadcasts, workshops in regional cities, round-tables for local authorities, seminars for parents and children, and summer computer courses.

TERRITORIAL PRIVACY

Video surveillance

According to the PDPA, public premises may be monitored by video or audio recording only for purposes of securing public order and safety and for the detection of crime or breaches of national security. The premises being monitored must be visibly marked as such, and the recording may only be used for the purposes of criminal or administrative proceedings. If the recordings are not used for the above-mentioned purposes within seven days, they must be destroyed.⁴⁷

The OPDP performed several inspections of the monitoring systems at public premises in the past. In 2007 and 2008, several inspections aimed at monitoring systems operated by municipalities were performed (involving the capital city of Bratislava and other towns such as Prešov, Prievidza, and Komárno, as well as several other minor municipalities). All inspections identified shortcomings in the operations of the monitoring systems or in maintaining the related documentation (the system's security guidelines). The most common shortcomings were failure to visibly mark the monitored premises and failure to destroy the recordings within the prescribed period.⁴⁸

Location privacy (GPS, mobile phones, location-based services, etc.)

In line with the Directive on privacy and electronic communications, the Act No. 610/2003 Coll. on Electronic Communications defines location data as any data processed in the network that indicates the geographical location of publicly available service users' terminal equipment.⁴⁹ Location data other than traffic data may only be processed if it has been anonymised or if the user's consent has been given and then only to the extent and time necessary to provide value-added services. The enterprise providing services shall inform the user of the purposes of the processing, the time-frame, and whether the data will be transferred to a third party to provide value-added services prior to obtaining the user's consent for location data other than traffic data. Users are entitled to revoke their consent at any time, and also to temporarily deny the processing of location data, free of charge.

There is an exception related to emergency calls, in which case the enterprise is obliged to provide coordination and an operations centre for the integrated rescue system even if

⁴⁷ Act No. 428/2002 Coll. on Protection of Personal Data (PDPA), *supra*, sections 10 (7) and 13 (7).

⁴⁸ Správa o stave osobných údajov 2007 – 2008 (Report on state of personal data), National Council of the Slovak Republic, June 2009.

⁴⁹ Act No. 610/2003 Coll. on Electronic Communications, *supra*.

the calling station (terminal equipment) has failed to supply identification or the user has not given consent to the processing of location data.

Travel privacy and border surveillance

As of 1 January 2008 the use of passport holders biometric data – digital facial scan and fingerprint – has been 'made compulsory for travel identification documents such as passports. These data are stored on an RFID chip contained in the travel document. The data contained in the biometric carrier may not be processed in any manner other than that stipulated by law; therefore, it may only be used for verification of the authenticity of the passport and the identity of its holder. For the purposes of issuing a passport, citizens are obliged to provide their biometric data and, on the other hand, the administrative body issuing the passport has the right to demand the data.⁵⁰

The Ministry of the Interior maintains a database of passports that falls within the scope of the PDPA, meaning that no special regulation applies to protection of data contained therein other than provisions of PDPA. The database is subject to supervision of the OPDP.

NATIONAL ID & SMART CARDS

Each and every citizen who has attained 15 years of age and has a permanent residence in Slovakia is obliged to have a national identity card (*občiansky preukaz*). The identity card contains the following personal data: name, surname and birth surname, sex, country of citizenship, date and place of birth, birth number, permanent address, a photographic image of the holder's face, and the user's signature. Furthermore, the identity card displays information as to whether the person's legal capacity has been limited or diminished. Due to its nature, the identity card is protected against misuse and fines up to the amount of €335 may be imposed for offences such as the unlawful seizure of another person's identity card, intentionally damaging or destroying it, or intentionally carrying out unlawful changes to the card.⁵¹

With the same status as a public deed, counterfeiting the national identity card is also considered a crime under the Criminal Code and can be sanctioned by imprisonment for up to three years.⁵²

The Ministry of the Interior maintains a database of identity cards that falls within the scope of the PDPA.

A project for central e-ID infrastructure is currently being implemented in Slovakia. The Ministry of Interior plans to introduce high-tech ID cards. Electronic ID cards will incorporate advanced electronic signatures, which are required by the Act on Electronic Signatures for communication with government bodies. To date, unique identifiers for

⁵⁰ Act No. 647/2007 on Travel Documents, Artt. 5 – 6.

⁵¹ National Identity Card Act No. 224/2006 Coll., Art. 3, 4 and 14.

⁵² Criminal Code, Art. 352.

citizens have been employed, and these are still being used within all sectors of applications. For the future, a new system has been planned, which will create new personal identifiers (called BIFO) using cryptographic algorithms.⁵³

RFID tags

No specific information has been provided under this section.

BODILY PRIVACY

The Criminal Procedural Code stipulates the obligation of an individual to undergo a bodily examination if it is necessary for determining whether the body bears the traces or after-effects of a crime. The examination is to be performed by a person of the same sex unless performed by a medical doctor. Furthermore, individuals are obliged to undergo blood sampling or similar, unless it is hazardous to the individual's health, for the purpose of securing evidence within a criminal investigation. Provision of biological samples that does not interfere with the individuals' physical integrity (i.e., non-invasive sampling) may be performed either by the individuals themselves or by law enforcement officials, with the individuals' consent.⁵⁴

Provision of biological samples for the purpose of DNA analysis is governed by special legislation, i.e., Act No. 417/2002 Coll. on Use of DNA Analysis for the Purpose of Identification of Individuals.⁵⁵ Under this act, DNA samples may be taken from individuals without their consent for the purpose of identification in the context of criminal proceedings, search for missing persons, or identification of unknown individuals, or from prison inmates. Upon the prior written consent of the individuals concerned, a DNA sample may be taken from the relatives of a missing person being sought. The resulting data is stored in a database maintained by the police. An individual's record is to be deleted from the database in the following cases: (i) if the charges against the individual were dropped or if the individual was found not guilty by the court, or (ii) if the individual was convicted or could not be prosecuted or convicted, e.g., due to lack of the individual's criminal liability; in the latter case the record shall be deleted after the lapse of 100 years after the individual's day of birth.

With regard to the provision of healthcare, the Act No. 576/2004 Coll. on Healthcare stipulates a general obligation on the part of healthcare providers to obtain informed consent of the patient to treatment (save for certain specific cases where informed consent cannot be obtained). However, there have been several cases in which Romani women were allegedly involuntarily sterilised in public health facilities. Thanks in part to the initiative of non-governmental organisations, several civil court cases were filed. In

⁵³ ePractice, eGovernment Factsheet – Slovakia – National Infrastructure (January 2010), available at <http://www.epractice.eu/en/document/288355>

⁵⁴ Code of Criminal Procedure, Art. 155.

⁵⁵ Available in Slovak at http://www.minv.sk/swift_data/source/mvssr/dokumenty/pravne_normy/zakon_o_dna.doc.

one of these, three Romani women claimed that they were sterilised without giving informed consent.⁵⁶

In 2006 the Constitutional Court ruled that regional prosecutors had violated the Constitution and the European Convention on Human Rights by improperly closing the investigation of the original claim, and awarded each of the claimants 50,000 Koruna (approx. €1,660).⁵⁷ The Court instructed the prosecution to reopen its investigation in 2007, but the investigation did not yield any new results. The NGO representing the victims filed another appeal to the Constitutional Court, which was dismissed in 2010.⁵⁸ Two additional cases were pending at regional courts following subsequent appeals, and four cases were pending before appellate courts. Three forced sterilisation civil suits that pre-date the 2005 law were filed at the ECtHR in 2004; two are still pending.⁵⁹

In April 2009 the ECtHR ruled in favour of eight Romani women who suspected they had been sterilised without their knowledge. The hospitals where the procedures had been performed allegedly denied them access to their medical records and the ECtHR ruled that this denial of access was a violation of privacy; the allegation of uninformed sterilisation was not at issue. Four of the women subsequently received access to their medical files, and at least one discovered she had been sterilised. The remaining four women continued to be denied access to their medical records despite the court ruling. In 2007 the Ministry of Health informed the NGO representing the Romani women that the women's medical records had been lost. After numerous unsuccessful civil proceedings, the plaintiffs were each awarded € 3,500 in damages.⁶⁰

WORKPLACE PRIVACY

Protection of employee privacy is one of the main tenets of the Slovak Labour Code. According to Article 11 of the "General Principles" section of the Labour Code, employers can only collect personal data that relates to the qualifications and professional experience of employees and data that may be relevant to the work carried out by employees. In addition, employees' consent to the collection and processing of their personal data is required and they must be informed of the purpose of collecting and processing the data. Employers are allowed to use the data only for the purpose that was notified to employees.⁶¹

⁵⁶ "2009 Human Rights Report:Slovakia,"US Bureau of Democracy, Human Rights, and Labor, 11 March 2010, at <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136057.htm>.

⁵⁷ Constitutional Court of the Slovak Republic, December 2006 – decision III. ÚS 194/06-46, available in Slovak at http://www.concourt.sk/rozhod.do?urlpage=dokument&id_spisu=79025.

⁵⁸ Constitutional Court of the Slovak Republic, May 2010, I. ÚS 174/2010, www.concourt.sk.

⁵⁹ 2009 Human Rights Report Slovakia," *supra*.

⁶⁰ *Id.*

⁶¹ Helena Barancová, *Zákonník práce. Komentár* (Labour Code. Commentary) 42 -43 (C.H. Beck 2010).

The protection of employee privacy starts even before the establishment of the employment relationship, i.e., during and after the job interview. According to Article 41 of the Labour Code, employers are only allowed to request information from first-time job applicants and then only information that relates to the work to be performed. Job applicants who have been employed before may also be asked to provide the new employer with a work report as well as a confirmation of employment. Employers must not request information about the job applicant's pregnancy, family relationships, integrity (except for work where the candidate's integrity is required by law or by nature of the work), political or religious affiliation, or union membership.⁶²

Furthermore, employers shall not, without serious grounds based on the specific nature of the employer's activities, interfere with employees' privacy in the workplace by monitoring them without notification or by inspecting private mail addressed to them. If employers have adopted a control mechanism, they are obliged to inform employees about the extent and methods of the control.⁶³

HEALTH & GENETIC PRIVACY

Medical records

Processing, providing, and making available a patient's medical records is regulated primarily in the 2004 Act on Healthcare. The medical records shall be processed by the general practitioner and, to the extent necessary, also by a specialist. The Act comprehensively stipulates cases where the doctor shall provide an excerpt from the medical records, and also cases where the doctor may grant access to the medical records (e.g., relatives, insurance company's review doctor), as well the extent to which the access shall be granted.

This regulation also governs the duties of healthcare providers (e.g., doctors, pharmacists, nurses, etc.) to provide personal data to the national filing systems, such as the National Health Register, which contains personal data of patients suffering from selected health problems/diseases, e.g., diabetes, cancer, etc. The controller of the National Health Registries is the National Health Information Centre. Only the statistical data summarising the incidence of a disease can be publicly disclosed, but in no case may the data relating to individual patients be divulged. Each individual's data in the register are treated as medical records under the Act on Healthcare.

Genetic identification

No specific information has been provided under this section.

⁶² *Id.*, at 41.

⁶³ *Id.*, at 42-43.

FINANCIAL PRIVACY

Under the Act No. 483/2001 Coll. on Banks, the banks are obliged to request their clients to prove their identity when carrying out any transaction, except for certain transactions under €2,000, and clients are obliged to comply with such request. Identity may be proved by showing the national identity card (*občiansky preukaz*), or by providing a signature in cases where the client is known to the bank the signature is identical to the specimen signature in the bank's records. However clients are required to present a national identity card when giving a signature specimen.⁶⁴

All client information and documents that are not publicly available and that relate to the clients' businesses, account(s), and balances are protected by banking secrecy. The bank shall keep this information confidential and protect it against disclosure, misuse, damage, destruction, loss, or theft. Information subject to banking secrecy may only be disclosed to third persons with the client's prior written consent or written instruction, except where there is a statutory obligation requiring the bank to disclose the information to public authorities such as the National Bank of Slovakia, law enforcement agencies, tax and customs authorities, Slovak Intelligence Service, etc., upon their written request. Clients are entitled to request information as to what personal data relating to them are kept in the bank's database. Any unlawful or intentional disclosure of banking secrets is considered a crime under the Criminal Code and may be sanctioned with a term of imprisonment from six months to three years.⁶⁵

In 2007, the European Commission Directorate-General for Justice, Freedom, and Security Data Protection Unit asked the OPDP for cooperation in the investigation of the "SWIFT case". Among other things, it asked for the official opinion of the OPDP on the status of measures taken by the banks in respect of the legal obligation to inform their clients about the processing of the personal data collected for the purpose of bank payments carried out via SWIFT (Society for Worldwide Interbank Financial Telecommunication). The Chief Inspector of the OPDP appealed by letter to 24 banking institutions, asking them to carry out a complex revision of their duties relating to trans-border payments performed via SWIFT, focusing on evaluating whether the processing of personal data caused any violation of the rights and freedoms of their respective clients; the National Bank of Slovakia was also included. When collecting, processing and subsequently transferring the personal data across borders, each bank is obliged to give its clients sufficient information about the conditions of their personal data's processing. The OPDP asked the banking institutions to provide a comprehensive and complete position on their own particular measures and mechanisms that either had been or would be executed in order to comply with the statutory requirements. If a banking institution did not take the relevant measures, it was obliged to specify which mechanisms and particular measures would be executed. Using these findings, the Section of Inspection of the OPDP formulated the information that was sent by the President of the OPDP to the

⁶⁴ Act No. 483/2001 on Banks, *supra*, Art. 89.

⁶⁵ Criminal Code, Art. 264.

European Commission on 14 May 2007. By the end of August 2007, the questionnaire concerning fulfilment of the obligation to inform respective bank clients about international payment transfers performed by SWIFT had been sent to the EC.⁶⁶

The obligation of clients to provide their personal data upon a trader's request is stipulated in the Act No. 566/2001 Coll. on Securities. Securities traders are allowed to make photocopies of clients' personal identification cards for the purpose of obtaining their personal data. Without the clients' consent, traders may only disclose the obtained personal information to statutory prescribed entities (state authorities) and only for statutorily prescribed purposes.⁶⁷

E-GOVERNMENT & PRIVACY

The Act No. 275/2006 on Public Administration Information Systems (20 April 2006) provides a framework for the development of public authorities' information systems. On 30 September 2009 the amendment to the above-mentioned Act was agreed by the Slovak Government. The relevant amendment was approved in December in the National Council of the Slovak Republic and signed by the President of the Slovak Republic.⁶⁸

OPEN GOVERNMENT

The Act No. 211/2000 Coll. on Free Access to Information was approved by the Parliament in May 2000. It sets broad rules on disclosure of information held by all "obligees", which means state agencies (including parliament, government, courts, etc.) municipalities, legal entities established by law and by state agencies, as well as legal entities and natural persons that have been given the power by law to make decisions in the area of public administration.⁶⁹ There are limitations on information that (a) is classified; (b) constitutes a trade, bank, or tax secret; (c) is a tax secret; (d) is a bank secret; (e) is intellectual property; (f) would violate privacy; (g) was obtained "from a person not required by law to provide information, who upon notification of the Obligee instructed the Obligee in writing not to disclose information"; (h) is information published regularly by the Obligee under a special act; (i) "concerns the decision-making power of the courts and law enforcement bodies"; or (j) identifies localities of protected animals and plants, minerals and fossils. Information requests to obligees must be

⁶⁶ 13th Annual Report of the Article 29 Working Party on Data Protection, *supra*.

⁶⁷ Act No. 566/2001 Coll. on Securities, Art. 73(a), available in English at http://www.nbs.sk/_img/Documents/_Legislative/_BasicActs/A566-2001.pdf.

⁶⁸ ePractice, eGovernment Factsheet – Slovakia – Legal Framework (January 2010), available at <http://www.epractice.eu/en/document/288352>.

⁶⁹ Act No. 211/2000 Coll. on Free Access to Information, available in Slovak at http://www.civil.gov.sk/SNARCHIV/uk_the_act_on_free_access_to_information.htm.

disposed without undue delay, but not later than ten days. Appeals are made to higher agencies and can be reviewed by an administrative court.⁷⁰

During the implementation of this Act in practice, difficulties have been found in some cases regarding appeals against decisions made by obligees who do not have their own superiors, e.g., municipalities, the National Property Fund of SR, etc. In these cases, it is not clear which is the appropriate appellate body. For example, in the case of municipalities, the provisions of two different acts collide. On one hand, the Act on Free Access to Information states in Article 19 that, "If it is a decision of the municipal office, the decision on the appeal shall be made by the mayor." In practice, this is not possible because the municipal office is also an executive body of the mayor. On the other hand, Act No. 369/1990 Coll. on Municipalities states in Article 13 that, "in administrative proceedings the mayor is the administrative body." This means that the mayor is the only body allowed to make first-degree administrative decisions. The municipal office is not allowed to do this. Under Article 27 of the Act on Municipalities, the court is the appellate body to the mayor's decision on the rights and responsibilities of natural persons or legal entities in matters of self-governance, including the disclosure of information. During the more than three years of implementing the Act on Free Access to Information there has been no adjudication that would unify these two contradictory provisions of two different acts. Nonetheless, the courts have accepted a doctrine that the mayor's decision on the appellate level is subject to judicial review by the competent Regional Court according to the relevant provisions of Act No. 99/1963 Coll. on Civil Court Procedure regulating judicial review of administrative decisions. The fact remains that the courts have no time limit within which they must decide, and the first-instance proceedings led by the Regional Court may be followed by appellate proceedings before the Supreme Court. The consequence is that the process for obtaining information may be considerably extended, while the value of the information originally requested declines in value.

There are also separate requirements for disclosure of environmental information that cover private organisations. These became effective on 1 January 2001⁷¹ and revoked Act 171/1998 Coll. of the National Council on Free Access to Environmental Information. In February 2001, the government approved a draft law on Protection of Confidential

⁷⁰ E-mail from Vlado Pirosik, Public Interest Lawyer, Environmental Lobbying Facility, Slovak Republic, to John Baggaley, Law Clerk, EPIC, 11 July 2003 (on file with EPIC). The Act on Free Access to Information stipulates the duty for obligees to provide information "without undue delay, but not later than in ten days." If a requester does not get the information from either the Obligee or from the appellate body (in the previous administrative proceedings), the requester has the right (Article 19, paragraph 4) to access the administrative court and let the court review both the administrative decisions. If the requester decides to use this right, from the moment she files a civil action, the proceeding is governed not by the Act on Free Access to Information, but by Act 99/1963 Coll. on Civil Court Procedure. Under this act, there is no obligatory time-limit imposed upon the courts. Typically, in Slovakia, this procedure takes five to six months.

⁷¹ Act No. 211/2000 Coll. on Free Access to Information, *supra*.

Information to harmonise the handling of classified documents with NATO standards, despite the Data Protection Commissioner's objections that it violated human rights.⁷²

In July 2005, it was reported that the Interior Ministry sought to change the existing free access to information law, which gives citizens the right to get information from public and municipal authorities. If the changes are introduced, a public official who withholds information will no longer be committing an offence. At present, an official who fails to provide information requested by a citizen can be fined up to €1,650 and be suspended from his job for up to two years. In the Interior Ministry's proposal, however, the offence clause would be left out of the freedom of information law. Jana Pôbišová, of the Interior Ministry, said that this is because the state or municipal employees do not act as private entities, but rather in the name of legal entities, the state, or municipal authorities, and should therefore not be punished as individuals. Activists claim, however, that if the clause is eliminated, it will be virtually impossible to identify who is responsible for withholding information.⁷³

Following a number of public procurement cases in which allegations of corruption were raised during the past years, the newly established government of the Slovak Republic has submitted a draft act for departmental discussion amending and supplementing the Act 40/1964 Coll., the Civil Code and Act No. 211/2000 Coll., on Freedom of Information and amending of certain laws (Freedom of Information Act).⁷⁴

According to the explanatory memorandum, the aim of the amendment is to ensure a proactive approach by the public authorities to increase the pressure on public authorities by making information available relating to the management of public resources and their responsibility for the management of public resources, and also to ensure better public awareness, and ultimately increase transparency with respect to the management of public resources.

Based on the draft amendment to the Civil Code, if one party to a written contract is a person required to make information available under Article 2 of the Freedom of Information Act and that contains information that is acquired with public funds or the use of public funds or the management of state or municipal property, or property of a higher territorial unit, or the European Union, shall enter into effect the day after its publication on the website of the person liable under the special regulation. If the person

⁷² "Government Approves New Version of Law on Confidential Information," BBC Summary of World Broadcasts, 2 March 2001.

⁷³ "Ministry Proposes Changes to Law on Access to Information," *The Slovak Spectator*, 22 July 2005, available at <http://www.slovakspectator.sk/clanok.asp?cl=20370>.

⁷⁴ Draft act amending and supplementing the Act 40/1964 Coll. Civil Code and Act No. 211/2000 Coll. on Freedom of Information and amending of certain laws (Freedom of Information Act), available in Slovak at <https://lt.justice.gov.sk/Document/DocumentDetails.aspx?instEID=-1&matEID=3072&docEID=128927&docFormEID=-1&docTypeEID=1&langEID=1&tStamp=20100813134422483>.

has not yet created the website, the contract shall be published in the Commercial Journal.

Exceptions to this provision are contracts for protection of life, health, property or the environment; these shall enter into force, if necessary, without prior publication.

The publication duty shall apply to all contracts which have been concluded prior to entry into force of the amendment; however, their effectiveness shall not be assessed in terms of the new regulation. The proposed entry into force date of the amendment is 1 December 2010 (1 January 2011 with regard to part of its content).

The Act No. 215/2004 Coll. on the Protection of Confidential Information states that Confidential Information Lists are created by the head of each authority that deals with confidential information. That means that one of the duties of the head of the authority is to determine the fundamental scope of classified information, and unless he or she determines otherwise, to decide on the period of, change to, and expiration of, the security classification level. The information can be classified as confidential information only in fields stipulated by the Government of the Slovak Republic in regulation No. 216/2004.

On 19 August 2002, the National Council of the Slovak Republic adopted the Act on Access to Documents Concerning the Activities of the State Security Services between 1939 and 1989 and on Establishment of the Institute of National Memory Act No. 553/2002 Coll. (National Memory Act). The National Memory Act allows Slovak citizens and foreigners to request access to documents containing information about the applicants that was collected and maintained by the state security services between 1939 and 1989. The Act purports to provide historians, victims, and their relatives with access to documents collected by the former state security services.⁷⁵

The National Memory Act sets forth the principles for evidence, collection, registration, disclosure, and management of certain documents created and maintained by the security services of the German Third Reich and the former Soviet Union as well as the Czechoslovak and Slovak security agencies in the so-called "totality era," the period from 18 April 1939, to 31 December 1989. Specifically, the National Memory Act deals with documents concerning crimes committed against Slovak nationals as well as Slovak citizens of other nationalities. The crimes in question include (i) Nazi crimes, (ii) communist crimes, (iii) other crimes against peace or humanity, or war crimes, and (iv) other retaliations for political reasons.⁷⁶

In 2009 the Supreme Court of the Slovak Republic decided in a case initiated by a natural person against the National Memory Institute, a public law institution established by the

⁷⁵ Email from Zuzana Babicová, Office for Personal Data Protection, Slovak Republic, to John Baggaley, EPIC, 16 June 2003 (on file with EPIC).

⁷⁶ *Id.*

National Memory Act to carry out the collection, preservation, maintenance, and public divulgence of the relevant archives.

The case concerned the public disclosure of the plaintiff's personal data stored in the secret police archives under the category of "confidants" i.e., persons deemed to be of interest to the secret police, but who were not knowingly collaborating with the secret service as were informants, agents, etc. The plaintiff asserted that his privacy had been violated on the grounds that by publicly disclosing his personal data on the website of the National Memory Institute archives, the archives had created the chance that – in the eyes of the broader public opinion – his position of "confidant" might be interchanged or mistakenly confused with the position of people collaborating with the secret police as, e.g., agents and informants.⁷⁷ The legal action was filed under the Civil Code regulation on personal privacy protection, Section 11 *et seq.* The Supreme Court of the Slovak Republic, deciding on the appeal of the Nation's Memory Institute, upheld the decision of the regional court of second instance. The decision prohibited the National Memory Institute from disclosing publicly, in any form, the personal data of the plaintiff – deriving from the list of personal files of the members of security units (No. 23461) – without the plaintiff's consent.

This decision summarises the line of argumentation that has been followed by the courts in the past and, in certain aspects, represents a landmark decision that may be used in the future as a precedent for further privacy protection actions seeking termination of the disclosure of a "confidante's" data.

The decision is interesting in two other aspects. Firstly, it appears that the Supreme Court has succumbed to the layperson's interpretation of the term "confidante", which sometimes is identified with collaborating persons. In fact, the term "confidante" had been excluded from this category of persons by the Act, as well as by the case-law of the Constitutional Court. Thus, the Supreme Court based the infringement of the plaintiff's privacy (dignity) on the mere possibility of mistaken identity with collaborating persons. Secondly, the decision may be considered somewhat controversial taking into account that it dismissed the statutory duty of the National Memory Institute to disclose the transcripts of records, which represents a statutory licence for the disclosure of personal data of natural persons.

OTHER RECENT FACTUAL DEVELOPMENTS

In 2008, a new Act No. 167/2008 Coll. on Periodicals and Agency News Service and the amendment and supplementing of certain acts (Press Act)⁷⁸ replaced the previously Act. No. 81/1966 Coll. on Periodical Press and other Means of Mass Communication as amended.

⁷⁷ Slovak Supreme Court, RefNo. 5 Cdo 83/2008, at nssr.blox.sk.

⁷⁸ Available in English at <http://www.culture.gov.sk/uploads/3q/P0/3qP0AW8PvDmgayCVare-sg/act-168.pdf>.

In particular, the new Press Act provides the right of the publisher of periodical press and news agency to get and publish information about public authorities.⁷⁹ It establishes the duty of the publisher to protect the source and the content of the information. It further regulates the responsibility of the publisher and the news agency for the content of the information published,

Beside reaffirming the Slovak legal system's already established right to ask that false statements of facts about a person or legal entity be corrected, the new Press Act introduced the right of reply and right of supplementary information. These new rights should reflect the conclusions drawn in the public debate concerning how to strike a fair balance between the right of free expression and the press, on the one hand, and the right of protection of name and reputation of natural persons and legal entities on the other.

The right of reply is currently being reconsidered by the present Ministry of Culture and Tourism within the planned amendment to the Press Act, as the Slovak Press Syndicate raised an objection in particular in respect of the missing criteria for assessment of exerting the right to reply.⁸⁰

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

Noteworthy are *e.g.* the activities of non-governmental organisation "eSlovensko", *o.z.* ("citizens' association"), which operates the Slovak Awareness Centre under the EU "Safer Internet" Programme. The Slovak Awareness Centre also initiates and coordinates activities associated with the celebration of Safer Internet Day.⁸¹ In cooperation with its partners including the OPDP, eSlovensko prepares media plans and produces outputs for the national campaigns and competitions, such as the above-mentioned project www.zodpovedne.sk.⁸²

⁷⁹ Id. See, in particular, Article 3 stating that, "Public authorities, budgetary organisations and grant-funded organisations that they establish and legal entities established by law are obliged, on a basis of equality, to provide the publishers of periodicals and press agencies with information on their activities in order to supply true, timely, and impartial information to the public."

⁸⁰ "Krajcer rokoval o tlačovom zákone" ("Krajcer Discussed the Press Act"), [Webnoviny.sk](http://www.webnoviny.sk/media/krajcer-rokoval-o-tlacovom-zakone-/230856-clanok.html), 5 October 2010, available in Slovak at <http://www.webnoviny.sk/media/krajcer-rokoval-o-tlacovom-zakone-/230856-clanok.html>.

⁸¹ English summary of the eSlovensko *o.z.* activities available at http://www.zodpovedne.sk/kapitola_ostatne.php?cl=english_language.

⁸² Personal data protection focused episode available at <http://www.youtube.com/watch?v=BS3BZJWbEco&feature=related>.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Slovakia is part to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol that establishes an individual complaint mechanism.⁸⁴

Slovakia is a member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁸⁴ It has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)⁸⁵ and its Additional Protocol regarding supervisory authorities and transborder data flows.⁸⁶ Slovakia has signed and ratified the Convention on Cybercrime (ETS No. 185).⁸⁷

In 2006, the European Court of Human Rights (ECtHR) issued a decision on the impossibility of challenging a judicial declaration of paternity in court under Slovakia's legal system. In 1970, a court determined that the appellant was the father of a minor, to whom he subsequently paid support. Decades later, retesting with improved methods determined that the appellant was not in fact the child's father. However, he was unable to remove this status from several public documents, and was concerned how this legal finding of paternity would affect the disbursement of his estate. The ECtHR found that the appellant's inability to change this finding was a violation of the individual's right to privacy found at Article 8 of the European Convention on Human Rights.⁸⁸

As of 2009, the ECtHR had rendered two rulings against Slovakia for violating the right to privacy. In one case, a domestic court restricted the legal capacity of a person suffering from mental illness. The woman was required to wait three years before applying to have her full legal capacity restored, during which time she was restricted from acting on her own before public authorities. In March 2009, the ECtHR ruled that this extended period was excessive and interfered with her right to privacy. In the second case, the Ministry of the Interior authorised an investigative team to wiretap a lawyer's mobile phone in order to obtain information concerning one of the lawyer's clients who was suspected of being

⁸³ Slovakia has been part to the ICCPR and to its First Optional Protocol since 28 May 2003. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁸⁴ Signed 21 February 1991, ratified 18 March 1992, entered into force 1 January 1993, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=28/09/2010&CL=ENG>.

⁸⁵ Signed 14 April 2000, ratified 13 September 2000, entered into force 1 January 2001, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=1&DF=10/09/04&CL=ENG>.

⁸⁶ Signed 8 November 2001, ratified 24 July 2002, entered into force 1 July 2004, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=8&DF=28/09/2010&CL=ENG>.

⁸⁷ Signed 4 February 2005, ratified 8 January 2008, entered into force 1 May 2008 available at <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

⁸⁸ European Court of Human Rights, Appl. No. 10699/05 10 October 2006, *Paulik v. Slovakia*, <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbk&action=html&highlight=PAULIK&sessionId=59734949&skin=hudoc-en>.

involved in organised crime activities. The ECtHR ruled that such interference with the right to privacy was unlawful.⁸⁹

Slovakia joined the Organisation for Economic Cooperation and Development (OECD) in September 2000.

On 1 May 2004 Slovakia joined the European Union. Further obligations have arisen, in particular from the membership of the Slovak Republic in Europol, the Schengen Information System, Customs Information System, Working Group on Police and Judicial Cooperation, Coordination Working Group for Eurodac and Schengen Evaluation Working Group (SCHEVAL).

* Updates to the Slovak Report published in the 2010 edition of EPHR have been provided by: Marian Lauko and Michal Marhefka, Weinhold Legal, Slovak Republic.

⁸⁹ "2009 Human Rights Report:Slovakia,"supra. Judgements, decision, reports and other relevant documentation of the ECtHR can be consulted on-line at <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>.

REPUBLIC OF SLOVENIA

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The right to privacy appears in two forms in the 1991 Slovenian Constitution,¹ as an individual right of a private character and as a human right, meaning that it also has a public nature.²

Privacy rights are covered in the second section of the Constitution, which protects various aspects of privacy. Article 35 on the Protection of the Right to Privacy and of Personal Rights states, "The physical and mental integrity of each person shall be guaranteed, as shall be his right to privacy and his other personal rights." Article 37 on the Protection of Privacy of Post and Other Means of Communication states, "The privacy of the post and of other means of communication shall be guaranteed. In accordance with the statute, a court may authorise action infringing on the privacy of the post or of other means of communication, or on the inviolability of individual privacy, where such actions are deemed necessary for the institution or continuance of criminal proceedings or for reasons of national security."³

Article 38 on the Protection of Personal Data specifically deals with data protection. It states, "The protection of personal data relating to an individual shall be guaranteed. Any use of personal data shall be forbidden where that use conflicts with the original purpose for which it was collected. The collection, processing and the end-use of such data, as well as the supervision and protection of the confidentiality of such data, shall be regulated by statute. Each person has the right to be informed of the personal data relating to him which has been collected and has the right to legal remedy in the event of any misuse of that data."⁴

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

Slovenia has been a member of the European Union since 2004, which means that all EU directives are effective in the country. Slovenia enacted in 1999 the Personal Data

¹ Constitution of the Republic of Slovenia 1991, available at <http://www.up-rs.si/up-rs/uprs-eng.nsf/dokumentiweb/063E5907BE5B679CC1256FB20037658C?OpenDocument>.

² Komentar Ustave Republike Slovenije (Comments about the Constitution of the Republic of Slovenia) 369 (Sturm & Lovro eds., Ljubljana, Fakulteta za podiplomske državne in evropske studije 2002).

³ The means of communication are interpreted in the widest sense of the word: it may include telephone communications, emails, SMS messages and the like, since the form or content of communication is irrelevant in this context. Privacy protection also applies to private telecommunication systems, as well as traffic data, which are also an integral part of communications (i.e., telephone numbers, data about the duration of a communication or the quantity of data transmitted, etc.). *Id.* at 395-396.

⁴ Constitution of the Republic of Slovenia 1991, *supra*.

Protection Act (PDPA) based on the EU Data Protection Directive 1995/46/EC⁵ and the Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).⁶ In this law, private entities may process personal data only if they have obtained individuals' written consent, or if law regulates the data processing.

On 1 January 2005, a new version of the PDPA came into force. The new act, which modernises the previous version from 2001, follows some changes in the area of personal data processing that occurred in the recent years. PDPA now covers automatic decision making, use of video surveillance cameras, biometrics, collecting of data about entrances and leavings from premises. PDPA meets all requirements of the 1995 EU Data Protection Directive.⁷

The PDPA provides that everything that is not explicitly allowed in connection with personal data collection and processing is prohibited. Public entities may only process personal data for which they have been granted legal authorisation, while private entities must receive written consent from individuals. Persons whose personal data are gathered must be informed in advance of the purpose of the collection of data (by giving their written consent or where the purpose of collection is authorised by law). In principle, personal data can be gathered and stored for only as long as needed to meet that objective, and deleted or blocked once the objective is met. All exemptions must be defined in the law. Use of video surveillance in the workplace is allowed only under special circumstances (if it is necessary for security of the people or wealth, protecting secret data or business secrets and this purpose cannot be achieved by less intrusive means). Employees must be presented with a written notice about this measure, the same applies to the use of biometrics in the private sector.

The PDPA also defines in detail the duties of the data controller. It is prohibited to use the same identifier in databases maintained in the areas of public safety, state security, defence, judiciary and health. The connection between these databases is allowed only if there is a legal basis or the individual has given his or her written consent. The data controller of such databases must enable access for the individual free of charge within 15 days of receiving his or her request, as well as provide a copy of an individual's personal data within 30 days of receiving the request. If a data controller fails to fulfil this obligation, he or she must provide a motivation for doing so in writing. In case an individual's personal data are transferred to recipients, the data controller must supply, at that individual's request, the list of recipients within a 30-day deadline.

⁵ Directive 1995/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, Official Journal L. 281, 23 November 1995, at 31–50, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

⁶ Personal Data Protection Act, Official Gazette of the Republic of Slovenia, No.86/04 and 113/05, available at <http://www.ip-rs.si/index.php?id=339>.

⁷ Directive 1995/46/EC, *supra*.

If an individual provides evidence that his or her personal data were gathered in breach of the law, the data controller must delete the data, or update and correct them if the data were inaccurate or incomplete. The data controller must bear those costs, and must also keep a separate catalogue for each database, which contains, among other things, a detailed description of the kind of data gathered and the manner in which they are gathered, the purpose of their use and the duration of storage, the list of their users and a description of how they are secured. Furthermore, the Ministry of Justice, which is responsible for the protection of personal data, must keep a register of all databases containing personal data. Information in this register is provided by data controllers and is publicly available on the Internet.

Special protections are set out for "sensitive data," defined as data on racial or other origins, political, religious or other beliefs, trade union membership, sexual behaviour, criminal convictions and medical data. This data must be specially labelled and may only be transferred across telecommunications networks if it is protected by "encryption methods" and an "electronic signature" that can guarantee illegibility. The law also imposes cross-border restrictions providing that data may only be transferred to countries that have a data protection legal framework as adequate as the Slovenian one. Article 62 explicitly states that there are no cross-border restrictions for the EU member states.

Amendments to PDPA also include exemptions for notification of data filing systems to the Information Commissioner, and the striking of a data controller's obligation to prepare internal acts governing protection of personal data for data controllers with less than 50 employees. There were also adopted special rules governing the costs regarding right of access of an individual to his/her personal data, processed by data controllers.

Sector-based laws

Besides the PDPA, there is also specific legislation regarding processing of personal data in different specified sectors. Among this sector-based legislation is the Electronic Communications Act (*ZEKom-B*) that was recently amended in 2009.⁸ The amendment to the Act shortened the data retention period (from 24 months to 14 months for telephone communications, and eight months for internet communication) and defined new rules (with appropriate safeguards) for fast disclosure of traffic and location data in cases involving the protection of human life.⁹ Additional safeguards regarding privacy and data retention are defined in the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Data Stored, adopted in 2008.

⁸ A 2007 version of the Act (before it was amended in 2009) is available in English at <http://www.ip-rs.si/index.php?id=504>.

⁹ ZeKOM-B, 2009 amended version available in Slovenian at <http://www.uradni-list.si/1/objava.jsp?urlid=2009110&stevilka=4985>. Cfr. Section "Data Retention," *infra* in this Report.

In 2008 the Patients Rights Act was also adopted. Some of its provisions deal with medical privacy.¹⁰

The Law on National Statistics regulates the privacy of information collected for statistical purposes.¹¹

The Penal Code specifies sanctions for an invasion of territorial privacy in Articles 149 and 152. Article 149 prohibits unauthorised recording or image taking of individuals or their premises if such an act entails a serious invasion of privacy. Article 152 specifies sanctions for the violation of dwellings through an unauthorised entry into, or search of, private facilities, or an attempt to do so.

DATA PROTECTION AUTHORITY

With the merger of two offices, the Inspectorate for Personal Data Protection and the Commissioner for Access to Public Information, the Information Commissioner, an autonomous and independent body, was established on the basis of the Information Commissioner Act (ICA) on 31 December 2005.¹² The body supervises both the protection of personal data and access to public information.¹³ The competencies of the Information Commissioner, as laid down in ICA, Personal Data Protection Act (PDPA) and Inspection Act (IA), are relatively wide.¹⁴

The formation of the office of the Information Commissioner had a strong impact on personal data protection in Slovenia. Much of the strengthened activities can be attributed to substantially increased staff, which resulted in swifter reactions to complaints, an increased number of legal opinions, a more pre-emptive approach to data protection and a wider public awareness regarding the right to privacy.

As concerns the Information Commissioner's inspection competencies, the number of investigated cases continued to increase dramatically – a total of 231 complaints were received in 2006 (up from 91 in 2005 and 78 in 2004). Of those, 88 were directed towards the public sector and 143 towards the private sector. Most complaints in the public sector dealt with the unlawful transfer of personal data (35), unlawful collection of personal data (17) and insufficient protection of personal data (16), whereas unlawful transfer of personal data (41), unlawful implementation of video surveillance (28), and disproportional collection of personal data (24) were among the most common

¹⁰ Patient Right's Act (ZPacP), in Slovenian at <http://www.ip-rs.si/zakonodaja/zakon-o-pacientovih-pravicah/>.

¹¹ Law on National Statistics, 25 July 1995.

¹² Information Commissioner Act, published in Official Gazette of the Republic of Slovenia, No. 113/2005, unofficial English translation available at Information Commissioner's website, at <http://www.ip-rs.si/index.php?id=325>.

¹³ *Id.*

¹⁴ Inspection Act, Official Gazette of the Republic of Slovenia No.43/07.

complaints regarding the private sector. In 41 cases, the State Supervisors found no breaches of the PDPA and these cases were dismissed.¹⁵

During 2009, the Information Commissioner received 624 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act; namely 219 in the public sector and 405 in the private sector. There were 165 applications and complaints against public sector legal entities, 54 procedures were initiated *ex officio*; whereas 332 applications and complaints were made against private sector entities, and 73 procedures initiated *ex officio*. Statistical data indicates that the number of applications as to alleged violations of Slovenia's Personal Data Protection Act remained at almost the same level as in 2008 (from 1996 to 2008 the number of complaints increased exponentially). Following assessment of the received applications and *ex officio* cases, 124 inspection procedures were initiated in relation to public sector entities, and 267 in private sector entities. 298 physical inspections were carried out in the scope of inspection procedures. On the basis of Article 33 of the Inspection Act, 66 cautions were issued in relation to minor irregularities. Also handed down were 47 regulatory and administrative decisions whereby the liable persons were ordered to undertake measures to rectify the established irregularities. Finally, 338 inspection procedures were concluded with a decision to stay the proceedings. In 2009, most cases of suspected violations of the Personal Data Protection Act pertained to: illegal collection or request for personal data (134 instances); disclosure of personal data to unauthorised users by a personal data collection controller (110); illegal publication of personal data, for example on notice boards and in the media (77); illegal video surveillance (57); insufficient security measures to ensure adequate protection of personal data (54); misuse of personal data for the purpose of direct marketing (38); other issues, such as illegal implementation of biometrics, as well as the processing of personal data in a manner discordant with the purpose for which it was collected (27).¹⁶

The Information Commissioner also manages and maintains the Register of data filing systems of data controllers which is available at the Commissioner's website.¹⁷

In 2008 the Information Commissioner decided on a case pertaining to the illegal processing of personal data in relation to two insurance companies. The inspection procedure revealed that personal data in relation to 2,382 erstwhile insured persons had been transferred, without any legal basis or the consent of the individuals to which the data pertained. The Information Commissioner levied fines as a consequence of the unlawful collection and transmission of personal data pertaining to 26 individuals, for whom conclusive evidence has been provided, as well as for making such data available and not providing any traceability as to the transfer itself. One insurance company lodged

¹⁵ Email from Sonia Bien and Andrej Tomsic, Information Commissioner of Slovenia, to Allison Knight, Research Director, Electronic Privacy Information Center, 30 May 2007 (on file with EPIC).

¹⁶ For more detailed information, see Information Commissioner 2009 Annual report, available in English at http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual-report-2009.pdf.

¹⁷ Information Commissioner of Slovenia, in Slovenian at <http://www.ip-rs.si>.

an appeal against the Information Commissioner's ruling and requested judicial protection; the other insurance company has settled one half of the imposed fine, and formally appealed in relation to the remainder. The fines are the highest ever imposed by the Information Commissioner.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

In 2008, the Information Commissioner issued a regulatory decision in a case against the Ministry of Foreign Affairs regarding the lawfulness of the processing of personal data by means of acquiring a copy of telephone numbers from a fixed telephone network including those numbers which had been dialled as well as those numbers from which incoming calls had been made. The Ministry was ordered to destroy the CD on which the related list of telephone numbers was stored.¹⁸

For the purpose of the internal investigation within the Ministry and with the aim of identifying the employee who handed over a diplomatic mail to a journalist of the daily newspaper all traffic data from a certain period were collected. Thus a database was created containing approximately 110,000 items of traffic data. In accordance with the Electronic Communications Act¹⁹ the traffic data are granted double protection, namely the protection of the privacy of correspondence and other means of communication according to Article 37 of the Constitution of the Republic of Slovenia and also the protection of personal data according to the Article 38 of the Constitution.²⁰ Since traffic data are considered to be personal data as they relate to an identified or identifiable natural person, in a case of illegal intervention such as this, there was a double violation of rights, namely on the side of the employees of the Ministry as well as on the side of all those called by the employees or who dialled the latter's telephone numbers. The Information Commissioner stated that the Ministry acquired and used the data for the inadmissible purpose of investigating the traffic data to establish which employees called the newspaper. Additionally, from the point of view of the principle of proportionality, the case of a clear lack of proportionality was established as by virtue of the acquisition of the aforementioned traffic data, no evidence has been found that someone actually leaked a specific document.²¹

Other relevant case law concerning privacy and data protection is categorised and discussed under the corresponding section.²²

¹⁸ 12th Annual Report of Article 29 Data Protection Working Party (2008), 16 June 2009, at 92, available at <http://www.ip-rs.si/index.php?id=325>.

¹⁹ *Cfr.* Section "Data retention," *infra*.

²⁰ *Cfr.* Section "Constitutional Privacy and Data Protection Framework," *supra*.

²¹ 12th Annual Report of Article 29 Data Protection Working Party (2008), *supra*, at 92.

²² *Cfr.* Section "Data Protection Authority," *supra* and Sections "Data Retention," "Video surveillance," "Health & Genetic Privacy," and "Financial Privacy," *infra*.

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

The right to privacy of communication is guaranteed by the Constitution²³ and is also covered by Article 150 of the Penal Code that prescribes sanctions for the violation of the secrecy of means of communication. This article prohibits unauthorised opening of letters and other postal messages and interception of messages transmitted via telecommunications networks, or reading of their contents without opening a letter or other postal messages. Similarly, it prohibits unauthorised acquaintance with the content of a message transmitted by telephone or other telecommunications equipment, as well as the unauthorised forwarding of someone's letter to a third party. Article 151 further prohibits the publication of private communications without consent by the authorised person.

Privacy of communication may only be invaded by a court order, and if such an invasion is deemed necessary for the purpose of criminal proceedings, or in order to protect the security of the state. In Slovenia, this area is regulated by the Criminal Proceedings Act and the Slovenian Intelligence and Security Agency Act (SISAA) and carried out by the police and Slovenian Intelligence and Security Agency (SOVA).²⁴

The Criminal Proceedings Act includes a detailed list of criminal offences and cases in which the privacy of communications may be invaded (with a court order), but the SISAA is not as specific. For example, it stipulates that state security is threatened by "activities aimed against...the strategic interests of the Republic of Slovenia", but experts draw attention to the problems potentially arising from such a wording that enables broad interpretations of "strategic interests" in contrast to other more well-defined criminal offences. However the SOVA does not prosecute criminal offenders. If it deals with a suspected criminal offence, it must provide information about it to the director general of the police force and the public prosecutor. SOVA is compelled to inform the Prime Minister about its activities and findings, as well as the President of the Republic, the President of the National Assembly and other ministers if these activities are related to their fields of competence.

In general, a judge's warrant must be issued prior to a house search or telephone tapping. A new Law on the Police, adopted in 1998, allows secret observation and following, and secret police collaboration, to be authorised under very special circumstances by a

²³ Cfr. Section "Constitutional Privacy and Data Protection Framework," *supra*.

²⁴ Criminal Proceedings Act (ZKP-UPB4), consolidated version, in Slovenian at <http://www.uradni-list.si/1/objava.jsp?urlid=200946&stevilka=2283>; the Slovene Intelligence and Security Agency Act (ZSOVA-UPB2), consolidated version, in English at <http://sova.gov.si/en/media/zsova.angl.upb2.pdf>.

General Police Director.²⁵ However, the wording of the SISAA allows for potential abuse on the part of the SOVA, because it could result in SOVA acquiring too easily a court warrant for communications interception.

Article 50 of the Postal Services Act states that providers of postal services should enable an authorised body to access, on the basis of a court order, the content of post. Both telephone operators and providers of postal services must ensure an indelible record of such moves.²⁶

In 2008, the Commissioner lodged a request for a constitutional review of the Slovenian Intelligence and Security Agency Act, a review of the provisions regarding the strategic telecommunications supervision, which implies emergence of personal data filing systems.²⁷ The Commissioner requested that the Constitutional Court determine the discrepancies between certain provisions of the Act and Article 38 of the Constitution (basic human right to data protection or information privacy).²⁸ The Commissioner also requested that the Court determine whether the provisions of the Act were in accordance with Article 37 of the Constitution which provides for communication privacy and defines the conditions and limitations regarding breaches of this fundamental right.²⁹ Communication privacy may only be suspended under very strict conditions, for the institution or course of criminal proceedings or for reasons of national security when prescribed by law and on the basis of a court order. The Constitutional Court rejected the Information Commissioner's request for formal reasoning, as the applicant did not show that the question of constitutional review arising in connection with a procedure he was conducting and therefore procedural conditions have supposedly not been fulfilled. The Constitutional Court was of the opinion that the Security Agency Act is precise enough in defining that wiretapping of international communications (so-called strategic surveillance of international communications) is only allowed when the telephone number and person are not defined. It has to be stressed that during the inspection process the Commissioner has found out that the surveillance was conducted according to the specific telephone number and hence an identifiable person. The law, however, does not allow for strategic surveillance of the international communication, but the constitutional legal question of this case was whether the surveillance of the strategic international communication can be allowed by the director of the Surveillance Agency as the law stipulates or only the court has that power as Constitution demands. The question remains unanswered. The Commissioner was of the opinion that the article giving the director the power to order surveillance was unconstitutional.

²⁵ Article 49, Law on the Police, 18 July 1998.

²⁶ Postal Services Act (ZPSto-2), in Slovenian at http://www.aperk.si/sl/zakon_o_postnih_storitvah_zpsto_2.

²⁷ 12th Annual Report of Article 29 Data Protection Working Party (2008), *supra*, at 94-95.

²⁸ *Cfr.* Section "Constitutional Privacy and Data Protection Framework", *supra*.

²⁹ *Id.*

Data retention

On 1 May 2004, the Electronic Communications Act came in effect. This Act regulates Internet communications; is compatible with the EU Privacy and Electronic Communications Directive, and replaces the former Telecommunications Act. Article 104 is about traffic data. It requires that subscribers and users' traffic data processed and stored by an operator be erased or made anonymous as soon as it is no longer needed for the transmission of a message. Operators may store and process traffic data required for billing and interconnection payments only until payment for services or if they have the user's prior consent. Location data other than traffic data relating to users may be processed only in anonymous form or on the basis of the user's prior consent, according to Article 106. Article 107 states that operators shall be obliged at their own expense to ensure adequate equipment and appropriate interfaces enabling lawful interception of communications in their networks, and minister for information society shall prescribe the equipment and determine appropriate interfaces in ordinance, with agreement with the minister for internal affairs, the minister for defence, and the director of SOVA.

On 1 June 2004, an important discussion took place at a meeting among representatives of the Ministry of Information Society, the Ministry of the Interior, police authorities and some Internet service providers (ISPs) (including a representative of SISPA, the Slovenian ISP association) to discuss the implementation of the requirement of the Electronic Communications Act that compels operators to pay the expenses for equipment enabling lawful interception of communications in their networks.³⁰ Since these expenses were estimated to be between €100,000 and €700,000 per operator, small ISPs had a good reason to fear for their survival. In response to those concerns, representatives of the Ministry of the Interior and the police proposed to create one central interception centre to decrease the costs per operator.³¹ Concerns were also shared that small ISPs may not have enough people and expertise to operate interception devices. The police offered to help manage them.

The Act on Electronic Communications was amended in December 2006 in order to transpose the EU Data Retention Directive into the Slovenian legal system.³² The amendments foresaw a 24-month retention of traffic data; both the Information Commissioner and members of civil society criticised the amendment. The amendment concerning data retention of telephony services entered into force on 15 September 2007, whereas data retention in the field of Internet, email and Internet telephony entered into

³⁰ Not all Slovenian ISPs are members of SISPA.

³¹ Proceedings from the meeting: Ministry of Information Society, Realisation of lawful interception of telecommunications traffic which flows over the Internet, 1 June 2004 (on file with EPIC).

³² Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 15 March 2006, OJ L 105, 13 April 2006, at 54-63, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML>.

force on 15 March 2009. Inspections concerning retention of traffic data are assigned to the Information Commissioner.

As reported above, the Electronic Communications Act (*ZEKom-B*)³³ was recently amended in 2009. The amendment to the Act shortened data retention period (from 24 months to 14 months for telephone communications and eight months for internet communication) and defined new rules (with appropriate safeguards) for fast disclosure of traffic and location data in cases for the protection of human life.

National databases for law enforcement and security purposes

No specific information has been provided under this section.

Cybercrime

Intrusion into a computer system is the subject of Article 242 of the Penal Code, but such an intrusion is punishable only if it is connected with business dealings, and made with the aim of acquiring illegal property-related benefits, or causing material harm to others.³⁴ Article 154 provides for sanctions and prohibits any use of personal data that is in breach of the law, or any intrusion into an electronic database for the purpose of obtaining some item of information for personal use or for a third party's use. Article 225 also prohibits unauthorised access to an unprotected database, the modification and copying of its content, or the insertion of viruses. The conditions under which personal data may be gathered, processed and used are regulated by the PDPA.

INTERNET & CONSUMER PRIVACY

E-commerce

The revised Consumer Protection Act (CPA) that was enacted in January 2003 incorporates the EU E-Commerce Directive (2000/31/EC).³⁵ Article 45(a) states that companies (e.g., direct marketing companies) may use the automatic telephone dialling system only with consumer's previous consent. The same is true for fax messages and email messages (i.e. spam). The company must also exclude the consumer from the contact list if he or she makes such a request. The fines average €4,200 for physical persons and €12,600 for companies. The CPA only protects individuals, but Article 109 of the Electronic Communications Act protects companies from receiving spam.

³³ ZeKOM-B, 2009, *supra*.

³⁴ Unfortunately, this wording could lead to a situation in which an intrusion into a computer system not resulting in material harm, or not yielding other kinds of benefit for the intruder, would not be sanctioned. In such a case Article 309, which sanctions the production or acquisition of tools for intrusion into a computer system, has to be applied.

³⁵ Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), 8 June 2000, OJ L 178 17 July 2000, at 1-16, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF>.

There is no regulation of cryptography in Slovenia. The Electronic Commerce and Electronic Signature Act and the PDPA are even encouraging the use of cryptography and digital signatures. Slovenia also has a right against self-incrimination, which means that a suspect is not compelled to reveal his cryptographic keys.³⁶

TERRITORIAL PRIVACY

Video surveillance

Video surveillance is covered in PDPA and the Private Protection Act that was enacted in November 2003. PDPA requires that administrators of video surveillances system publish a notice about video surveillance. The notice must contain information about who is performing video surveillance, where, and where an individual can get information about data retention periods. The video surveillance system must be protected from unauthorised access. Article 43 of Private Protection Act allows video surveillance systems to be operated only by private guards with a license. The law contains provisions about maximum retention periods of video and audio data. It also mandates video surveillance users to notify people about the monitoring. Failure to notify can carry penalties of up to €12,500.

In 2006, the Information Commissioner inspected the unlawful video surveillance that was going on for some years in a well-known shopping mall. Paragraph 3 Article 77 of the PDPA clearly states that video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. The inspection procedure performed by the Information Commissioner revealed that the shopping centre had indeed been conducting video surveillance in changing rooms, thus breaching the individual's right to privacy in national data protection legislation. This case was given great publicity which resulted in an overflow of complaints against several applications of video surveillance that eventually led to both greater awareness as well as increased respect of legal provisions governing video surveillance.³⁷

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Slovenia is included in the US visa waiver program and is required to produce biometric passports. Slovenia began issuing the passports in August 2006.³⁸

³⁶ Article 5 of the Criminal Proceedings Act.

³⁷ Email from Sonia Bien and Andrej Tomsic, *supra*.

³⁸ See http://travel.state.gov/visa/temp/without/without_1990.html.

NATIONAL ID & SMART CARDS

Slovenia has ID cards. The ID Card Act requires all adults to have and carry a valid ID card with a photograph (Article 2) and to show it to authorities when required. Non-compliance with this requirement carries fines of up to €420.⁴⁰

BODILY PRIVACY

Article 79 of the PDPA states that biometric measures in the public sector may only be provided for by statute if it is required for the security of people or property or to protect secret data and business secrets and if this purpose cannot be achieved by milder means. Irrespective of this provision, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders. This provision provides legal ground for the introduction of biometric passports that were introduced in 2006 to comply with US VISA Waiver Program (VWP) requirements.⁴⁰

Article 80 of the PDPA regulates that the private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance. If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall, prior to introducing the measures, be obliged to supply the Information Commissioner with a description of the intended measures and the reasons for the introduction thereof. The Information Commissioner is obliged to decide within two months whether the intended introduction of biometric measures complies with the PDPA.

The Information Commissioner received 40 applications concerning the implementation of biometric measures during 2007, 16 applications in 2008, whereas in 2009 it received just 10 such requests, which means that the number of such applications is decreasing. Six decisions as to the admissibility of biometric measures were issued in 2009, of which two had been lodged in 2008; one application was withdrawn by the applicant. Four decisions vindicated the implementation of biometric measures; limited implementation was approved in three instances, while two decisions explicitly proscribed the introduction of biometric measures.⁴¹

Police have a right to take a picture, fingerprints, and saliva samples from suspects, as provided by Article 149 of the Criminal Proceeding Act. Police also can use DNA samples for criminal investigations.

³⁹ The ID Card Act – Consolidated version, (ZOIzk-UPB2) in Slovenian at <http://www.uradni-list.si/1/objava.jsp?urlid=200871&stevilka=3100>.

⁴⁰ *Id.*

⁴¹ Information Commissioner's Annual Report for 2009, in English at http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual-report-2009.pdf.

WORKPLACE PRIVACY

The Labour Relations Act prohibits employers from asking employees or employment candidates questions about family matters, marital status, pregnancy, or other information that is not work-related.⁴²

The Information Commissioner also prepared draft legislation regarding workplace privacy in 2009, but the draft has not been considered in parliament yet.

Case law also dealing with a form of monitoring employees by the Ministry of Foreign Affairs has been reported above.⁴³

HEALTH & GENETIC PRIVACY

Medical records

In 2008 the Patients Rights Act was adopted, which additionally defines rules regarding medical privacy and enacts additional safeguards regarding medical privacy.⁴⁴

During the same year, the Commissioner dealt with serious cases of inappropriate protection of sensitive personal data.⁴⁵ During transport to the place where the data (orders for laboratory examinations) were supposed to be destroyed, cardboard boxes containing the data fell out of the truck and caused the data to be scattered across the motorway. The data controller – a primary healthcare centre – had entrusted the transport and destruction of files containing personal data to a contracted data processor, registered for performing activities of waste collection and transport. The healthcare centre, however, had not arranged mutual obligations regarding data processing by contract, which it should do according to PDPA. It had not given appropriate instructions as to the protection of data during transport and destruction, nor had it supervised the execution of procedures and measures for personal data protection by the contracted processor. Due to inappropriate protection of personal data and non-compliance with the statutory provisions regarding contractual processing of personal data, the Commissioner fined both the data controller (the health centre) and the processor – the company contracted to transport and destroy the documentation.⁴⁶

Another widely publicised case of inappropriate protection of sensitive personal data was uncovered during inspection supervision of the Institute of Oncology. The medical documentation – medical files containing data on deceased patients – was found to be stored in more than a hundred open, unprotected cardboard boxes placed in the corridor. Additionally, in the same widely accessible corridor, two cabinets were placed containing

⁴² Article 26 of the Labor Relations Act.

⁴³ *Cfr.* "Major Privacy & Data Protection Case Law," *supra*.

⁴⁴ Patient Right's Act (ZPacP), *supra*.

⁴⁵ 12th Annual Report of Article 29 Data Protection Working Party (2008), *supra* at 93-94.

⁴⁶ *Id.*, at 93.

partial documentation on patients currently receiving medical treatment. The data controller, which should have protected the data appropriately according to statutory provisions on sensitive data, was fined by the Commissioner.⁴⁷

FINANCIAL PRIVACY

The Commissioner has also been supervising protection of personal data by the employees in different registers of public administration, namely the justifications for access to the central register of taxpayers.⁴⁸ According to the PDPA data controller, in this case the Tax Administration of the Republic of Slovenia was obliged to enable subsequent determination of when personal data were entered into the filing system, used or otherwise processed. Thus the Commissioner was able to investigate all access to the computer base of taxpayers related to 15 publicly well known persons from Slovenia. The Tax Administration handed over to the Commissioner a list of employees who accessed the data of the aforementioned 15 persons within a period of eight months in 2008. Each of the employees was requested to justify the processing of the data and it was determined that only 47 out of 200 employees had accessed the data lawfully, namely for the purpose of conducting a taxation procedure. The rest of the employees had no justifiable reason for accessing the data. Curiosity was named as the most common reason for access to public persons' age or address data. The Commissioner issued warnings to the civil servants who accessed the data without sufficient legal basis as a lesson that personal data may not be accessed without lawful justification.

E-GOVERNMENT & PRIVACY

On 3 May 2005, the Electronic Central Register started to operate in Slovenia. This is a reference electronic population register enabling authorised administrators to access the population registry electronically. The register combined three separate registries that were kept on paper. It includes all information associated with births, deaths, and marriages, as well as name changes, adoptions, recognitions of fatherhood, and divorces. At the same time, an electronic register of households was set up. This means that all registers associated with administrative bodies have now been computerised. The project was launched in 2004 and cost SIT216 million (€900,000), which includes the upgrade of the population register as well as the registers of foreigners and citizenships.⁴⁹

The *eDavki* (eTaxes) portal enables all legal and natural entities to conduct business with the Tax Office electronically. Since 2004, taxpayers can use it to submit their income tax returns online by using a qualified certificate issued by any registered certification authority in the country. The entire process consists of filling out a form, validating data,

⁴⁷ *Id.*, at 93-94.

⁴⁸ *Id.*, at 94.

⁴⁹ "E-Register of Births, Deaths and Marriages Launched," Public Relation and Media Office, available at <http://web.archive.org/web/20060111015038/http://www.uvi.si/eng/slovenia/publications/slovenia-news/2014/2018/>.

digitally signing, and time stamping the form. The application also allows taxpayers to calculate the amount of their tax and import or export their data. Since 2007, the taxpayers automatically receive their prefilled tax declaration with the pre-calculation. If they don't object, they then just receive or pay the calculated amount of tax.⁵⁰

Citizens can consult databases with job offerings and to subscribe to a weekly electronic supply of pre-selected jobs related to the given profile of the job seeker. The unemployed can register as job seekers. Employers can also consult databases of candidates. Both Slovenian online job search services are at stage four maturity. The first one is provided by the Employment Service of Slovenia and the second by the Ministry of Public Administration.⁵¹

OPEN GOVERNMENT

Every person has the right to acquire information held by a public body, according to Article 39 of the Slovenian Constitution. In 2003, the Access to the Public Sector Information Act (APSIA)⁵² was enacted. It determines which public bodies are responsible for providing information and establishes an independent body, the Deputy for Access to Public Sector Information, whose main function is to be an appeal administrative body. The APSIA guarantees a free insight into public sector information and costs of transcripts are limited only to material costs. All public sector information must also be provided on the Internet, according to Article 10. Some types of information, such as personal data, or information important for national security are excluded from public sector information. The Ministry of Information Society is also required to issue a catalogue of public institutions that are bounded to APSIA. Slovenian Freedom of Information legislation is based on the guidelines of Article XIX⁵³ and is harmonised with all the European laws dealing with access to public information. The new version of the APSIA Act is being prepared. If it is adopted, it will extend the right to access public information with the introduction of the so-called "public interest test." The test allows Deputy to decide that some information must be made public, even when the legal exceptions to the contrary exist, if the greater public interest in that information prevails. Another proposed change is that commercial use of public information will not be free of charge as it is now.

⁵⁰ A detailed list and a short description of Slovenian E-government services are available in English at <http://www.epractice.eu/en/document/288365>.

⁵¹ *Id.*

⁵² APSIA is available at <http://www.ip-rs.si/index.php?id=324>.

⁵³ See <http://www.article19.org/>.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

There is no NGO dealing with privacy in Slovenia, There are, however, some blogs and web-based newspapers covering issues of privacy, such as *Slo-Tech.com* and *pravokator.si*.⁵⁵

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Slovenia is adopting part to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and acceded to its First Optional Protocol that establishes an individual complaint mechanism.⁵⁵

Slovenia is a member of the Council of Europe (CoE) and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁵⁶ It has also signed and ratified the Convention No. 108.⁵⁷ In May 2004, Slovenia ratified the CoE Convention on Cybercrime⁵⁸ and the Additional Protocol with provisions against racism and xenophobia in virtual networks.⁵⁹

On 1 May 2004, Slovenia joined the European Union.

* Updates to the Slovenian Report published in the 2010 edition of EPHR have been provided by: Matej Kovačič, University of Ljubljana, Slovenia; Andrej Tomsic, Office of the Information Commissioner, Slovenia.

⁵⁴ See <http://slo-tech.com/> and <http://hr-cjpc.si/pravokator/>, both in Slovenian.

⁵⁵ Slovenia became part of the ICCPR on 6 July 1992 and acceded to its First Optional Protocol on 16 July 1993. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁵⁶ Signed 14 May 1993; ratified 28 June 1994; entered into force 28 June 1994.

⁵⁷ Signed 23 November 1993; ratified 27 May 1994; entered into force 1 September 1994.

⁵⁸ Convention on Cybercrime (CETS No. 185), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&CL=ENG>.

⁵⁹ Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (CETS No. 189), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&CL=ENG>.

KINGDOM OF SPAIN¹

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The Spanish Constitution recognises the right to personal privacy, secrecy of communications, and the protection of personal data. Article 18 of the Constitution states, "(1) The right of honour, personal, and family privacy and identity is guaranteed. (2) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of a *flagrante delicto*. (3) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except in the case of infractions, and only by judicial order. (4) The law shall limit the use of data processing to guarantee personal and family honour, the privacy of citizens, and the full exercise of their rights."²

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The first Spanish Data Protection Act (LORTAD) was enacted in 1992, and was succeeded in 1999 by an amended Data Protection Act (LOPD) that brought Spanish law in line with the European Union Data Protection Directive.³ The LOPD applies to information held by the public and private sectors. The law establishes the right of citizens to know what personal data is contained in electronic records, and grants citizens the right to correct or delete incorrect or false data in those records. Additionally, the LOPD also restricts the disclosure of personal information to a third party by requiring the consent of the individual to the specific purpose for which the data was collected. Additional protections are also provided for sensitive personal data. Consumer groups, however, are concerned about the law's provisions allowing use of information without consent unless the consumer has opted out of such use. In 1999, regulations on the

¹ The EPHR 2010 "Spain" report has been updated in October 2010 by Antoni Farriols Sola, Comisión de Libertades e Informática (Madrid, Spain), in November 2010 by Ferran Adell, Universitat Autònoma de Barcelona (Barcelona, Spain), and in January 2011 by Javier Sempere (Agencia de Protección de Datos de la Comunidad de Madrid, Spain).

² Constitution of Spain, as amended August 1992, available at <http://www.constitucion.es/constitucion/lenguas/ingles.html>.

³ See Organic Law 5/1992 of 29 October 1992 Regulating the Automated Processing of Personal Data), Ley Orgánica 5/1992 de 29 de Octubre 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), enacted on 14 January 2000, available at http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=1992/24189; see also Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data (LOPD), (Ley Orgánica 15/99 de 13 de Diciembre 1999 de Protección de Datos de Carácter Personal (LOPD), available at http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=1999/23750.

secondary measures required to be taken to protect electronic data systems were issued in accordance with the LOPD.⁴

A new Royal Decree of 19 January 2008, which entered into force on 19 April 2008, implements the LOPD to prevent the use of personal data without the data subject's knowledge and prior consent. The data subject will be able to exercise his right to access, rectify, cancel or oppose the information, and revoke his consent with the data controller easily and free of charge. The Decree also establishes higher security measures for several types of personal data.⁵

Royal Decree 1720/2007 implements the Organic Law 15/1999 of Data Protection and introduces some novelties: it regulates minors' consent (under 14 years of age, it is necessary to get the parents' consent) and establishes the security measures that must be followed to process personal data in non-computerised databases. The new decree also establishes the administrative procedure a data controller must follow to avoid providing data subjects access to their personal data, the procedure to register codes of conduct, and the conditions upon which a data controller is authorised to process personal data for historic, statistical or scientific purposes. The Royal Decree also addresses other issues that were previously regulated in other royal decrees and instructions,⁶ such as international transfers of personal data, the enforcement process by the Spanish Data Protection Authority, the data subject's exercise of his right to access his personal data, as well as cancellation, rectification and objection rights.

Another Royal Decree of 8 January 2010 modified the LOPD to prevent the exchange and matching of personal data between databases without data subject consent.⁷

⁴ See Royal Decree No. 994/1999 of June 11, which Approves the Regulation on Mandatory Security Measures for the Computer Files which Contain Personal Data (Real Decreto 994/1999, del 11 de junio, por el que se Aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal), available at http://noticias.juridicas.com/base_datos/Admin/rd994-1999.html.

⁵ Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, 21 December 2007, BOE No. 17, 19 January 2008 (Royal Decree No. 1720/2007, 21 December 2007), available at https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf.

⁶ An Instruction ("instrucción") is a legal document elaborated by the AEPD that is binding for data controllers and regulates a specific area related to data protection (e.g., surveillance or international transfers).

⁷ Real Decreto 3/2010 Disposición adicional cuarta. Modificación del Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal aprobado por Real decreto 1/20/2007, 8 January 2010 (Royal Decree 3/2010), available in Spanish at https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/art.81.5b_RDLOPD.pdf.

Sector-based laws

Organic Law 4/2007 of 12 April 2007 about Universities⁸ allows the publication on the Internet of the grades of university students. Law 30/2007 of 30 October 2007 about Public Contracts⁹ regulates the conditions under which public bodies may contract data processors to process personal data.

DATA PROTECTION AUTHORITY

The Spanish Data Protection Authority (*Agencia Española de Protección de Datos*, or AEPD) is charged with enforcing the LOPD.¹⁰ In 2000, the country's data protection laws and the AEPD's authority to enforce those laws were challenged and the Constitutional Tribunal of Spain issued three judgments clarifying the issues at stake.¹¹ The first was a constitutional challenge against the 1992 law, for breach of the provisions of the country's constitution relating to distribution of power between the State and other agencies (in this case the AEPD). The court rejected this challenge. The second concerned another constitutional challenge which was originally brought against the 1992 law but which carried over to the 1999 law. This judgment upheld the constitutionality of the law generally, although the court struck down certain provisions allowing government agencies to transfer personal information about Spanish citizens without their permission. The court ruled that these provisions infringed on the privacy rights guaranteed to citizens by Title 18 of the Spanish Constitution.¹² The third case concerned an employer's processing of an employee's health data. The court ruled that the applicant's constitutional privacy rights were breached when the employer noted the employee's medical diagnosis on his sick leave records.

As part of their enforcement of the country's data protection laws, the AEPD maintains a registry of information databases in Spain and can investigate violations of the LOPD. As

⁸ Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, BOE Núm. 89, 13 abril 2007 (Organic Law 4/2007 of 12 April 2007 that amends Organic Law 6/2001 about Universities of 21 December 2001), BOE No. 89, 13 April 2007.

⁹ Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (Law 30/2007 about Public Contracts, 30 October 2007), BOE núm., 31 octubre 2007, available at <http://www.cert.fnmt.es/legsoporte/Ley%2030-2007.pdf>.

¹⁰ See Spanish Data Protection Authority <https://www.agpd.es/index.php?idSeccion=8>; see also <https://www.agpd.es> (in Spanish).

¹¹ Judgments Nos. 290/2000 <http://www.tribunalconstitucional.es/jurisprudencia/Stc2000/STC2000-290.html>, 292/2000 <http://www.tribunalconstitucional.es/jurisprudencia/Stc2000/STC2000-292.html>, and 202/1999 http://www.boe.es/g/es/bases_datos_tc/doc.php?coleccion=tc&id=SENTENCIA-1999-0202.

¹² Judgment No. 292/2000, *supra*.

of December 2007,¹³ there were 1,017,266 registered information databases, of which 61,553 were held by private entities, and 955,713 were held by public entities, compared to 815,093 databases registered as of December 2006, of which 56,138 were held by private entities and 758,955 were held by public entities.¹⁴

In 2007 the number of queries to the Citizen Services of the AEPD followed a growth trend that has resulted in an increase of 30 percent (for a total of 47,741 consultations). Access to the AEPD website has increased from 1,518,714 in 2006 to 2,230,120 hits in 2007.¹⁵

During 2007¹⁶ AEDP staff grew to 103, from 99 in 2006.¹⁷ In 2007, 849 defence of citizens' rights procedures (*procedimientos de tutela de derechos*) were defended,¹⁸ compared to 556 in 2006 and 579 in 2005.¹⁹ Also in 2007, there were 879 defence of citizen's rights procedures, 617 regarding the right to access one's personal data, 545 on the right of cancellation, 26 on the right to modify one's personal data and 32 regarding the right of opposition. There were 849 resolutions, of which 617 were admitted and 155 dismissed.²⁰ The AEPD has issued 396 penalties in 2007, compared to 326 in 2006.²¹

Between 2008 and 2010, the AEPD published various guides about how to implement the LOPD: a "Data Protection Guide for Database Owners" that includes tools and rules to administer databases in compliance with the LOPD;²² a "Guide on Data Security";²³ a

¹³ In 2005, 387 penalisation proceedings were started, compared with 148 in 2002. Preliminary investigations increased 60%, from 723 in 2002 to 1158 in 2005. Proceedings against public authorities increased threefold, from 13 in 2002 to 52 in 2005. AEDP, 2005 Annual Report, Summary 18, available at http://www.agpd.es/upload/English_Resources/RESUMEN%20MEMORIA_2005.pdf.

¹⁴ AEPD, 2007 Annual Report, available at https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2007/common/pdfs/memoria_AEPD_2007.pdf.

¹⁵ *Id.* at 57.

¹⁶ During 2005 AEDP staff grew from 89 to 98. AEDP, 2005 Annual Report, Summary 18, *supra* at 2.

¹⁷ AEPD, 2007 Annual Report, *supra*.

¹⁸ AEDP, 2007 Annual Report, *supra* at 49.

¹⁹ Email from Esperanza Zambrano Gómez, Spanish Data Protection Agency, to Guilherme Roschke, Skadden Fellow, Electronic Privacy Information Center, 2 August 2007 (on file with EPIC).

²⁰ AEPD, 2007 Annual Report, *supra* at 49.

²¹ AEPD, 2007 Annual Report, *supra* at 41.

²² Guía de Protección de Datos para Responsables de Ficheros, available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf (only in Spanish).

²³ Guía de Seguridad de Datos, available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf (only in Spanish).

report on children's rights and parents' duty;²⁴ a guide about how to use video surveillance while complying with the LOPD for companies, associations and individuals;²⁵ and a last one, in 2009, about how to protect workers' personal data.²⁶ The AEPD also developed its website: a new web section now includes practical information about data protection on the Internet.²⁷

In November 2009, the AEPD organised the 31st International Conference of Data Protection and Privacy Commissioners. At the conclusion of this meeting, commissioners presented the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data. The purpose of the document is to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data, together with the facilitation of international flows of personal data around the world.²⁸

The AEPD's annual reports in 2008 and 2009 show that Internet, video surveillance, and lists of defaulters constitute the bulk of data protection-related complaints.

In October 2008, the AEPD's Director made an appearance before the Constitutional Commission of the Spanish Lower Chamber to report the results of the AEPD's 2007 Annual Report. In his speech, the Director said that the priority of the AEPD is the citizens, so it is necessary to raise awareness among citizens regarding the right to data protection by providing more information and supporting their complaints and appeals when they realise that their rights have been violated. He also said that the themes of interest to the AEPD are video surveillance, mobile and Internet advertising, the dissemination of images through the Internet or YouTube or, for example, search engines.²⁹ He stressed: "The conclusion is clear: public awareness in Spain is above the European average."³⁰

²⁴ Children Rights and Parent's Duty, available at https://www.agpd.es/portalwebAGPD/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf.

²⁵ Guide on Video Surveillance, available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia_en.pdf.

²⁶ Guía de la protección de datos en las Relaciones Laborales, available at https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_relaciones_laborales.pdf.

²⁷ AEPD Web portal https://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2010/index-ides-idphp.php.

²⁸ Propuesta Conjunta de Estándares Internacionales de Protección de Datos y Privacidad, available at https://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/index-ides-idphp.php.

²⁹ Appearance before the Constitutional Commission of the Low Chamber of the Director of the AEPD to report on the 2007 Annual Report of the AEPD, 1 October 2008, available at https://www.agpd.es/portalweb/canaldocumentacion/comparecencias/common/pdfs/comparecencia_2008.pdf.

³⁰ *Id.* at 3.

In April 2008, the AEPD organised a public briefing to discuss the new developments incorporated into the LOPD. The meeting gathered more than 2,000 people from the public and private sectors.³¹

The AEPD's 2007 Annual Report includes a section with recommendations that came out of the experience the authority gained, that are particularly relevant to the general public. At the legal level, it affirmed the need to regulate the anonymous online or offline publication of court decisions and regulations of internal reporting systems, managed by workers within a company, in order to ensure the complainant's confidentiality and the rights of the accused. It also stressed the need for a "Plan for the Promotion of Good Practices" as a guarantee of privacy.

The AEPD also noted in its 2007 Annual Report that in the case of peer-to-peer (P2P) litigation, where the legal subjects of privacy and copyright merge, only a law could define which personal data can be used and for which purposes, as well as define the right balance between data protection and intellectual property.³² In that regard, the AEPD recommended an initiative to promote special precautions to avoid the unwanted exchange of sensitive personal data on the Internet via P2P networks.³³

(See more details under the "E-commerce" section.)

In January 2005, the AEPD decided that in the interest of transparency and to promote public knowledge of its decisions, it would publish all of its resolutions on its website within a month from the day after the persons concerned had been informed of a decision.³⁴ The only exception would be with regard to the registration of databases in its record of authorised information databases.

Two issues on which the AEPD has been particularly active in 2004 and 2005 is the fight against "spam", and the encouragement of small- and medium-sized businesses (*pequeñas y medianas empresas, or PYMES*) to register their databases in the General Register of Personal Data (*Registro General de Protección de Datos, or RGPD*). Although registry of information databases is compulsory, only 10 percent of PYMES that are active in the Spanish territory are complying with the law.³⁵ With regard to "spam", the AEPD announced the signing of a Memorandum of Understanding on 23 February 2005 with the US Federal Trade Commission. This memorandum is aimed at

³¹ I Sesión Anual Abierta de la AEPD, 22 April 2008, available at https://212.170.242.196/portalweb/jornadas/1_sesion_abierta/index-ides-idphp.php.

³² AEPD, 2007 Annual Report, available at https://www.agpd.es/portalweb/canaldocumentacion/memorias/memorias_2007/common/pdfs/memoria_AEPD_2007.pdf.

³³ *Id.*

³⁴ Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre la publicación de sus resoluciones https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatul/Instruccion1-2004.pdf.

³⁵ "Solo El 10% de Las PYMES Españolas Cumple La Ley de Protección de Datos", *Atlántico*, 13 April 2005.

establishing administrative cooperation between Spain and the United States in order to combat the problem of "spam". The AEPD also announced that almost a hundred investigations had been launched in relation to this phenomenon, and these investigations had given rise to 14 legal actions for breaches of data protection rules, of which six have been resolved. Of these six resolved cases, two were classified as "serious breaches", two as "minor breaches", and in the remaining two, proceedings were discontinued.³⁶ In general, however, fines of up to €30,000 are applicable for breaches of anti-spam regulations.

In the 2004 opinion on "The Qualification of the IP Address as Personal Data,"³⁷ the AEPD ruled that IP addresses can be considered "personal data" and therefore, that every data controller that processes such information has to comply with the LOPD requirements. Failure to comply may subject the violator to fines of up to €300,000.³⁸

MAJOR PRIVACY & DATA PROTECTION CASE LAW

On 16 August 2010, a judge started to investigate the complaint of an Internet users association (APEDANICA) according to which Google illegally captured and stored from 2008 data from users connected to WiFi networks when it collected photos for its Street View service.³⁹ According to the AEPD, the facts might constitute a violation of the Organic Law of Protection of Information.⁴⁰

(See more details under the "Location privacy" section.)

An important case the Supreme Court decided in 2008 is the one where the defendant, the "Association against Torture" (*Asociación Contra la Tortura*), had published on the Internet a list of the names and surnames of people being investigated for torture. In a 26 June 2008 decision, the Court confirmed the AEPD's resolution that had considered that the association had published personal data on the Internet without the data subject's

³⁶ AEPD, press statement, 23 February 2005, available at <https://www.agpd.es/upload/Prensa/Nota%20eeuu.pdf>.

³⁷ Agencia Española de Protección de Datos, "Carácter de Dato Personal de La Dirección IP," (Informe 327/03), available at <https://www.agpd.es/index.php?idSeccion=390> (in Spanish).

³⁸ Marta Escudero & Javier Maestre, "Como Consecuencia, Muchos Webmasters Deberán Registrar Sus Ficheros en la Agencia," 5 July 2004, available at http://www.kriptopolis.com/more.php?id=201_0_1_0_M.

³⁹ AFP, "Spanish Judge Probes Complaint over Google's Street View," 16 August 2010 <http://www.google.com/hostednews/afp/article/ALeqM5j2pPKEWPkNBcWqrYYj-BUIHA3Ntg.%C2%A0>. See also "Spanish DPA Opens Infringement Procedures for Google Streetview", EDRI-gram - Number 8.20, 20 October 2010 <http://www.edri.org/edrigram/number8.20/spanish-dpa-streetview-infringement>; "Google Street View Faces Citizens' Reservation in EU", EDRI-gram - Number 8.16, 25 August 2010, <http://www.edri.org/edrigram/number8.16/google-streetview-rejected-germany-france-spain>; Fiona Govan, "Spain Takes on Google over Privacy Violations in Street View", *Daily Telegraph*, 17 August 2010 <http://www.telegraph.co.uk/technology/google/7950503/Spain-takes-on-Google-over-privacy-violations-in-Street-View.html>.

⁴⁰ AEPD, "La AEPD Abre Una Investigación a Google por La Captación de Datos de Redes WIFI en España", available in Spanish at https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/mayo/100519_NP_GOOGLE_WIFI_WEB.pdf.

consent, and had fined it. The Supreme Court considered that freedom of speech was not a defence.⁴¹

On 28 January 2008, the Court of Justice decided that the "copyright directives do not require the disclosure of personal data in civil proceedings, and that Member States' competent authorities should take measures to ensure the balance between copyright and intellectual property, on the one hand, and privacy and personal data protection, on the other."⁴² (*See more details under the "E-commerce" section.*)

The Supreme Court does not support the cancellation of one's personal data in baptismal records: it revoked the Decision of the *Audiencia Nacional* of 10 October 2007 that had endorsed the view held by the AEPD since 2004. The AEPD had ruled that baptismal records are files that contain personal data; therefore data protection principles, such as the principle of data quality and accuracy should apply to them.⁴³

In 2007, the Supreme Court decided two cases about privacy in the workplace, one involving an employer's use of his employees' fingerprints to control their activities at work, the second dealing with an employer's use of email and Internet monitoring tools in the workplace.

(*See more details under the "Major privacy and Data Protection Case Law" section.*)

In December 2004, 12 persons from different social movements in the region of Catalonia filed a complaint with the AEPD as a result of the alleged inclusion of their personal data and photographs in an illegal database of a "political" nature held by the National Police Force's Provincial Information Brigade (*Brigada Provincial de Información*). The plaintiffs had no criminal records, but were part of a group of 30 people whose photographs had been shown to three persons accused of throwing Molotov cocktails at the police station of Sants (a neighbourhood in Barcelona) during their interrogation on 3rd October 2004. This procedure would have been legal if the people whose photographs were shown had had criminal records. A further concern is that the photographs that were shown were not from their national ID cards (DNI), but had been taken during their participation in public activities. The plaintiffs claimed that Article 7.4 of the 1999 LOPD was contravened, as it forbids "databases created with the exclusive scope of storing personal data that reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin, or sexual preferences." The police denied holding a database to identify people related to social movements, and stated that it only maintains

⁴¹ AEPD, "Desestima el Recurso de Casación Interpuesto por la Asociación Contra la Tortura. El TS Confirma el Criterio de la AEPD al Sancionar y Cancelar La Difusión de Datos de Funcionarios en la Web de la Asociación contra la Tortura", available at https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2008/notas_prensa/common/julio/NP_180708_tribunal_supremo.pdf.

⁴² *Id.*

⁴³ AEPD, "El Tribunal Supremo no Admite La Cancelación de Datos en Libros de Bautismo." [The Supreme Court Does not Support The Cancellation of Data in Baptism], available at https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2008/notas_prensa/common/sept/np_080930_sentencia_TS.pdf.

a database of citizens with judicial precedents, although it also admitted using a database for investigations, which operates under the control of the Data Protection Authority.⁴⁴

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Under the criminal code, interception of electronic communications requires a court order.⁴⁵ There have been several scandals in Spain over illegal wiretapping by the intelligence services. In 1995, Deputy Prime Minister Narcis Serra, Defence Minister Julian Garcia Vargas, and military intelligence chief Gen. Emilio Alonso Manglano were forced to quit following revelations that they had monitored the conversations of hundreds of people, including King Juan Carlos.⁴⁶ More recently, Juan Alberto Perote, the former head of operations of the *Centro Superior de Información de la Defensa* (CESID, the Spanish secret service, which was part of the armed forces until it was replaced by the CNI in 2002), was found guilty on 12 April 2005, and sentenced to four months in prison. In the first trial in 1999, Manglano and Perote both received six-month sentences and five CESID officers were sentenced to six months, although the Constitutional Tribunal annulled this ruling on 29 March 2004 after it deemed that the judge who heard the case was not impartial. Charges brought against Emilio Alonso Manglano and the five CESID officers by private individuals and groups placed under surveillance were dropped. Perote criticised the decision against him, claiming that his director, Manglano, and members of the Socialist Party government of the time knew about "this activity," which was carried out between 1983 and 1991.⁴⁷

An exclusionary rule applies to evidence collected by means of illegal wiretaps or bugs, and in November 2000, the Barcelona High Court (*Audiencia de Barcelona*) threw out a case because the evidence was so tainted.⁴⁸ In May 2001, prosecutors asked for 12-year sentences for each of two detectives accused of placing illegal wiretaps.⁴⁹ In December

⁴⁴ "12 Activistas de Barcelona Denuncian que La Policía Les Incluye en Un Fichero Ilegal", *El País*, 30 December 2004.

⁴⁵ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=1995/25444, Penal Code, Sections 197-199.

⁴⁶ "Spain Socialists Seek Opposition Apology on Bugging," Reuters, 6 February 1996.

⁴⁷ "Perote, Condenado a Cuatro Meses de Arresto por Las Escuchas del Cesid," *El País*, 13 April 2005; and "Cuatro Meses de Prisión para Perote por las Escuchas del Cesid," *El País*, 4 April 2005.

⁴⁸ "Secreto Comunicaciones Audiencia Invalida Pruebas Obtenidas por "Pinchazo" Teléfono," Spanish Newswire Services, 23 November 2000.

⁴⁹ "Pinchazos Telefónicos: Fiscalía Pide 24 Años Para Detectives por Pinchar Teléfonos," Spanish Newswire Service, 7 May 2001.

2004, the Supreme Court claimed that "the approval of an adequate regulation for telephone interceptions" cannot be postponed, after acquitting two suspected drug traffickers because telephone interceptions used to sentence them in the *Audiencia Nacional* were deemed to be irregular. The Court added that Spain has already been condemned by the European Court of Human Rights for failing to specify the nature of offences that can give rise to these interceptions and to fix a time limit for them.⁵⁰

The 2003 General Telecommunications Act (LGT) guaranteed the right of individuals to use strong cryptography but also contained a provision – Article 36 –allowing for a key recovery system.⁵¹ Previous versions of this provision were strongly opposed by civil liberties advocates.⁵² The new Article 36 does not change much from the former Article 52 that compelled the notification of the algorithms used, but still remains ambiguous with regard to any reference to the creation of a key escrow system.⁵³

In early 2004, the National Police Corps (*Cuerpo Nacional de Policía*) and the Civil Guard (*Guardia Civil*) reportedly started using a new software program, SINTEL, that still enables them to directly tap into telephonic communications without the need to get prior court authorisation. SINTEL, which was designed in an October 2001 secret agreement, works in real time. In addition to recording the content of the communication, the software also provides the identity of both callers and the places from which they are calling.⁵⁴

SINTEL has generated a controversial debate about the necessity of some of the tools used to fight against crime in Spain while defending citizens' fundamental rights. The Spanish Internet Users Association (*Asociación de Internautas*) filed a motion⁵⁵ before the court of the National Audience (*Audiencia Nacional*)⁵⁶ in order to assess whether the

⁵⁰ "El Supremo Cree Inaplazable Regular El Control de Teléfonos," *El País*, 13 December 2004.

⁵¹ Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones., http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2003/20253, partial English translation at https://www.agpd.es/upload/Ley_32-2003_LGT.pdf.

⁵² See Global Internet Liberty Campaign, "New Spanish Telecommunications Law Opens a Door to Mandatory Key Recovery Systems," July 1998, available at <http://www.gilc.org/crypto/spain/gilc-crypto-spain-798.html>.

⁵³ See "No al Artículo 36 Restricciones a La Criptografía: La Nueva Ley General de Telecomunicaciones Impone la Obligación de Revelar Las Claves de Cifrado," March 2003, available at <http://www.spain.cpsr.org/02042003.php>; Mercé Molist, "El Congreso no Aclara El Depósito del Cifrado en La Ley de Telecomunicaciones," *El País*, 12 June 2003.

⁵⁴ Policía y Guardia Civil Pueden Pinchar Los Teléfonos Informáticamente," 19 February 2004, available at http://www.nodo50.org/tortuga/article.php3?id_article=204.

⁵⁵ Internet Users Association motion available at http://www.internautas.org/archivos/pdf/STS_intercepcion_comunicaciones.pdf.

⁵⁶ Audiencia Nacional, homepage <http://www.audiencianacional.es/>.

police may get access to the SINTEL database of personal data without any judge's consent and without sufficient evidence of wrongdoing. The motion was rejected.⁵⁷

At the beginning of 2010, the Supreme Court decided that police can access certain data (telephone numbers, names and surnames) from the mobile agenda of arrested people without a judicial order, but not the content of calls, since they are protected by the constitutional right to secrecy of communications.

National security legislation

The terrorist attack on a Madrid commuter line on 11 March 2004 was followed by announcements of a raft of measures to be introduced with regard to the problem of Islamist terrorism; most notably measures concerning the placement of "radical" imams and former *mujahedins* (Muslims who fought in Afghanistan or the Balkans) under surveillance, and of establishing databases in order to establish their numbers.⁵⁸

The draft National Defence Law,⁵⁹ published on 31 March 2005, seeks to expand the scope of activities of the National Intelligence Centre (*Centro Nacional de Inteligencia*, or CNI),⁶⁰ by directing it to "contribute . . . in obtaining, evaluating and interpreting the necessary information to prevent and avoid any risk or threat that affects the independence and integrity of Spain, national interests and the stability of the State of law and its institutions" (Article 26). The Law was finalised on 17 November 2005.⁶¹ The words "risk or threat" alter the wording of the decree that established the CNI, which considered its scope as preventing and avoiding "danger, threat or aggression against," which cannot be interpreted as widely. Experts cited in *El País* newspaper suggested that "risk that affects the integrity of Spain" is so ambiguous as to be liable to be interpreted as giving the intelligence service a role in countering political proposals such as the so-called *Plan Ibarretxe*, proposed by the *lehendakari* (head of the Basque government) to change the status of the Basque autonomous region.⁶²

⁵⁷ Tribunal Supremo, Sala de lo penal, Sentencia N° 1078/2009, available at <http://www.audiencianacional.es/>.

⁵⁸ "Censo de Ex Muyahidines e Imanes Radicales", *El País*, 30 May 2004.

⁵⁹ Proyecto de Ley Orgánica de la Defensa Nacional 121/000031, Boletín Oficial de las Cortes Generales, 31 March 2005.

⁶⁰ Spain's secret service agency.

⁶¹ Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional, available at http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2005/18933.

⁶² "El Borrador Permite al Servicio Secreto Investigar Cualquier Riesgo que Afecte a La Integridad de España," *El País*, 18 March 2005.

Data retention

In 2007, the Parliament passed the Data Retention Law (Law No. 25/2007 Law of 18 October 2007),⁶³ that implements the EU Data Retention Directive (2006/24/EC).⁶⁴ It provides that the retention period is 12 months and bans the anonymity of prepaid card mobile phone users.

When the Parliament was preparing to implement that Directive, Internet and civil liberties organisations posed a strong reaction to it and all of them fully endorsed the European-wide campaign "Data Retention is no Solution".⁶⁵

National databases for law enforcement and security purposes

As a result of the terrorist attacks of 2001 in the United States and of 2004 in Madrid, two new laws were enacted to fight against terrorism. These two laws are written to complement each other and directly impact the field of data protection by creating new databases in public ownership.

The first law aims at preventing and freezing terrorism funding.⁶⁶ It sets up the Commission for Monitoring the Funding of Terrorist Activities. This institution has the authority to freeze funds, bank accounts, and other financial assets belonging to entities or persons linked to terrorist activities. It develops its findings within the administrative sphere and collaborates with the judiciary to transmit its conclusions to the judge in criminal trials. The law establishes the obligations of financial entities (e.g., banks, credit entities, exchange bureaus) and all subjects referred to in the law against money laundering (Law 19/2003, described below) to collaborate in providing all the information required (including personal data) in relation to frozen funds. This law also provides that, with regard to the provisions of the LOPD, the files created by the Monitoring Commission will be considered files in public ownership, and therefore exempt with regard to the rights of access, rectification, and cancellation. However, this law was recently modified by Law 10/2010 of 28 April 2010 on the prevention of money

⁶³ Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones (Law 25/2007 on the Retention of Data Related to Electronic Communications and Public Communications Networks, 18 October 2007), BOE núm. 251, 19 octubre 2007 (BOE No. 251, 19 October 2007), available at http://noticias.juridicas.com/base_datos/Admin/125-2007.html.

⁶⁴ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:01:EN:HTML>.

⁶⁵ "Data Retention is no Solution," <http://www.dataretentionisnosolution.com>. See also CPSR-ES, "¿Cómo Te Afecta La Retención de Datos?", 27 September 2005 http://wiki.dataretentionisnosolution.com/index.php/Texto_cpsr_es.

⁶⁶ Ley 12/2003, de 21 de mayo, de Prevención y Bloqueo de la Financiación del Terrorismo, (Law 12/2003 of 21st May 2003 on Preventing and Freezing Terrorism Funding), available at http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2003/10289; see also <http://www.igsap.map.es/cia/dispo/26927.htm>.

laundering and funding of terrorism.⁶⁷ One of its provisions allows the creation of a database of persons with public responsibility, including their relatives' name and surnames, and its purpose is to prevent money laundering and the funding of terrorism. The law implements Directives 2005/60/EC and 2006/70/EC.

The second regulation is Law 19/2003 regulating the movement of money and international transactions, enacted in July 2003.⁶⁸ This law works to prevent money laundering and is closely linked with the law regarding the funding of terrorist activities. It was approved as a modification to the law of 1993 preventing money laundering. The new rule also incorporates Directive 2001/97 on the prevention of money laundering into national legislation.⁶⁹

This law applies not only to terrorist crimes, illegal drug trafficking, and organised crime (current situation) but also to all other serious crimes (punishable with more than three years in prison) and related money-laundering activities. The law also imposes new obligations on subjects, such as auditors, external accountants (not only internal company accountants), and tax advisors. Notaries, lawyers, and attorneys must also collaborate with full respect to professional secrecy and without prejudice to the constitutional right to defence.

Organic Law 10/2007 of 8 October 2007 regulates the police's DNA database the controller of which is the Department of Interior. In this database are included DNA records obtained from criminal investigations (without data subject's consent) and from the identification of corpses. This law establishes that the DNA record will be deleted when the crime falls within the limitation period. If the data subject is guilty, deletion will occur according to the law of criminal records; but if she is not guilty, her DNA will be deleted.

National and international data disclosure agreements

There is nothing to report under this section.

Cybercrime

On 3rd June 2010, Spain ratified the Council of Europe's Convention of Cybercrime.

Critical infrastructure

There is nothing to report under this section.

⁶⁷ Ley 10/2010, de 28 de abril de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, available at http://noticias.juridicas.com/base_datos/Admin/l10-2010.html.

⁶⁸ Ley 19/2003, de 4 julio, sobre Régimen Jurídico de los Movimientos de Capitales y de las Transacciones Económicas con el Exterior y sobre Determinadas Medidas de Prevención del Blanqueo de Capitales, available at http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2003/13471.

⁶⁹ Directiva 2001/97/CE del Parlamento Europeo y del Consejo, de 4 de diciembre de 2001 sobre Blanqueo de Capitales: Prevención de la Utilización del Sistema Financiero (European Parliament and Council Directive 2001/97/EC of 4 December 2001 related to Money Laundering: Preventing Use of the Financial System), available at <http://europa.eu.int/scadplus/leg/es/lvb/l24016.htm>.

INTERNET & CONSUMER PRIVACY

E-commerce

The AEPD noted in its 2007 Annual Report that in the case of peer-to-peer (P2P) litigation, where the legal subjects of privacy and copyright merge, only a law could define which personal data can be used and for which purposes, as well as define the right balance between data protection and intellectual property.⁷⁰ The Director of the AEPD referred to the Court of Justice's decision of 28 January 2008, according to which the "copyright directives do not require the disclosure of personal data in civil proceedings, and that Member States' competent authorities should take measures to ensure the balance between copyright and intellectual property, on the one hand, and privacy and personal data protection, on the other."⁷¹

At the administrative level, the Spanish Data Protection Authority recommended an initiative to promote special precautions to avoid the unwanted exchange of sensitive personal data on the Internet via peer-to-peer (P2P) file-sharing networks. The AEPD stressed that users should be aware of the risks of disseminating information stored on their computers, as well as avoiding inadvertent sharing on the Internet of any folders in which files with personal data have been stored.⁷²

Cybersecurity

There is nothing to report under this section.

Online behavioural marketing and search engine privacy

On 1st December 2007, the AEPD issued a recommendation about Internet search engines. The document recommends that the information included in search engine privacy policies on the use of users' personal data is not clear enough, and probably not understandable for the general community of Internet users. It also notes that it is necessary to limit the use and storage of personal data. Once the information is no longer necessary for the purposes of the service, it must be deleted. Search engine services are under the obligation of allowing data subjects to exercise the rights of removal and opposition where their personal data are listed on other websites. It also called attention to the need to establish international standards to define and agree upon rules for guaranteeing privacy on the Internet.⁷³

The AEPD has received a lot of complaints from people exercising their right as data subjects to cancel the publication of their personal data in the official gazettes. The Data

⁷⁰ AEPD, 2007 Annual Report, available here.

⁷¹ *Id.*

⁷² *Id.*

⁷³ Spanish Data Protection Agency, "Declaración de la AEPD sobre Buscadores de Internet (2007)" [Statement on Internet Search Engines], 1st December 2007, available at https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores_en.pdf.

Protection Authority of Madrid (*Agencia de Protección de Datos de la Comunidad de Madrid*, or APDCM) made a Recommendation (2/2008) about the publication of personal data in official gazettes⁷⁴ and on the websites of public institutions of the Region of Madrid.⁷⁵ The issue arose after it was shown that people's names and identifying information can be easily found in the official gazettes by the simple use of an online search engine. The Recommendation mandates public institutions of the Region of Madrid, whenever they publish administrative acts in official gazettes or on their websites (such as fines, subventions, etc.) to apply the quality principle. For example, in the case of subventions, the quality principle dictates only to publish the total score of subventions, not their partial one. Official gazettes also have implemented that principle in a way that prevents the names of people published in them from being indexed by online search engines. As an answer, the City Council of Madrid issued an Instruction⁷⁶ regarding the publication of personal data in its Official Gazette, while the Data Protection Authority of Catalonia (*Autoridad Catalana de Protecció de Dades/Autoritat Catalana de Protecció de Dades*⁷⁷) published a recommendation regarding the publication on personal data on the Internet.⁷⁸

Online social networks and virtual communities

The claims before the AEPD grew by 45 percent in 2008, with a particular worry by citizens for the Internet and online social networks.⁷⁹

The AEPD has worked with Tuenti (the Spanish social network for young people with more than 8 million users) and Facebook in order to implement a system of user verification (parental consent) for children under 14 years of age.

⁷⁴ Official Gazettes are journals published everyday by which public bodies publish their administrative acts and resolutions. [Note of the editor.]

⁷⁵ This concerns the administrations of the Region of Madrid, city councils, professional associations and public universities.

⁷⁶ BOAM nº 6341, 3rd January 2011, available at <http://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Boletin-Oficial-del-Ayuntamiento/Buscador-Boletines/1-Instruccion-Medidas-Agencia-Protec.-Datos-Cdad.-de-Madrid?vgnextfint=default&vgnextoid=4442a3045ef2d210VgnVCM2000000c205a0aRCRD&vgnextchannel=7a698db0ae967010VgnVCM1000009b25680aRCRD>.

⁷⁷ Autoritat Catalana de Protecció de Dades, homepage <http://www.apd.cat>.

⁷⁸ Recomendación 1/2008 de la Agencia Catalana de Protección de Datos sobre la Difusión de Información que Contenga Datos de Carácter Personal a través de Internet, April 2008, available at <http://www.apdcat.net/media/687.pdf>.

⁷⁹ EFE, "Las Reclamaciones ante Protección de Datos Crecieron un 45% en 2008. Los Españoles Presentan Una 'Preocupación Extraordinaria' ante El Auge de Las Redes Sociales en Internet", El País.com, 15 April 2009, available at http://www.elpais.com/articulo/sociedad/reclamaciones/Proteccion/Datos/crecieron/45/2008/elpepusoc/20090415elpepusoc_4/Tes.

Online youth safety

The Law 34/2002 of 11 July 2002 on Information Society and E-commerce was modified by Law 56/2007 of 28 December 2007 on Measures to Promote E-commerce.⁸⁰

The LOPD prohibits the collection of personal data from minors under 14 years of age without their parents' or tutors' consent. As many profiles on social networking websites belong to minors under 14, several initiatives have been launched in the last two years in Spain to improve how those websites protect and control minors' activities. Greater involvement by national education authorities and parents has also been demanded.

On 9 February 2010 the Safe Internet International Day was celebrated (*Día Internacional de Internet Seguro*), promoted by the European Commission and organised in the European union by INS@FE, the European network of awareness centres "promoting safe, responsible use of the Internet and mobile devices to young people",⁸¹ and in Spain, by the association "Protégeles" (Protect Them).

The AEPD has also organised several activities aimed at raising awareness of privacy among minors with guidelines and a special area in its website.⁸²

In 2009 and 2010, the Madrid Data Protection Authority (APDCM) launched a project addressed to minors with presentations about privacy risks on the Internet that it delivered in all 404 secondary schools of the Region of Madrid with the help of school teachers, directors and tutors, 60 privacy experts (magistrates, lawyers and consultants). The APDCM gave students a manual on Internet privacy⁸³ produced by the Commission on Liberties and Information Technology (*Comisión de Libertades Informáticas*, or CLI).⁸⁴ Other data protection authorities (from Catalonia and the Basque Country) have also elaborated materials addressed specifically to minors.⁸⁵

⁸⁰ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (Law 34/2002 of 11 July 2002 about Information Society Services and Electronic Commerce), available at http://noticias.juridicas.com/base_datos/Admin/l34-2002.html.

⁸¹ INS@FE, homepage <http://www.saferinternet.org/>.

⁸² AEPD, Internet y Datos Personales http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2010/index-ides-idphp.php; <http://www.agpd.es/portalweb/canalciudadano/menores/index-ides-idphp.php>.

⁸³ Manuales prácticos del proyecto CLI-PROMETEO 2008-2009, available at http://www.madrid.org/cs/c=PAPD_Generico_FA&cid=1253706444391&language=es&pageid=1252308394307&pagename=PortalAPDCM%2FPAPD_Generico_FA%2FPAPD_fichaPublicacion&vest=1252308394307.

⁸⁴ Comisión de Libertades Informáticas, homepage <http://www.asociacioncli.es>.

⁸⁵ Autoridad Catalana de Protecció de Dats (Catalan Data Protection Authority), Privacitat para Joves http://www.apdcat.net/es/contingut.php?cont_id=305&cat_id=250; Datuak Babesteko Euskal Bulegoa - Agencia Vasca de Protección de Dats (Basque Data Protection Authority), Reda and Neto: Caring for our Personal Data <http://www.avpd.euskadi.net/s04-kontuzdt/es>; Agencia Española de Protección de Dats (Spanish Data Protection Authority), Internet y Datos Personales https://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2010/index-ides-idphp.php.

The non-profit association CLI developed the "CLI-PROMETEO" Project aimed at promoting the use of information technologies among minors and teenagers, together with the protection of personal data. The project has been subsidised by the Department of Industry, Tourism and Trade and supported by diverse institutions, among them the Spanish AEPD.

TERRITORIAL PRIVACY

Video surveillance

Organic Law 4/1997⁸⁶ regulates the use of surveillance by police and to control traffic, while Law 19/2007 against Racism and Xenophobia in Sports⁸⁷ regulates its use at sports events. The Law about the Private Security of 1992⁸⁸ and the Royal Decree of Private Security⁸⁹ regulate their use by security companies and in banks.

In December 2006, the AEPD published a new regulation on video surveillance.⁹⁰ Images obtained from cameras located in public places are to be considered personal data, and the files containing both images and data derived from them are to be protected. Cameras will only be used when other, proportionate means of surveillance are not easily available. A distinctive label must be placed in a visible place, and the derived data will be erased after one month. This regulation includes recording, transmission, conservation and storage, including real-time reproduction and broadcasting. Personal recording for home use, and image use by law enforcement agencies are exempted.

⁸⁶ Ley Orgánica 4/1997, de 4 de agosto, por la que se Regula la Utilización de Videocámaras por las Fuerzas y Cuerpos de Seguridad en Lugares Públicos (Law 4/1997 of 4 August 1997 that Regulates the Use of Video Surveillance by Security Forces and Authorities in Public Places), available at http://noticias.juridicas.com/base_datos/Admin/lo4-1997.html.

⁸⁷ Ley 19/2007, de 11 de julio, contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte (Law 19/2007 of 11 July 2007 against Violence, Racism, Xenophobia, and Intolerance in Sports), available at http://noticias.juridicas.com/base_datos/Admin/l19-2007.html.

⁸⁸ Ley 23/1992, de 30 de julio, de Seguridad Privada (Law 23/1992 of 30 July 1992 about Private Security), available at http://noticias.juridicas.com/base_datos/Admin/l23-1992.html.

⁸⁹ Real Decreto-ley 2/1999, de 29 de enero, por el que se modifica la Ley 23/1992, de 30 de julio, de Seguridad Privada (Royal Decree 2/1999 of 29 January 1999), available at http://noticias.juridicas.com/base_datos/Admin/rdl2-1999.html.

⁹⁰ Agencia Española de Protección De Datos, Instrucción 1/2006, de 8 de noviembre sobre el Tratamiento de Datos Personales con Fines de Vigilancia a través de Sistemas de Cámaras o Videocámaras, 12 December 2006, available in Spanish at http://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Instruccion_1_2006_videovigilancia.pdf, available in English at https://www.agpd.es/upload/English_Resources/Instruccion%20videovigilancia%20EN.pdf.

The APDCM published Instruction 1/2007⁹¹ about the use of video surveillance for security purposes, to control restricted areas or traffic, and for other health-related, investigative, or scientific purposes. The data controller has to justify that video surveillance is necessary and report about it to the APDCM in order to assess its proportionality. The data protection authority of Catalonia also elaborated an Instruction about video surveillance in 2009 that mandates the data controller to report its video surveillance system to the authority.⁹²

Location privacy (GPS, mobile phones, location based services, etc.)

Google's Street View service started capturing information from 2008 from individuals connected through their WiFi wireless networks. According to the AEPD, the facts might constitute a violation of the Organic Law of Protection of Information.⁹³ On 16 August 2010, a judge started to investigate the complaint of an Internet users association (APEDANICA) according to which Google illegally captured and stored data from users connected to WiFi networks when it collected photos for its Street View service.⁹⁴

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Since August 2006, all passports issued by Spain are electronic ones that contain an RFID tag.⁹⁵ Holding an e-passport is compulsory for citizens from countries that belong to the Visa Waiver Program (all countries belonging to the European Economic Area (EU member states, plus Norway, Iceland, and Liechtenstein), Switzerland, New Zealand, Australia, and Brunei) for travelling to the United States, and therefore all comply with the same technical specifications.⁹⁶ In 2006, the private watchdog Commission on

⁹¹ APDCM, Instrucción 1/2007 de 16 mayo 2007 sobre el Tratamiento de Datos Personales a través de los Sistemas de Cámaras o Videocámaras en el Ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid" (Instruction 1/2007 of 16 May 2007 on the Processing of Personal Data through Photo or Video Surveillance by the Public Bodies and Administrations of the Community of Madrid).

⁹² The report must include the number of cameras used, if cameras are fixed or moving, if they are placed less than 50 metres from a hospital, church, or school, and justify the proportionality of their use.

⁹³ AEPD, "La AEPD Abre Una Investigación a Google por La Captación de Datos de Redes WiFi en España", available here.

⁹⁴ AFP, "Spanish Judge Probes Complaint over Google's Street View," 16 August 2010 <http://www.google.com/hostednews/afp/article/ALeqM5j2pPKEWPkNBcWqrYYj-BU...> See also "Spanish DPA Opens Infringement Procedures for Google Streetview", EDRI-gram - Number 8.20, 20 October 2010 <http://www.edri.org/edriagram/number8.20/spanish-dpa-streetview-infringem...> "Google Street View Faces Citizens' Reservation in EU", EDRI-gram – Number 8.16, 25 August 2010, <http://www.edri.org/edriagram/number8.16/google-streetview-rejected-germa...> Fiona Govan, "Spain Takes on Google over Privacy Violations in Street View", *Daily Telegraph*, 17 August 2010 <http://www.telegraph.co.uk/technology/google/7950503/Spain-takes-on-Google-over-privacy-violations-in-Street-View.html>.

⁹⁵ Home Office (Ministerio de Interior), Información sobre Trámites / Pasaporte / Pasaporte Electrónico http://web.archive.org/web/20080614191030/http://www.mir.es/SGACAVT/pasaport/pasaporte_electronico.html.

⁹⁶ Visa Waiver Program (VWP) http://travel.state.gov/visa/temp/without/without_1990.html.

Liberties and Information Technology (*Comisión Libertades e Informática*, or CLI) and other groups expressed concerns about the adoption of RFID technologies in passports, noting that RFID-enabled passports have been hacked in some countries.⁹⁷

NATIONAL ID & SMART CARDS

On 11 December 2003, the Parliament enacted the Law on Digital Signatures.⁹⁸ The legislation established an electronic identification card (*DNI electrónico*) that includes a certificate used to generate a digital signature.⁹⁹ The card had to be fully rolled out by 2007, but it is still ongoing. It allows individuals and businesses to digitally sign documents, and provides the same value as a regular handwritten signature. The government seeks to encourage the development of electronic commerce and promote consumer confidence in Internet-based transactions.¹⁰⁰ The electronic ID card includes two elements: a chip with information relating to the citizen's identity and electronic signature, as well as biometric data (fingerprint and photograph). Privacy groups criticise the law because, as they assert, it would make the card compulsory for all and would create a huge database of citizens' personal data that would be subject to serious security risks. They have urged that the project be revised to ensure the full protection of Spanish citizens' privacy.¹⁰¹ In mid-February 2006, the Ministry of Interior announced that root keys had been generated.¹⁰² The first e-DNI was issued on 16 March 2006,¹⁰³ and after a trial testing period e-DNIs were routinely being issued.¹⁰⁴ By March 2010, the number of e-DNI issued had raised to 9 million.¹⁰⁵ However, according to the National Institute

⁹⁷ Asociación de Internautas, "La CLI Se Opone a que Se Incrusten RFID en El Futuro Pasaporte Electrónico y, Posteriormente, en El DNI Electrónico, 7 March 2006, <http://www.internautas.org/privacidad/html/3517.html>. Kriptópolis, Pasaporte hacia la Inseguridad, 19 November 2006 <http://www.kriptopolis.org/pasaporte-hacia-la-inseguridad>.

⁹⁸ Ley 59/2003, de 19 de diciembre, de Firma Electrónica http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2003/23399.

⁹⁹ See generally <http://www.dnielectronico.es>.

¹⁰⁰ "La Ley de La Firma Electrónica Entra en Vigor," *Redes and Telecoms*, 12 December 2003, available at <http://www.redestelecom.com/Actualidad/Noticias/Comunicaciones/Legislaci%C3%B3n/20031212036>.

¹⁰¹ "El DNI Electrónico Se Tramitará en España El Próximo Año," *El País*, 5 May 2003.

¹⁰² Dirección General de la Policía y de la Guardia Civil, El Ministro del Interior Pone en Marcha el Sistema de Certificación del Nuevo DNI Electrónico, 16 February 2006 http://www.dnielectronico.es/oficina_prensa/noticias/noticia04.html.

¹⁰³ Dirección General de la Policía y de la Guardia Civil, El Ministro del Interior Entrega el Primer Ejemplar del Nuevo DNI Electrónico a Una Ciudadana de Burgos, 16 March 2006 http://www.dnielectronico.es/oficina_prensa/noticias/noticia09.html.

¹⁰⁴ Dirección General de Relaciones Informativas y Sociales, "Comienza la Expedición del Nuevo DNI Electrónico en Trece Ciudades Españolas, 5 July 2006 http://www.mir.es/DGRIS/Notas_Prensa/Policia/2006/np070504.html (last checked in 2007).

¹⁰⁵ Asociación de Internautas, "El Uso del DNI Electrónico Sigue Siendo Escaso a pesar de Haber Casi 15 Millones de Documentos Nuevos Expedidos", 29 March 2010 <http://www.internautas.org/html/6078.html>.

of Statistics, as of October 2009, only 3.4 percent of people had actually used their e-DNI to digitally sign electronic transactions.¹⁰⁶

The Commission on Liberties and Information Technology (CLI) complained about the lack of debate with regards to the introduction of the planned electronic ID card,¹⁰⁷ warning that measures that are to be introduced may contravene fundamental rights, such as the rights to privacy and to the protection of personal data.¹⁰⁸ It also stressed that it will be important for adequate security measures to be adopted in relation to the introduction of this identification document, as it may contain elements that will make it possible to access sensitive personal information about cardholders, such as race and religious affiliation in the case of photographs. The CLI has warned about the possibility that DNA details be included, and that it would be illegal for the national electronic ID card to include medical information – or to turn the ID card into a multipurpose document required to access health services, as was suggested in February 2004 by the former Minister of Public Administration, Julia García Valdecasas.¹⁰⁹

Since 2009 the Spanish government has launched information campaigns about the electronic ID card, stressing its benefits for citizens.¹¹⁰ On 3 November 2009 a Royal Decree modified some of the requirements to obtain digital identification certificates for the national ID card.¹¹¹

RFID tags

In 2006, the CLI and other groups expressed concerns about the adoption of RFID technologies in passports, noting that RFID-enabled passports had been hacked in some countries.¹¹²

BODILY PRIVACY

There is nothing to report under this section.

¹⁰⁶ "Casi Diez Millones de Españoles Tienen DNI Electrónico, pero Pocos Lo Usan", *Expansión.com*, 13 April 2009, available at <http://www.expansion.com/2009/04/13/funcion-publica/1239603801.html>.

¹⁰⁷ "El DNI Electrónico no Puede Incluir Datos Personales Ajenos a La Identificación," *IBLNEWS*, 4 October 2004.

¹⁰⁸ "La CLI Advierte que el Contenido del DNI Electrónico no Puede Incluir Datos de Carácter Personal," *Asociación de Internautas*, 20 May 2005, available at <http://www.internautas.org/html/1/2934.html>.

¹⁰⁹ Comisión de Libertades e Informática, press statement, 19 February 2004.

¹¹⁰ At <http://www.dnielectronico.es/>.

¹¹¹ Real Decreto 1586/2009, available in Spanish at http://www.dnielectronico.es/marco_legal/RD_1586_2009.html.

¹¹² Asociación de Internautas, "La CLI Se Opone a que Se Incrusten RFID en El Futuro Pasaporte Electrónico y, Posteriormente, en El DNI Electrónico," 7 March 2006, <http://www.internautas.org/privacidad/html/3517.html>. Kriptópolis, "Pasaporte hacia la Inseguridad," 19 November 2006 <http://www.kriptopolis.org/pasaporte-hacia-la-inseguridad>.

WORKPLACE PRIVACY

The Supreme Court decided in July and September 2007 two cases about privacy in the workplace. The first one tried to determine whether it is possible for an employer to use fingerprints to control employees' work schedule, which the Court considered that in that case it is. The second case dealt with an employer's use of email and Internet monitoring tools in the workplace. The Court defined Internet and email as "a tool that employers provides to employees in order to facilitate their work", and considered that employers may use monitoring tools but only upon adequate notice to his employees.

On 7 November 2005, the Constitutional Court decided that trade unions can email workers even if the workers are not trade union members, in order to inform them of their activities. However, workers can exercise the right to cancel, or object to such mailing. The employer does not have the obligation to install an email system in his company. However, if the employer installs it, it has to facilitate its use by trade union of emails so that they may inform company employees about their activities.

HEALTH & GENETIC PRIVACY

Health privacy

The CLI, after four months of work with the Ministry of Health and Consumer Protection, supports the current implementation of the "Clinical Digital History in the National Health System" Project.

Some regions in Spain have implemented the electronic medical record. The Department of Health and the Regions are working on implementing the electronic prescription.¹¹³

Law 14/2007 of 3 July 2007 about Biomedical Investigations¹¹⁴ regulates many of the issues related to genetic data like, for example, the conditions to delete genetic data for biomedical investigation purposes. Organic Law 7/2006 of 21 November 2006¹¹⁵ regulates doping: the data that must be communicated to international doping authorities.¹¹⁶ Law 29/2006 of 26 July 2006,¹¹⁷ while it regulates the rational use of

¹¹³ "La Comunidad de Madrid Pone en Marcha La Receta Electrónica", estardia.es, 19 February 2007, available here.

¹¹⁴ Ley 14/2007, de 3 de julio, de Investigación biomédica, BOE nº 159, de 4 de julio de 2007 (Law 14/2007 of 3rd July 2007 about Biomedical Investigation), available here.

¹¹⁵ Ley Orgánica 7/2006, de 21 de noviembre, de Protección de la Salud y de Lucha contra el Dopaje en el Deporte. BOE nº 279, de 22 de noviembre de 2006 (Organic Law 7/2006 of 21 November 2007 about the Protection of Health and the Fight against Doping in Sports), available at <http://www.csd.gob.es/csd/estaticos/dep-salud/LDEP10EP.pdf>.

¹¹⁶ See Articles 34 to 36.

¹¹⁷ Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios, BOE nº 178 de 27 de julio de 2006 (Law 29/2006 of 26 July 2006 about the Safeguards and Rational Use of Medicines and Medical Devices), available at <http://www.red-tercel.com/ficheros/Ley%20del%20Medicamento.%202006..pdf>.

medicines, some of its provisions deal exclusively with the protection of patients' personal data. It is not necessary to obtain the data subject's consent to process a communication of personal data that are the consequence of implementing an information system based in prescription (paper or electronic).

Genetic privacy

Law 14/2007 of 3 July 2007 about Biomedical Investigations¹¹⁸ regulates many of the issues related to genetic data like, for example, the conditions to delete genetic data for biomedical investigation purposes.

FINANCIAL PRIVACY

On 29 June 2006, the AEDP opened an investigation into the SWIFT case.¹¹⁹ SWIFT, the Society for Worldwide Interbank Financial Telecommunication, handles financial wire transfers for banks throughout the world.¹²⁰ The AEDP investigation followed a complaint from Privacy International.¹²¹ SWIFT had been covertly disclosing financial data to U.S. authorities. Privacy International complained that this disclosure fell within the scope of the Spanish Data Protection Law, and that SWIFT handled over 45 million Spanish financial messages for over 140 Spanish banks and institutions.¹²² The AEDP later joined other European data protection Agencies in approving an Article 29 Working Group Opinion on the SWIFT matter.¹²³ The opinion concluded that SWIFT and European Financial institutions had failed to respect the provisions of the EU Data Protection Directive 95/46/EC.¹²⁴

¹¹⁸ Ley 14/2007, de 3 de julio, de Investigación Biomédica, see *supra* at 113.

¹¹⁹ AEDP, La Agencia Española De Protección de Datos Investiga Las Implicaciones del "Caso SWIFT" en España, 29 June 2006 http://www.agpd.es/upload/Prensa/Nota%20%20informativa_03_07_06.pdf.

¹²⁰ See generally <http://www.swift.com/>.

¹²¹ Simon Davies, Complaint: Transfer of Personal Data from SWIFT to the US Government, 27 June 2006, <http://www.privacyinternational.org/issues/terrorism/swift/spain.pdf>.

¹²² *Id.*

¹²³ AEDP, Las Autoridades Europeas de Protección de Datos Aprueban una Opinión sobre El Caso "SWIFT", 28 November 2006 http://www.agpd.es/upload/Prensa/OPINI%D3N%20Swift_28_11_2006.pdf.

¹²⁴ Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf.

E-GOVERNMENT & PRIVACY

Law 11/2007 of 22 June 2007 about e-government services¹²⁵ regulates the possibility for citizens not to have to provide personal data or documents other than in an electronic way. The law indeed mandates that in the national, regional, and city administrations all administrative procedures be implemented as electronic services before 31 December 2009.

The Law 11/2007 was further detailed in three royal decrees: Royal Decree 1671/2009 of 6 November 2009,¹²⁶ Royal Decree 3/2010 of 8 January 2010 about the National Security Structure of Electronic Services,¹²⁷ and Royal Decree 4/2010 of 8 January 2010 about the National Interoperability Structure of Electronic Services.¹²⁸

The APDCM published Recommendation 3/2008 about the use of electronic services by public institutions of the Region of Madrid¹²⁹ (content of privacy policies, use of intranets, etc.).

OPEN GOVERNMENT

Law 37/2007 of 16 November 2007 about the Reuse of Information of Public Administrations¹³⁰ regulates the possibility to reuse public information but free of personal data.

OTHER RECENT FACTUAL DEVELOPMENTS

In May 2008, a Tele5 TV documentary revealed that many of the court records that individuals entrust to Spanish judicial authorities and that contain sensitive personal data (psychological profiles, financial, employment, medical, and criminal records) are not

¹²⁵ Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, BOE nº 150 de 23 de junio de 2007 (Law 11/2007 of 22 June 2007 about Citizens' Electronic Access to Public Services), BOE No. 150 of 23 June 2007, available here.

¹²⁶ Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, available at http://noticias.juridicas.com/base_datos/Admin/rd1671-2009.html.

¹²⁷ Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (Royal Decree 3/2010 of 8 January 2010 about the National Security Structure of Electronic Services), available at http://noticias.juridicas.com/base_datos/Admin/rd3-2010.html.

¹²⁸ Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, BOE nº 25 de 29 enero de 2010 (Royal Decree 4/2010 of 8 January 2010, BOE No. 25 of 29 January 2010), available at http://noticias.juridicas.com/base_datos/Admin/rd4-2010.html.

¹²⁹ Recomendación 3/2008, de 30 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre tratamiento de datos de carácter personal en servicios de administración electrónica (BO. Comunidad de Madrid 11 septiembre 2008, núm. 217, [pág. 4]), available here.

¹³⁰ Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público, available at http://noticias.juridicas.com/base_datos/Admin/l37-2007.html.

stored, disclosed or destroyed in compliance with the LOPD. The AEPD declared that the judicial system lacked a uniform set of security measures, and that the problem was widespread among Spanish jurisdictions. One of the problems this scandal brought to light is the impossibility for the AEPD to take any sanction against the state administration and its employees, giving it the only option to declare that there is a violation of the LOPD.¹³¹

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

There is nothing to report under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Spain ratified the Universal Declaration of Human Rights of 1948,¹³² and on 27 April 1977, ratified the International Covenant on Civil and Political Rights.¹³³ Spain is a member of the Council of Europe (CoE) and has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108).¹³⁴ It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹³⁵ In November 2001, Spain signed the CoE Convention on Cybercrime,¹³⁶ and on 3 June 2010, ratified it. It is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Spain is also member of the Iberoamerican Data Protection Network.¹³⁷

¹³¹ Mónica C. Belaza, "La Indiscreta Basura Judicial. El Hallazgo de Papeles de Juzgados en La Calle Confirma que La Ley de Protección de Datos no Se Cumple. – La Administración no Puede Ser Sancionada", ElPaís.com, 31 May 2008, available at <http://www.elpais.com/articulo/sociedad/indiscreta/basura/judicial/elpep...> Auditta, "Abren Una Investigación tras Aparecer Expedientes Judiciales en La Basura" <http://www.proteccion-datos.net/abren-una-investigaciOn-tras-aparecer-expedientes-judiciales-en-la-basura.php>.

¹³² Available at <http://www.un.org/Overview/rights.html>.

¹³³ International Covenant on Civil and Political Rights, 16 December 1966, available at <http://www2.ohchr.org/english/bodies/ratification/4.htm>.

¹³⁴ Signed 28 January 1982; ratified 31 April 1984; entered into force 1 October 1985.

¹³⁵ Signed 24 November 1977; ratified 4 October 1979; entered into force 4 October 1979.

¹³⁶ Signed 23 November 2001.

¹³⁷ Red Iberoamericana de Protección de Datos. See generally https://www.agpd.es/portalweb/internacional/red_iberoamericana/index-ides-idphp.php.

KINGDOM OF SWEDEN

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Sweden's Constitution¹ consists of four fundamental laws: the Instrument of Government, the Act of Succession, the Freedom of the Press Act, and the Fundamental Law on Freedom of Expression. These laws serve as a basis for the Swedish political decision-making and contain several provisions relevant to data protection and citizens' freedoms and rights. For example, Section 2 of the Instrument of Government Act of 1974² provides for the protection of individual privacy. Section 13 of Chapter 2 of the same instrument also states that freedom of expression and information – which are constitutionally protected pursuant to the Freedom of the Press Act of 1949³ – can be limited with respect to the "sanctity of private life." Moreover, Section 3 of the same chapter provides for a right to protection of personal integrity (privacy) in relation to automatic data processing. The same article also prohibits non-consensual registration of persons purely on the basis of their political opinions. The European Convention on Human Rights (ECHR) was incorporated into Swedish law in 1994. The ECHR is not formally part of the Swedish Constitution but has, in effect, similar status.

In April 2004, the Swedish government decided to set up a Committee (*Integritetsskyddskommitten*, Committee on the protection of privacy) composed of experts and members of the *Riksdag* (the Swedish Parliament) to analyse legislation in Sweden concerning privacy and create a survey related to this issue.⁴ In spring 2007, the Committee presented an extensive report which contained the survey and analysis.⁵

"The committee describes in relative depth how legislation in different areas of society has developed, what kind of information the government and the *Riksdag* have had on which to base their decisions and also how the balance has been struck between the interest of protecting privacy and other interests."⁶

The last report of the Committee was presented in January 2008, and in it the Committee presented an analysis of how constitutional protection of privacy should be regulated and

¹ Swedish Constitution, English version available at http://www.servat.unibe.ch/icl/sw00000_.html.

² *Regeringsformen*, SFS 1974:152, available at http://www.riksdagen.se/templates/R_Page____6307.aspx.

³ *Tryckfrihetsförordningen*, SFS 1949:105, available at http://www.riksdagen.se/templates/R_Page____6313.aspx.

⁴ 11th Annual Report of the Article 29 Data Protection Working Party (2007), 24 June 2008, at 105, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/11th_annual_report_en.pdf.

⁵ *Id.*

⁶ *Id.*

what other measures are necessary.⁷ On 2 June 2010, the Swedish parliament voted in favour of a proposition that includes some of the Committee's proposals, though less far-reaching than in the original proposal. A new clause will be added to the Government Bill 2009/10:80, "A Reformed Constitution, which proposes extensive amendments to the Constitution and gives both citizens and non-citizens protection against significant privacy intrusions that occur without consent and result in surveillance or mapping of the personal life of the individual."⁸ The amendments to the Constitution must be confirmed during the coming legislature and will come into force in 2011, with a transition period until 2015.⁹ The amendments to the constitutional framework in Sweden must be considered to be significant but the issue of a more detailed regulation, as proposed by the Committee, still remains open.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Swedish Personal Data Act (PDA) or *personuppgiftslagen* (PUL) was enacted in 1998 to bring Swedish law into conformity with the requirements of the European Union (EU) Data Protection Directive 1995/46/EC.¹⁰ The PDA essentially incorporates the EU Data Protection Directive into Swedish law. It regulates the establishment and use, in both public and private sectors, of automated data files on physical/natural persons. The Act replaced the Data Act of 1973, which was the first comprehensive national act on privacy in the world.¹¹ The 1973 Act continued to apply until October 2001 with respect to processing of personal data initiated prior to 24 October 1998. An amendment of Section 33 of the Act entered into force in January 2000 in order to align even closer to the EU Data Protection Directive standards on the transfer of personal data to third countries.

In years past both the PDA and the EU Data Protection Directive, on which it is based, were criticised for being too restrictive. On 11 May 2006, the Swedish Parliament voted to amend the PDA to make it more focused on preventing the misuse of personal data.¹² The most significant change to the PDA is to exempt processing of "unstructured

⁷ *Id.*

⁸ Constitutional Board of the Swedish Parliament, *Betänkande* 2009/10:KU19, "*Vissa frioch rättigheter m.m.*" (Report 2009/10:KU19, "Certain Rights and Liberties etc."). at <http://www.riksdagen.se/webbnav/?nid=3322&rm=2009/10&bet=KU19>. Author's translation, original reads "*skydd mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.*".

⁹ *Id*http://www.riksdagen.se/templates/R_Page_6313.aspx.

¹⁰ *Personuppgiftslagen*, SFS 1998:204, English version available at <http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/>.

¹¹ *Datalagen*, SFS 1973:289.

¹² Swedish PDA Amendments of 2007, SFS 2006:398.

materials," such as scrolling texts, sounds and images, and email from the great majority of handling provisions in the PDA. The excluded material will be regulated by a simple rule – processing of personal data is not permitted if it constitutes a violation of the registered person's personal integrity. Guidelines in the legislation mandate that the data processor cannot process data for improper purposes such as harassment or defamation, or collect large amounts of information about a person without good cause. Data processors are required to correct personal data that is wrong or misleading and to observe secrecy and non-disclosure regulations. However, the amendment also decriminalises breaches committed by mere negligence; gross negligence is now required before a breach can be prosecuted under the PDA. The amendments came into force on 1 January 2007.

The PDA provides liberal exemptions for freedom of expression. It specifically states that in case of a conflict, the existing protections for freedom of the press (Freedom of the Press Act)¹³ and freedom of speech (Freedom of Expression Act)¹⁴ will prevail. The majority of the provisions in the PDA are also exempted in regard to processing that is carried out exclusively for journalistic purposes, or artistic or literary expression. In 2001, the Swedish Supreme Court ruled that the operator of a Web site dedicated to the criticism of several Swedish banks and bank officials did not violate the PDA, as he was protected by the exemptions for journalistic purposes.¹⁵ In another case, where a church volunteer had published information about church employees on the Internet without their consent, the Göta Court of Appeal decided in 2004 that this was not a matter of processing for journalistic purposes, or artistic or literary expression.¹⁶ The Court found that, in this case, the right to privacy outweighed the freedom of expression and the processing conflicted with several provisions in the PDA. However, due to the circumstances in this case, it was not seen as a serious offence, and the church volunteer was not convicted.¹⁷

Sector-based laws

Besides the PDA, there is also specific legislation regarding processing of personal data in different, specified sectors. Some examples include the Health Care Register Act of

¹³ SFS 1949:105, available at http://www.riksdagen.se/templates/R_Page____6313.aspx

¹⁴ SFS 1991:1469 and 2002:209, available at http://www.riksdagen.se/templates/R_Page____6316.aspx.

¹⁵ Supreme Court, 12 June 2001, see Nytt Juridiskt Arkiv (NJA) 2001 at 409, available in Swedish at <http://www.rattsinfosok.dom.se/lagrummet/index.jsp>.

¹⁶ Göta Court of Appeal, case B 747-00, 7 April 2004,.

¹⁷ EC Court of Justice, case C-101/01 6 November 2003, Bodil Lindqvist, OJ C 7, 10 January 2004, at 3, linked from http://ec.europa.eu/justice/policies/privacy/law/index_en.htm

1998,¹⁸ the Police Data Act of 1998,¹⁹ the Land Register Act of 2000,²⁰ the Schengen Information System Act of 2000,²¹ and the Act on processing of personal data within Social Services of 2001.²² Other statutes with provisions relating to data protection include the Secrecy Act of 1980,²³ the Credit Information Act of 1973,²⁴ the Debt Recovery Act of 1974,²⁵ and the Administrative Procedure Act of 1986.²⁶ In sectors that fall within the scope of the EU Data Protection Directive, the specific legislation takes into account the Directive's rules.²⁷ The EU Directive 2002/58/EC on privacy and electronic communications was essentially implemented in July 2003 by the entry into force of the Electronic Communications Act (ECA).²⁸

In 2002, the Parliament adopted new rules on voluntary publishing licences.²⁹ The rules on freedom of the press and freedom of expression apply to printed publications, radio and television, films, etc., and do not – in principle – apply to the Internet.³⁰ With the new rules, anyone may apply for and obtain such a licence, and thereby extend the rules on freedom of the press and expression to their Web site. This means that the keeper of a Web site who has obtained a publishing licence will be able to process personal data without having to comply with the provisions of the PDA.³¹ Specific privacy problems have occurred in this context regarding publication of credit information and phone directories on the Internet. Following remarks from the data protection authority, a specific inquiry has been set up within the Ministry of Justice to analyse whether the new legislation conflicts with provisions that aim at protecting privacy.³² A resulting

¹⁸ SFS 1998:544.

¹⁹ SFS 1998:622.

²⁰ SFS 2000:224.

²¹ SFS 2000:344.

²² SFS 2001:454.

²³ SFS 1980:100.

²⁴ SFS 1973:1173.

²⁵ SFS 1974:182.

²⁶ SFS 1986:223.

²⁷ See for example the Health Care Register Act of 1998 and the Credit Information Act of 1973.

²⁸ SFS 2003:389.

²⁹ Chapter 1, section 9 of The Fundamental Law on Freedom of Expression, SFS 1991:1469 and 2002:209, available at http://www.riksdagen.se/templates/R_PageExtended____6317.aspx

³⁰ See Section "Comprehensive law," *supra* in this report.

³¹ The Swedish Radio and TV Authority, at <http://www.rtvv.se>.

³² Ministry of Justice (JU) No. 2003:04, see terms of reference 2003:58.

government bill resolving some of these issues was approved by the Swedish Parliament in June 2010.³³ From 1 January 2011, any processing of personal credit information will have to be based on legitimate need. Such need would, for example be a landlord controlling potential tenants' financial status. The data subject will receive a copy of the document and the chance to correct faulty information. While not uncontroversial, especially by international comparison, the bill means real improvement from the previous situation, where ubiquitous peer-to-peer information gathering was possible almost without any limitation.³⁴

DATA PROTECTION AUTHORITY

Compliance with the PDA is monitored by the Data Inspection Board (DIB or *Datainspektionen*), a central government agency that carries out its functions independently. The DIB has 40 employees³⁵ who handle complaints from individuals concerning the processing of personal data. In 2009, the DIB handled 233 complaints about personal data processing.³⁶ The DIB has discretion to decide which complaints to pursue, but complainants always receive a response as to whether an investigation is initiated, and the outcome of any investigation.³⁷

The PDA requires that automated processing of personal data be notified to the DIB.³⁸ Several exemptions from the notification duty apply, for example if an entity appoints a personal data representative. The number of representatives has increased to 3,678 in 2009 from 3,562 in 2008.³⁹ Some processing operations that are likely to pose particular risks of improper intrusion of privacy must be notified for prior checking.⁴⁰

Initiatives have also been taken to use biometric data outside the government authority sector. In 2004 and 2005, the DIB handled several requests from schools regarding the use of fingerprint recognition devices to allow access to school canteens. The DIB said that processing of biometric data for this purpose was not compatible with the principles

³³ Parliament protocol 2009/10:139 from 17 June, 2010, at <http://www.riksdagen.se/webbnav/index.aspx?nid=101&bet=2009/10:139>. See Government Bill 2009/10:151 (Swedish only).

³⁴ This issue has engaged the Data Protection Agency considerably. See their press release on the new bill, 18 June 2010, in Swedish at <http://www.datainspektionen.se/press/nyheter/ja-till-starkare-integritetsskydd-vid-kreditupplysning/>.

³⁵ Official Web site, available in English at <http://www.datainspektionen.se/in-english/about-us/> (accessed September 2010).

³⁶ Earlier years: 279 in 2008, 233 in 2007, 307 in 2006, and 405 in 2005. Data Inspection Board's Annual Reports, available in Swedish at http://www2.datainspektionen.se/bt/ladda-ner-a-bestaell?page=shop.browse&category_id=10.

³⁷ *Id.*

³⁸ SFS 1998:204, § 36.

³⁹ Data Inspection Board's 2009 Annual Report, at 10.

⁴⁰ SFS 1998:204, §41.

of necessity and proportionality prescribed by the PDA and the EU Data Protection Directive. The fact that consent would be obtained from the students or their parents did not change this view. Despite this warning, biometrics, in the form of finger scans, are being used in the *Kvarnby* School in Stockholm to log in to school computers.⁴¹

The DIB published a report in 2005 about store bonus cards and found many privacy concerns.⁴² The report found that the cards contained detailed information about customers and their purchases. The DIB suggested that the companies gain consent from consumers before using the data for targeted advertising and improve the information given to new bonus customers so they could make an informed decision regarding their private data. The DIB also suggested the companies keep the data for as short a time as possible and restrict the information that is registered. In addition to the report, the DIB also issued supervisory decisions, including the three decisions of the DIB which have now been upheld by the County Administrative Court.

On 22 June 2006 the DIB issued a decision that SafeSite, a computer system that exchanges information and warnings between hotels and stores, did not violate the PDA because the warnings and descriptions examined by the Board were so vaguely formulated that they could not be considered personal data as it is defined in the PDA. SafeSite allows the warnings to be transferred to a document in order to make a police report.⁴³

The role of the Swedish DPA has been an issue of debate since the above-mentioned Committee on the protection of privacy proposed that the agency's mission should be expanded to a more general responsibility for privacy issues. The Committee rightly identified the absence of an institution with overall responsibility for privacy-related issues and suggested that this task should fall on an entirely new agency; or, at least that the DPA should get broader competences. These suggestions were too radical, however, and the conservative/liberal coalition government instead created a "Commission on Security and Integrity Protection" (*SÄKINT*), which is designed to monitor and control the use of covert surveillance by the police and secret services.⁴⁴ The *SÄKINT*'s first chairman was a former secret service General Director, but he resigned one year after his installation in 2008, his action supposedly related to the debate on the FRA

⁴¹ City of Stockholm Schools, "Precise Biometrics simplifies login procedures at the Kvarnby School, available here and here.

⁴² The Data Inspection Board, Report on Bonus Cards and the Personal Data Act, 2005:3, English summary available at <http://www.datainspektionen.se/Documents/rapport-bonus-cards.pdf>.

⁴³ See SafeSite's webpage, in Swedish at <http://www.safesite.se>,. Decision of the DIB of 20 June 2006

⁴⁴ *Förordning 2007:1141 med instruktion för Säkerhets- och integritetsskyddsnämnden* (Ordinance (2007:1141 Containing Instructions for the Swedish Commission on Security and Integrity Protection), at http://www.sakint.se/dokument/english/ordinance_instruction_scsip.pdf. The Commission actually replaced the earlier "Registry Board", which had similar tasks.

wiretapping.⁴⁵ The DPA, however, has neither received increased budgetary means, nor a broadened area of responsibility.⁴⁶

Major privacy & data protection case law

A case concerning biometric data in schools was presented, referring to a decision of the Data Inspection Board from 2004 regarding the collection and processing of students' fingerprints for the purpose of checking access to the school canteen.⁴⁷ "Regardless of the fact that consent was obtained, the decision was that the processing was not adequate or relevant and that such checks could be made in a less privacy-intrusive manner."⁴⁸ The Data Inspection Board's decision was appealed to the County Administrative Court who then upheld the decision.⁴⁹

In June 2007, the Administrative Court of Appeal in Stockholm passed its judgment in the Anti-Piracy Bureau case.⁵⁰

There was a debate in Sweden over whether police can access Internet records to fine file-sharers. A Swedish court of appeals upheld the country's first conviction of file-sharing.⁵¹

In 2009 the Swedish Parliament agreed the implementation of the Directive 2004/48/EC, commonly named the Intellectual Property Rights Enforcement Directive (IPRED). The Swedish implementing act (IPRED Act) has been widely debated as it was introduced in the wake of the above-mentioned FRA debate. It is intended to protect property rights and has been used by the Swedish Anti-Piracy Bureau to access copyrighted material and process against the server administrators. Since then, a number of cases have been brought to court by the music and publishing industries.⁵²

⁴⁵ "Statlig säkerhetsnämnd spricker," ("Government Security Commission Cracks") SvD, 9 December 2009, at http://www.svd.se/nyheter/inrikes/statlig-sakerhetsnamnd-spricker_379027.... See also Section "Wiretapping, access to, and interception of communications," *infra* in this report.

⁴⁶ The DPA in fact receives about the same budgetary means in 2010 as it did in 1991 (figure adjusted to consumer price index) although its tasks have multiplied. Figures available in: *Betänkande 1991/92:KU26 Anslag till datainspektionen* (Statement of the Constitutional Board Regarding Funding of the Data Protection Agency), in Swedish at <http://www.riksdagen.se>; *Regleringsbrev för budgetåret 2007 avseende Datainspektionen*, (Regeringsbeslut Fi2006/7202) (2007 Instructions to the Data Protection Agency), in Swedish at <http://www.esv.se>.

⁴⁷ 11th Annual Report of the Article 29 Data Protection Working Party, *supra*. See also Section "Data Protection Authority," *supra* in this Report.

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ See Section "Cybercrime," *infra* in this Report.

⁵¹ *Id.*

⁵² *Id.*

One of the most important and internationally known legal cases in Sweden occurred in 2008-2009 and concerned one of the world's biggest torrent trackers, The Pirate Bay.⁵³

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Secret camera surveillance, communications surveillance, and wiretapping require a court order according to the Act on Measures to Investigate Certain Serious Crimes⁵⁴ and Chapter 27 of the Code of Judicial Procedure. Communications surveillance and wiretapping used to be regulated by an act from 1952, which had to be extended on a yearly basis; covert camera surveillance was regulated in a similar way, albeit separately, by the Act on Secret Camera Surveillance.⁵⁵ In 2003, the scope of the 1952 Act was extended to terrorist crimes referred to in the legislation that implements the EU Framework decision 2002/475/JHA of 13 June 2002 on combating terrorism.⁵⁶ As of 1 January 2009, the limited regulations on covert camera surveillance were made permanent and moved into the Code of Judicial Procedure. The 1952 Act was abolished and replaced by the new legislation on "Certain Serious Crimes" (*vissa samhällsfarliga brott*) mentioned above. This law extends the competences of the secret services, as well as the scope of applicable crimes, to use wire tapping, wire surveillance, postal communications interference and secret camera surveillance. Suspects that have been monitored have to be informed about the surveillance after its termination.⁵⁷

Together with the recent introduction in Sweden of covert audio surveillance (*buggning*),⁵⁸ which has been a highly controversial issue for around 30 years, the

⁵³ *Id.*

⁵⁴ *Lag* (2008:854) *om åtgärder för att utreda vissa samhällsfarliga brott*.. Author's note: The terminology in Swedish legislation is sometimes confusing. A difference is made between "*teleavlyssning*" ("communications surveillance") and "*teleövervakning*" ("wiretapping"). These terms are difficult to translate, and to simplify the former is here translated to "communication surveillance" because it refers to the collection of communications data rather than contents. "Wiretapping" is the active monitoring of the contents of the communications. See <http://www.sakerhetspolisen.se/> (in Swedish) for more information.

⁵⁵ *Lag* (1995:1506) *om hemlig kameraövervakning*.

⁵⁶ Section 1 amended by SFS 2003:151. See Council Framework Decision 2002/475/JHA on combating terrorism, 13 June 2002, OJ L 164, 22 June 2002, at 3-7; Cf. Council Framework Decision 2008/919/JHA amending Framework Decision 2002/475/JHA on combating terrorism, 28 November 2008, OJ L 330, 9.12.2008, at 21.

⁵⁷ Parliamentary protocol 2008/09:17; Government proposition 2007/08:163, in Swedish at <http://www.riksdagen.se/Webbnav/index.aspx?nid=7175&nr=3&utsk=JuU&rm=2008/09>

⁵⁸ Parliamentary protocol 2007/08:24; Government propositions 2005/06:178, 2006/07:133 <http://www.riksdagen.se/Webbnav/index.aspx?nid=3120&doktyp=betankande&bet=2007/08:JuU3> (in Swedish)

Swedish secret services have gained unprecedented competences. Already demands from the Swedish Security Service have been made to extend these powers further, for example to avoid the mandatory court procedure before using such covert means of surveillance.⁵⁹ Parallel to the introduction of these new regulations, the above-mentioned Commission on Security and Integrity Protection (*SÄKINT*) was created in order to monitor the usage of the most repressive means of surveillance.⁶⁰

The Government has submitted a report to Parliament every year with details of all surveillance conducted. According to the 2003 government report⁶¹ to the Parliament, the use of secret surveillance had already increased "considerably" by 2002.⁶² In 2008, the number of instances of communications surveillance had almost doubled. The instances of wiretapping have increased by 500 percent since 1999. Both measures are conducted for an average period of 50 days and in about 40-50 percent of the cases, useful evidence can be gathered.⁶³ Human rights organisations, including the International Helsinki Federation for Human Rights, expressed concern in 2006 over increased use of surveillance techniques by the police and insufficient protection of the individual's right to privacy. This development has not gone unnoticed. The Swedish Helsinki Committee (SHC, now Civil Rights Defenders or CRD), a non-governmental organisation that monitors human rights compliance with the Helsinki agreement of 1975, has concluded that the state authorities' right to interfere in the private life of citizens, as allowed in certain instances by Swedish law, continued to lack both the necessary legality and transparency.⁶⁴ The CRD has called for an independent assessment of the necessity and effectiveness of secret surveillance methods used in Sweden. However, in connection with the legislation's becoming permanent, the Government stated that combating crimes related to national security have been given increased priority and that secret camera surveillance, wire surveillance, and wiretapping are all efficient tools for investigating terrorist and other serious crimes.⁶⁵

⁵⁹ Swedish Secret Service (2009), *Remissvar: "Utvärdering av buggning och preventiva tvångsmedel* (SOU 2009:70) (Remittance "Evaluation of bugging and preventive surveillance"), Dnr. AD 009-10106-09 .

⁶⁰ See Section "Data Protection Authority," *supra* in this report.

⁶¹ Government report to the Parliament in November 2003 (*Regeringens skrivelse* 2003/2004:36) (reporting on 2002 figures).

⁶² International Helsinki Federation for Human Rights (IHF), Human Rights in the OSCE Region: The Balkans, the Caucasus, Europe, Central Asia and North America, Annual report 2004 (events 2003), available at http://web.archive.org/web/20071222063812/http://www.ihf-hr.org/documents/doc_summary.php?sec_id=3&d_id=3860

⁶³ Government communication 2009/10:66, *Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2008* (Secret Wiretapping, secret communications surveillance and secret video surveillance in police investigations during 2008).

⁶⁴ International Helsinki Federation for Human Rights Annual report 2004, *supra*. With regard to the mission and activities of CRD, see <http://www.civilrightsdefenders.org/>.

⁶⁵ Parliamentary protocol 2008/09:17.

There were a number of government bills in 2006 that extended the use of secret surveillance, including *inter alia* a bill to allow telephone tapping for preventive reasons as well as bugging of conversations with the help of hidden microphones. On 31 May 2006 the Parliament decided to postpone discussion on the bill for at least a year and "insisted that safeguards against abuse of power be introduced into the bill, including an obligation for police to inform those subject to secret surveillance whenever this is considered safe for investigative reasons."⁶⁶ In 2007, a proposed bill would allow the National Defence Radio Establishment (*Försvarets Radioanstalt*, FRA) permission to use data mining software to search for sensitive keywords in all phone and email communications passing through cables or wires across the country's borders without a court order.⁶⁷ Until then the FRA could only listen to radio transmissions and did not have the authority to monitor and analyse Internet data traffic.⁶⁸ The FRA would need approval from a parliamentary committee on military intelligence affairs and would only be permitted to "tap into communications through pattern analysis and key word searches, and would not be entitled to target specific individuals."⁶⁹ Before this bill was approved on 18 June 2008, such traffic could only be monitored with court approval if police suspected a crime, although the agency was free to spy on airborne signals, such as radio and satellite traffic. The new legislation became widely controversial and has posed a threat to cross-border communications.⁷⁰ It allows for the interception of e-mail, telephone and faxes, and is therefore a threat to anyone dealing with a Swedish organisation.⁷¹ Even where domestic Internet communication is intended for two persons residing in Sweden, the same information may cross national borders through Germany, Denmark, and the USA.⁷² The implication is that people residing outside of Sweden, as well as Swedes, may be subject to the surveillance of FRA.⁷³

The FRA wiretapping law adopted on 18 June 2008 consists of four statutes: a newly adopted statute on signals intelligence and changes in three other statutes.⁷⁴ "FRA has a

⁶⁶ IHF, "Human Rights in the OSCE Region: Report 2007," at http://web.archive.org/web/20080802215207/http://www.ihf-hr.org/documents/doc_summary.php?sec_id=3&d_id=4387

⁶⁷ Paul O'Mahony, "Google likens Sweden to dictatorship," *The Local*, 30 May 2007, <http://www.thelocal.se/7452/20070530/>.

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ Laura Linkomies, Swedish surveillance threat to cross-border communications, *Privacy Laws and Business: Data Protection and Privacy Information Worldwide*, Issue 96, December 2008.

⁷¹ *Id.*

⁷² Editorial: Wiretapping – The Swedish Way, EDRI-gram Number 6.16, (27 August 2008), available at <http://www.edri.org/edriagram/number6.16/wiretapping-swedish-way>.

⁷³ *Id.*

⁷⁴ *Id.*

mandate to search for 'external threats', which involves everything from military threats, terrorism, IT security, supply problems, ecological imbalances, ethnic and religious conflicts, and migration to economic challenges in the form of currency and interest speculation."⁷⁵ Causing further controversy is the lack of any requirement that the FRA should have a reason to suspect crime or need a court order before being allowed to conduct surveillance of Swedish residents.⁷⁶ After criticism by privacy groups and a massive public debate about such sweeping powers, the Act was amended.⁷⁷ In addition, "a legal complaint has been made to the EU in July about this Act's possible breach of the EU's privacy and discrimination law with regard to cross-border legal consultations."⁷⁸ The European Commission, who would have to bring formal infringement procedures against Sweden, has not yet made any such action.⁷⁹

The law was supposed to enter into force by January 2009 but after the massive debacle surrounding the issue in Sweden, the government proposed a modified bill that included a number of privacy improvements to the original legislation. Among other aspects, the details of FRA monitoring are now subject to political scrutiny and the FRA must seek permissions for every search made. The amendment was approved by the Parliament on 14 October 2009 and the new, restricted competences of the FRA came into force on 1 December of the same year.⁸⁰ As of September 2010, the FRA has still to initiate its surveillance scheme. Technical problems regarding access points as well as resistance from some Internet service providers have allegedly delayed the actual surveillance from starting.

National security legislation

In 2002, the Swedish Parliament approved two anti-terrorism laws in order to implement the UN Convention for the Suppression of the Financing of Terrorism⁸¹ and the EU Council Framework Decision on Combating Terrorism.⁸² Sweden signed, but has not ratified, the Council of Europe Convention on the Prevention of Terrorism.⁸³ The Act on Criminal Responsibility for Terrorist Crimes entered into force in July 2003 and classifies

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ Act (2009:967) on changes in Act (2008:717) on military signal surveillance (*Lag om ändring i Lag om signalspaning iförsvarsunderrättelseverksamhet*)

⁷⁸ *Linkomies, supra.*

⁷⁹ *Id.*

⁸⁰ Statement of the Parliamentary board of defence, 2009/10:FöU3.

⁸¹ See <http://www.un.org/law/cod/finterr.htm>.

⁸² Council Framework Decision 2002/475/JHA on combating terrorism, *supra*.

⁸³ Council of Europe, Convention on the Prevention of Terrorism CETS No. 196, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=7&DF=27/07/2010&CL=ENG>

certain crimes – such as murder or kidnapping – as terrorist acts when committed against countries, their institutions, or their citizens with the aim of intimidating, altering, or destroying political, economic, or social structures.⁸⁴ Strict punishments apply. The Swedish Helsinki Committee noted, in addressing an appeal to the Swedish Government, that the definition of terrorist crimes in the Act is unclear, and that neither the Act nor the EU Decision addresses the issue of how to draw the line between politically motivated violence and terrorism.⁸⁵ In July 2003, the Parliament also adopted an Act on surrender from Sweden⁸⁶ in accordance with the EU Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant.⁸⁷ The Act came into force in January 2004. At the same time, a new Act on Joint Investigation Teams for Criminal Investigations came into force.⁸⁸ The Act applies to joint investigation teams for criminal investigations set up between authorities in Sweden and those in one or more EU Member States. The Act implements the EU Council Framework decision 2002/465/JHA of 13 June 2002 on joint investigation teams.⁸⁹ The Act contains rules on, for example, conditions for the use of information received through a joint investigation team.⁹⁰

Data retention

In March 2006, the EU enacted Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.⁹¹ The Directive aims to harmonise the rules on retention of traffic data throughout the EU in order to facilitate judicial cooperation in criminal matters. All traffic data generated in publicly available electronic communications, such as telephony or the Internet, would have to be retained by service providers for law enforcement purposes. The data would have to be kept for a minimum period of six months and a maximum period of two years.⁹² Member States had until 15 September 2007 to transpose the requirements of the Directive into national laws; however, the issue became controversial in Sweden after the FRA debate and the application of this Directive has been postponed even though it meant facing an

⁸⁴ SFS 2003:148.

⁸⁵ International Helsinki Federation for Human Rights (IHF) Annual report 2004, *supra*.

⁸⁶ SFS 2003:1156, available in English at <http://www.sweden.gov.se/sb/d/3288/a/19568>.

⁸⁷ OJ L 190, 18 July 2002, at 1-20.

⁸⁸ SFS 2003:1174, available in English at <http://www.sweden.gov.se/sb/d/3288/a/19568>.

⁸⁹ OJ L 162, 20 June 2002, at 1-3.

⁹⁰ See sections 5 – 7 of the Act 2003:1174.

⁹¹ EU Directive 2006/24/EC, 15 March 2006, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT>

⁹² *Id.*

infringement procedure commenced by the European Commission and a fine.⁹³ The Swedish debate on privacy and surveillance cooled off during 2010, but the introduction of Directive 2006/24/EC is still debated in government circles. The liberal wing wants to postpone implementation even longer, to the price of paying another fine to the Commission, while other fractions of the ruling conservative/liberal coalition aim at implementing the Directive during the next legislative period. In any case, the issue was too sensitive to bring up before the September elections, especially with the FRA experience from 2008, and the Directive has not been debated publicly at all.⁹⁴

National databases for law enforcement and security purposes

The question of collecting and storing DNA information about all Swedish citizens has been subject to public debate. In June 2004, proposals were made to widen the scope of DNA use in law enforcement.⁹⁵ According to current legislation, DNA samples fall under the rules in Chapter 28 of the Code of Judicial Procedure and rules in the Police Data Act of 1998. The inquiry tasked with reviewing the current legislation suggested introducing specific rules regarding DNA samples in law enforcement and allowing such samples to be taken from persons who are arrested, taken into custody, or suspected of crimes that can lead to imprisonment, but also from other persons if it is required in the investigation of such crimes. According to the inquiry's report, results from DNA analyses should be put into the DNA register kept by the National Police Board regarding persons who are suspected of, or sentenced for, crimes where the penalty includes imprisonment. The current rules on the DNA register only allow registration of those who have been convicted of a crime that involves a penalty of more than two years' imprisonment. According to Section 24 of the Police Data Act, registration must be limited to such data that provides information about identity – other DNA information must not be registered. The inquiry suggested that information in the register should be deleted when the preliminary investigation is withdrawn or when charges against the individual in question have been withdrawn or rejected. Information regarding persons who have been

⁹³ Each Member State is responsible for the implementation of EU law (adoption of implementing measures before a specified deadline, conformity and correct application) within its own legal system. The European Commission is responsible for ensuring that EU law is correctly applied. Consequently, where a Member State fails to comply with EU law, the Commission has powers of its own to try to bring the infringement to an end and, where necessary, may refer the case to the European Court of Justice. More information are available at http://ec.europa.eu/community_law/infringements/infringements_en.htm. For the FRA debate see Section "Wiretapping, access to, and interception of communications," supra in this report.

⁹⁴ See "*Regeringen skjuter på datalagring*" ("Government Postpones Data Retention"), SvD 21 October 2009, available at http://www.svd.se/nyheter/inrikes/regeringen-skjuter-pa-datalagring_3686789.svd. Details on the developments vis-à-vis the European Commission stem from a panel debate on surveillance and privacy with Camilla Lindström of the liberal party *Folkpartiet*, and Anna Pettersson from *Nej-till-FRA*, held at Södertörn University, 16 September 2010.

⁹⁵ Ministry publications series 2004:35, *Genetiska fingeravtryck*, 7 July 2004, Ministry of Justice, available in Swedish at <http://www.regeringen.se/sb/d/108/a/27189>.

convicted should continue to be retained until the person is deleted from the register of convicted persons in accordance with the specific rules in the Act of 1998.

In November 2007, the Ministry of Justice presented a report with a proposal for a new act on the processing of personal data by the police in crime combating activities replacing the Police Data Act of 1998.⁹⁶ The proposed new act regulates all processing by the police in their crime combating activities and will apply to the National Police Board, the police authorities and the Swedish National Economic Crimes Bureau.⁹⁷ The new act grants law enforcement agencies longer periods of record keeping (five instead of three years, see Chapter 3 paragraphs 9-15) as well as extended scope of records such as DNA. The new Police Data Act also emphasises the general accessibility of records across institutional boundaries (Chapter 3). In the case of specific crimes such as terrorism, records can now be kept for up to 70 years. A declared aim of the new act is to make preventive policing possible.⁹⁸ Another important development from the 1998 act is that records that used to be treated as separate are now subjects of common regulation to a certain extent. The aim was to enable and regulate data sharing between law enforcement agencies. The act, and especially the problematic process of its development between 2007 and 2010 has been criticised by the Data Protection Agency for being vague, opaque, and determined to grant law enforcement agencies with new rights rather than to ensure citizens' privacy.⁹⁹

National and international data disclosure agreements

In 2004, Sweden put forth a proposal for new EU Framework rules on the exchange of information between law enforcement authorities; two years later it was approved by the Council as Framework Decision 2006/960/JHA.¹⁰⁰ The proposal required law enforcement authorities in EU Member States to supply certain information and intelligence to similar authorities in other EU Member States, upon request, for the purpose of investigating crimes, particularly serious offences and terrorist acts. The proposal has been criticised by privacy groups as being too broad and going far beyond

⁹⁶ 11th Annual Report of the Article 29 Working Party on Data Protection, *supra*.

⁹⁷ Polisdatlag (Police Data Act)(SFS 2010:361), in Swedish at <http://www.notisum.se/rnp/sls/lag/20100361.htm>.

⁹⁸ *Regeringens proposition* Government bill 2009/10:85, in Swedish at 1, at <http://www.regeringen.se/content/1/c6/13/76/19/f0fb01a9.pdf>.

⁹⁹ *Datainspektionen* 2008. Yttrande (Dnr 1548-2007) ang *Departementspromemorian* (DS 2007:43) *Behandling av personuppgifter i polisens brottsbekämpande verksamhet* (Statement (1548-2007) of the Swedish Data Protection Agency regarding processing of personal data in police investigations), at <http://www.regeringen.se/content/1/c6/13/76/19/f0fb01a9.pdf>

¹⁰⁰ Council of the European Union, Draft Framework decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, in particular as regards serious offences including terrorist acts (10215/04), available at <http://register.consilium.eu.int/pdf/en/04/st10/st10215.en04.pdf>. See also Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, 18 December 2006, OJ L 386, 29.12.2006, at 89.

the relatively narrow range of offences covered by other EU instruments, such as the Europol Convention.¹⁰¹

Cybercrime

In June 2007, the Administrative Court of Appeal in Stockholm passed its judgment in the Anti-Piracy Bureau case.¹⁰² The case dealt with the issue of whether IP numbers are to be considered personal data.¹⁰³ The Anti-Piracy Bureau, which is a cooperative economic association, "had collected scattered pieces of information, in particular IP numbers, in connection with file-sharing of copyrighted material on the Internet."¹⁰⁴ The Data Inspection Board stated in its decision that "IP numbers were to be considered personal data and that the processing carried out by the Anti-Piracy Bureau was in breach of the Personal Data Act (PDA), since it implied processing of offences within the meaning of Section 21 of the PDA."¹⁰⁵ The law remains that "only public authorities may process personal data concerning legal offences involving crime, unless the Board has granted an exemption from that prohibition."¹⁰⁶ In its decision of June 2005, the Board ordered the Anti-Piracy Bureau to stop the processing. The Anti-Piracy Bureau claimed that the IP numbers could not be considered as personal data since the Bureau did not have access to the personal data identifying the owner of a subscription that uses a certain IP address and appealed the decision.¹⁰⁷ As a result, both the County Administrative Court and the Administrative Court of Appeal upheld the Data Inspection Board's decision.¹⁰⁸ Subsequent to the 2005 decision, the Anti-Piracy Bureau applied for an exemption from the prohibition of Section 21 of the PDA for the purpose of "processing IP numbers so that it could report, for instance, to the police and inform Internet service providers of subscribers' copyright infringements."¹⁰⁹ The Data Inspection Board granted an exemption, and the Bureau was allowed to process personal data relating to offences until the end of 2008.¹¹⁰

¹⁰¹ Council Act of 26 July 1995, drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C 316, 27.11.1995, at 1.

¹⁰² 11th Annual Report of the Article 29 Data Protection Working Party, *supra*.

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

There was a debate in Sweden over whether police can access Internet records to fine file-sharers. A Swedish court of appeals upheld the country's first conviction of file-sharing.¹¹¹ This case is of note because the conviction was based on supporting evidence consisting of an IP address linked to a file-sharing network. Previously, in October 2006, a Swedish judge ruled that evidence insufficient to prove guilt.¹¹² This case could continue to the Swedish Supreme Court and shows that "electronic evidence, such as traffic, location, and time data, can originate, be scattered, and end on different formats and different coordinates in time and space, and may easily be manipulated and hard to identify, due to services offering anonymity or pseudonymity."¹¹³

In 2009 the Swedish Parliament agreed to the implementation of Directive 2004/48/EC, commonly named the Intellectual Property Rights Enforcement Directive (IPRED). The Swedish implementing act (IPRED Act) has been much debated, as it was introduced in the wake of the above-mentioned FRA debate. It is intended to protect property rights and has been used by the Swedish Anti-Piracy Bureau to access copyrighted material and open process against the server administrators. Since then, a number of cases have been brought to court by the music and publishing industries.

The first case that tried using IPRED concerned alleged file-sharing of audio books from a customer of the service provider E-Phone. The publishers wanted E-Phone to hand out information regarding the identity of the person behind an IP address, but E-Phone refused. The case went to the highest instance in Sweden, but was referred to the Court of Justice of the European Union in order to get a prejudicating verdict. The Swedish court wanted the relationship with the Directive 2006/24/EC – the data retention directive mentioned above – clarified. Even though Sweden has yet to implement the Directive, there are uncertainties as to whether the IPRED act is illegal. In the meantime, many other cases were brought but none has been completed. IPRED is celebrated as a failure among file-sharers and entertainment industries alike.¹¹⁴

One of the most important and internationally known legal cases in Sweden occurred in 2008-2009 and concerned one of the world's biggest torrent trackers, The Pirate Bay. The case originated from a controversial raid in March 2006 by the Swedish police on the premises of the Web farm hosting The Pirate Bay, PRQ. Suspicions were aired that the

¹¹¹ Niklas Pollard, "Swedish court upholds file-sharing conviction," Reuters, 12 June 2007 <http://www.reuters.com/article/internetNews/idUSL1220452220070612>.

¹¹² Jan Libbenga, "Swedish file sharers fined," *The Register*, 19 October 2006 http://www.theregister.co.uk/2006/10/19/swedish_file_sharers_fined/; see also "Filesharing and Digital Evidence Case in Sweden," Digital Civil Rights in Europe 11 October 2006 http://www.edri.org/edrigram/number4.19/p2p_sweden.

¹¹³ *Id.*

¹¹⁴ "Tungt bakslag för Ipred" ("Heavy Backlash for IPRED"), *Dagens Nyheter*, 16 September 2010, available at <http://www.dn.se/kultur-noje/nyheter/tungt-bakslag-for-ipred-1.1171556>; Government proposition 2008/09:67 *Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG* (Civil penalties for intellectual property - the implementation of Directive 2004/48/EC, available at http://www.riksdagen.se/webbnav/index.aspx?nid=37&dok_id=GW0367.

raid was a result of pressure by the US government and the Motion Picture Association of America. Large demonstrations against the raid were held in Sweden by the youth organisations of both the Green and Left political parties as well as the newly formed Pirate Party. The entertainment industry, as represented by the Swedish Anti-Piracy Bureau, the International Federation of the Phonographic Industry (IFPI), and lawyer Monique Wadsted, finally won the case on 17 April 2009. The four proprietors of Pirate Bay were sentenced to pay one of the highest fines in Swedish history – over SEK100 million, roughly equivalent to €10 million. However, due to the circumstances, the sum was reduced to €3 million Euro, still disproportionate in the Swedish context. Critics claimed that the courts were partisan and had accepted too many of the entertainment industry's arguments.¹¹⁵ The Pirate Bay proprietors were accused of having sought personal gain from the tracker activity through the advertisements on the site, in addition to the violation of copyright law.¹¹⁶

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

The provision on unsolicited e-mail contained in the EU Directive 2002/58/EC was implemented in April 2004 when the Swedish Marketing Act was amended to reflect the Directive in this respect.¹¹⁷ As a result of this amendment, direct marketing by email now requires prior consent. The National Post and Telecom Agency is in charge of supervising compliance with the Electronic Communications Act.¹¹⁸ Monitoring of the Marketing Act, including the provisions on unsolicited email, falls under the scope of the Swedish Consumer Agency.¹¹⁹

The provisions on privacy in publicly available electronic communications services are found in Chapter 6 of the ECA. This includes provisions on security in public communications networks, processing of traffic and location data, cookies, public directories, etc. The PDA applies to processing of personal data in electronic communications networks and services to the extent that the ECA does not stipulate otherwise. The National Post and Telecom Agency emphasises the importance of

¹¹⁵ "Fällande dom i det s.k. Pirate Bay-målet" ("Verdict in the so Called Pirate Bay Trial"), *Sveriges Domstolar*, 17 April 2009, available at http://www.domstol.se/templates/DV_Press___10382.aspx.

¹¹⁶ Case description B13301-06 of the International attorney's office in Stockholm, available in Swedish at http://www.wired.com/images_blogs/threatlevel/2009/04/piratebayverdicts.pdf.

¹¹⁷ SFS 1995:450, paragraph13(b).

¹¹⁸ <http://www.pts.se> (in Swedish).

¹¹⁹ <http://www.konsumentverket.se> (in Swedish).

enhancing the level of user knowledge and awareness about security on the Internet.¹²⁰ However, Sweden is second from the bottom in the EU when it comes to protecting its citizens' private integrity, according to Privacy International's 2006 privacy ranking.¹²¹

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

For three consecutive years (2007-2009) the Swedish Data Inspection Board has conducted a survey of young people's attitudes toward privacy in general and privacy on the Internet in particular.¹²²

Online youth safety

For three consecutive years (2007-2009) the Swedish Data Inspection Board has conducted a survey of young people's attitudes toward privacy in general and privacy on the Internet in particular.¹²³ As already mentioned, since 2007 the Swedish Data Inspection Board has conducted a survey of young people's attitudes toward privacy in general and privacy on the Internet in particular.¹²⁴ The previous studies have shown that young people are very active on the Internet and that they like to remain anonymous. They do, however, engage in unsafe behaviours on the Internet as well as in their everyday lives.¹²⁵

¹²⁰ See generally, *Post & Teletyrelsen*, Reports, at <http://www.pts.se/en-gb/Documents/Reports/>.

¹²¹ Privacy International, "National Privacy ranking 2006 – European Union and Leading Surveillance Societies," <http://www.privacyinternational.org/survey/phr2005/phrtable.pdf>.

¹²² For more information see Section "Online youth safety," *infra* in this report.

¹²³ Survey reports are available at <http://www.datainspektionen.se/in-english/in-focus-youth-and-privacy/>.

¹²⁴ *Id.*

¹²⁵ Data Inspection Board, *Youth and Privacy 2009*, 2009:1, available in English at <http://www.datainspektionen.se/Documents/rapport-ungdom-2009-eng.pdf>. The study is based on a Web survey of 533 young individuals. The sample is representative with regard to gender, region, and age among 14 to 18-year-olds. See Sections "Wiretapping, access to, and interception of communications", and "Cybercrime," *supra* in this report..

The 2009 results clearly indicate that young people have a more negative attitude toward surveillance in general.¹²⁶ One possible explanation might be the debates surrounding the FRA and IPRED legislation during 2008.¹²⁷ Almost half of the respondents stated that the debate around the FRA legislation made them think more about issues of privacy.

Young people would easily consider revealing information that has traditionally been considered private, including their political and religious views. Issues that young people judged more private include their financial situation or on whom they have a crush.¹²⁸

The police are the most trusted of all the various government agencies and authorities. Young people trust private businesses the least and generally believe that the worst violation of privacy consists of businesses searching for information about them. On the Internet, however, the government searching for information is considered the worst violation of privacy.¹²⁹

Young people continue their extensive use of IT, and primarily the Internet. One major change since the first survey about young people's attitudes toward privacy is the sharp increase in the number of respondents who are most likely to surf the Internet on their own computer.¹³⁰

Many young people have experienced various kinds of cyber bullying. Boys are most likely to be the victims of cyber bullying with one exception: girls are much more likely to have been the victims of sexual harassment. While only a fourth of the young people have used the abuse function on a community, individuals who have used it reported that it had been effective.¹³¹

While surveillance is becoming less acceptable, a considerable majority of respondents will tolerate it if it would prevent serious crimes. Video surveillance is the most accepted form of technological surveillance. Personal presence (police, security guard, or break monitor) is preferred over technological surveillance and is considered the most effective for crime prevention.¹³²

While respondents continue to be quite knowledgeable about privacy on the Internet, many are less familiar with the world outside the computer. They are least informed about personal identity numbers. Although most respondents know that one of the missions of

¹²⁶ See Sections "Wiretapping, access to, and interception of communications" and "Cybercrime," *supra* in this report.

¹²⁷ Data Inspection Board, *Youth and Privacy 2009*, *supra*.

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² *Id.*

the Swedish Data Inspection Board is to inform people about risks on the Internet, almost half believe that it also controls spam.¹³³

TERRITORIAL PRIVACY

Video surveillance

The 1998 Public Camera Surveillance Act¹³⁴ and the Public Camera Surveillance Ordinance¹³⁵ restrict the use of such surveillance. In principle, video surveillance in places to which the public has access requires a permit from the County Administrative Board. In certain situations, it is sufficient to notify the County Administrative Board about the surveillance. The notification duty applies to post offices, banks, and stores where the surveillance only covers entrances, exits, and cash points. In a few other situations neither a permit nor notification is required. In all cases, the Act requires that clearly visible notices about the video surveillance are posted. Image and audio material may be stored for up to a month. The police and courts are able to store material for longer if it comprises part of an investigation of a crime. Penalties for breach of the law include fines or a maximum imprisonment of one year.

The 1998 Act was a significant liberalisation of the earlier regulations and a sharp increase in CCTV surveillance followed during the 2000s.¹³⁶ The Act has been subject to review by an inquiry that presented its report in November 2002.¹³⁷ The Act underwent reviews in 2002 and again in 2009, and a new act is expected to be enacted after the elections in September 2010. The new regulation marks an even larger liberalisation, foremost in two areas: first, private CCTV surveillance is *de facto* completely deregulated. This is the result of the inability of state agencies to control private CCTV applications. Secondly, video material can be stored for up to three months instead of the current 30-day period.¹³⁸ Rhetorically, the new act is legitimised by a need to make regulations more comprehensive, and it combines regulations from the old act and the Personal Data Act. This results in a more prominent role for the Data Protection Agency, which controls the implementation of the Personal Data Act. The proposed new law sees

¹³³ SFS 1998:150.

¹³⁴ SFS 1998:314.

¹³⁵ En ny kameraövervakningslag (A New Camera Surveillance Act), SOU 2009:87, annex 2). See also Ola Svenonius. Surveillance intensification – privacy simulation: Swedish surveillance and its basic conditions. (2004), available at http://www.ztg.tu-berlin.de/transport/docs/thesis_svenonius.pdf.

¹³⁶ Swedish Government Official reports (SOU) 2002:110, *Allmän kameraövervakning* (Public Camera Surveillance), Ministry of Justice, available at <http://www.regeringen.se/sb/d/108/a/437>.

¹³⁷ SOU 2009:87, at 15. Readers should compare this with the German case, where even a 48-hour period has been subject of controversy! See *Humanistische Union* (2009), "So weit die Kamera reicht" ("As far as cameras go"), available at http://www.humanistische-union.de/themen/datenschutz/videoueberwachung/videoueberwachung_details/back/videoueberwachung/article/so-weit-die-kamera-reicht.

¹³⁸ 12th Annual Report of the Article 29 Data Protection Working Party (2008), 16 June 2009, at 103, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/12th_annual_report_en.pdf.

the DPA as the main inspection authority in the area of CCTV surveillance. It remains to be seen if the DPA will be granted additional budget and manpower to adequately fulfil this responsibility.

In 2008, the Data Inspection Board sent out a Web questionnaire to schools and one of the issues was if and to what extent schools used video surveillance on their premises.¹³⁹ The result showed that video surveillance had increased by 150 percent compared to 2005, when a similar investigation was made. The Data Inspection Board then inspected seven schools and found that the video surveillance of students during daytime in many respects infringed against the Personal Data Act. The inspections also showed that there was a considerable lack of knowledge of the legislation on data protection and the Board therefore issued a checklist to make it easier for schools to decide when video surveillance is permitted. Appeals were lodged against the Board's decisions of 1 October 2008.¹⁴⁰

Location privacy (gps, mobile phones, location based services, etc.)

No specific information has been provided under this section.

Travel privacy (travel identification documents, biometrics, etc.) And border surveillance

Sweden implemented Council Regulation No. 2252/2004 on Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States. The Swedish passport contains a digital facial image that is stored in a chip included in the passport.¹⁴¹ The biometric data that can be retrieved from the facial image is to be destroyed immediately after the delivery of the passport to the applicant or after a passport check. No other kinds of data than those already registered will be entered into the centralised register of passports.¹⁴²

Between 2006 and 2008, the Data Inspection Board carried out inspections regarding public transport companies' new ticket systems with smart cards that leave electronic traces (systems based on RFID technology).¹⁴³ When the passenger uses his electronic ticket the following data is recorded: card number, date, time, and stop/gate. If the card holder has registered his smart card with the transport company the card number is connected with the passenger's personal identification number, name, and address. In this way, the electronic traces from the card can be connected to a specific person. The Data

¹³⁹ *Id.*

¹⁴⁰ See <http://web.archive.org/web/20070813221357/http://www.polisen.se/inter/nodeid=33591&pageversion=1.html><http://www.polisen.se/inter/nodeid=33591&pageversion=1.html>.

¹⁴¹ See fact sheet from the Ministry of Justice, (Ju 05.04) March 2005, available in Swedish at <http://www.regeringen.se/content/1/c6/04/02/02/aa286ad5.pdf>.

¹⁴² 12th Annual Report of the Article 29 Data Protection Working Party (2008), *supra* at 105.

¹⁴³ *Id.*

Inspection Board decided that such traces could only be stored for 60 days and thereafter must be de-identified. One of the transport companies concerned appealed against the Data Inspection Board's decision to the County Administrative Court, which in January 2009 repealed the Board's decision and remitted the case for a new review.¹⁴⁴

NATIONAL ID & SMART CARDS

Identification of individuals within public administration is based on the system of national identification numbers.¹⁴⁵ Such numbers have been used in Sweden since the 1940s. Since 1994, the data protection legislation includes restrictions on the use of identification numbers. Under Section 22 of the PDA, national identification numbers may only be processed without consent if the processing is clearly justified with regard to the purpose of the processing, the importance of secure identification, or some other substantial reason.

On 1 October 2005, the Swedish Government introduced the "official" electronic ID card containing biometric data. The new "national identity card" (*nationellt identitetskort*) is not compulsory and does not replace previous paper ID cards. It can be used as a proof of identity and citizenship and as a valid travel document within the Schengen area. It complies with ICAO standards for biometric travel documents; it is issued by the passport offices and manufactured by the same supplier as the biometric passport.¹⁴⁶ In addition to the contactless chip containing a digital picture of the holder, it also has a traditional chip which may be used to securely access e-Government services in the future.¹⁴⁷

Rfid tags

RFID technology is used by public transport companies' new ticket systems.¹⁴⁸

BODILY PRIVACY

No specific information has been provided under this section.

¹⁴⁴ The personal identity number uses ten digits where the first six give the birth day in YYMMDD format; the national Swedish ID uses a 12-digit number to allow YYYYMMDD. This is followed by a hyphen. People over the age of 100 replace the hyphen with a plus sign. The seventh through ninth digits are a serial number – an odd number for men, an even number for women. The tenth digit is a checksum.

¹⁴⁵ ePractice, eGovernment Factsheet – Sweden – National Infrastructure (June 2010), available at <http://www.epractice.eu/en/document/288382>.

¹⁴⁶ *Cfr.* Section "E-Government & Privacy," *infra* in this report.

¹⁴⁷ *Cfr.* Section "Travel privacy (travel identification documents, biometrics, etc.) and border surveillance," *supra* in this report.

¹⁴⁸ "Sweden Concerns over Employer Monitoring," BNA World Data Protection Report, Volume 2, Issue 4, April 2002. The proposal is available at http://naring.regeringen.se/propositioner_mm/sou/pdf/sou2002_18a.pdf (in Swedish with summary in English).

WORKPLACE PRIVACY

In 1999, the Swedish government established a Committee to study workplace privacy issues. In March 2002, the Committee issued a proposal recommending specific legislation to protect the personal information of current and former employees, and employment applicants in both the private and public sectors.¹⁴⁹ The proposal has not led to legislation. In 2005, the DIB issued a report about workplace privacy and found that few employers monitored email, used camera surveillance, or used biometrics. The study also found that few employers had procedures for deleting data in accordance with the PDA.¹⁵⁰

HEALTH & GENETIC PRIVACY

Medical records

With regard to privacy in the health and medical sector, the use of information technology has increased. While information technology can facilitate documentation of health and medical care and contribute to using resources more efficiently, it also involves new challenges in terms of privacy and data protection. The National Board of Health and Welfare has proposed in a report that the Act on Patients' records should explicitly allow that one comprehensive record is kept for each patient.¹⁵¹ The Board has said that using one record covering all occasions when a patient has sought medical care at different care providers would even further reduce the time spent on documentation of medical treatment. Moreover, the Board has said that this requires that there are no obstacles in terms of secrecy and that jointly processing personal data is allowed. The DIB has pointed to several problems that this proposal poses from both a secrecy perspective and a privacy point of view.¹⁵²

Personal data processing in the health and medical sector was until 2008 regulated by the Health Care Register Act of 1998 and the Patients' Records Act of 1985. In 2005, the DIB issued a report about accessibility to patient data that found that there was a lack of working routines to check that unauthorised users do not gain access to patient's data. The report created a list of guidelines that the medical community needs to review and implement to protect sensitive information.¹⁵³ As a result, new rules on patients' records

¹⁴⁹ The Data Inspection Board, *Monitoring in Working Life*, 2005:3, English summary available at <http://www.datainspektionen.se/Documents/rapport-monworklife-summary.pdf>http://www.datainspektionen.se/pdf/rapporter/bonus_cards.pdf.

¹⁵⁰ Referred to in terms of reference No. 2004:95, by the Ministry of Health and Social Affairs.

¹⁵¹ The Data Inspection Board's Report 2002:1, "*Nationella kvalitetsregister*" ("National Quality Registry"), available in Swedish at <http://www.datainspektionen.se/Documents/rapport-nationella-kvalitetsregister.pdf>.

¹⁵² The Data Inspection Board, "Increased Accessibility to Patient Data," 2005:1, English summary available at <http://www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf>.

¹⁵³ Patientdatalag ("Patient Data Act") SFS 2008:355, at <http://62.95.69.3/SFSdoc/08/080355.pdf>.

and health care were introduced in 2008.¹⁵⁴ The new legislation means both threats to and regulation of patient privacy: it introduces Internet journals that can be accessed by several specialists at the same time, thus reducing the patient's control over her/his records. This "cohesive journal" (Chapter 6) is, however, subject to strict regulations by means of "internal secrecy" (Chapter 4) and is based on consent of the patient.¹⁵⁵ The Swedish DPA oversees the act's implementation.

Sweden has signed, but not ratified, the Council of Europe Convention on Human Rights and Biomedicine, which mandates confidentiality of personal data, its Additional Protocol on the Prohibition of Cloning Human Beings, and its Additional Protocol concerning Biomedical Research.¹⁵⁶

GENETIC IDENTIFICATION

According to current legislation, DNA samples fall under the rules in Chapter 28 of the Code of Judicial Procedure and rules in the Police Data Act of 1998.¹⁵⁷

FINANCIAL PRIVACY

No specific information has been provided under this section.

E-GOVERNMENT & PRIVACY

Voting is open to those aged 18 and older but is not mandatory.¹⁵⁸ National elections are managed by the Swedish Election Authority or *Valmyndigheten*, which was established in July 2001.¹⁵⁹ The Election Authority is responsible for all voting material from voter registration cards to paper ballots, including development of and support for the information technology systems used during the election process. The Election Authority keeps a register with voter registration information for the purpose of producing voter

¹⁵⁴ *Id.* See also Datainspektionen 2009. "Patientdatalagen och den personliga integriteten" ("Patient Data Act and Privacy"), Fact sheet on the Patient Data Act, in Swedish at <http://www.datainspektionen.se/Documents/faktablad-patientdatalagen.pdf>.

¹⁵⁵ Council of Europe, Convention on Human Rights and Biomedicine, CETS No. 164, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/164.htm>; Additional Protocol to the Convention on Human Rights and Biomedicine, on the Prohibition of Cloning Human Beings, CETS No. 168, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/168.htm>; Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, CETS No. 195, available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/195.htm>.

¹⁵⁶ For more information *cfr*: Section "National databases for law enforcement and security purposes," *supra* in this report.

¹⁵⁷ CIA Country Fact Book, 1 January 2004, available at <https://www.cia.gov/library/publications/the-world-factbook/geos/sw.html>.

¹⁵⁸ <http://www.val.se> (in Swedish).

¹⁵⁹ SFS 2001:183.

registration cards.¹⁶⁰ Voter registration information is also kept in secured files at the Central Bureau of Statistics.¹⁶¹ The Election Authority prepares a list of those who are entitled to vote in the election based on information that, 30 days prior to the election day, is contained in the population registration database in accordance with the Processing of Personal Data in the Swedish Tax Agency's population registration and the Land Registration Act.¹⁶² Individuals are sent a voting card with the voter's name and number in the electoral roll, what elections the voter may participate in, and the voter's polling station and its opening hours.¹⁶³ Voting can take place at a voting booth, by messenger, or by mail.¹⁶⁴ Voters who cannot vote at their polling station on election day may vote in advance at any voting place, such as the municipal office, a library, school, or post office.¹⁶⁵ Advance voting begins 18 days before election day. Voting secrecy is highly valued. Ballots are cast on paper ballots that are placed in envelopes, which are then given to a poll official to place in the appropriate ballot box.

So far, Swedish citizens have been using non-official electronic ID cards issued by the Swedish Post and software-based electronic IDs like the "BankID" (developed by the largest Swedish banks) and "SteriaeID" to access certain e-Government services. In November 2006, approximately 3 million such eIDs had been issued. A rough estimate of the use of eIDs in Sweden is that more than 1 million users make approximately 2.5 million transactions (including both authentication and signatures) a month using eIDs for e-Government and other services on the market.¹⁶⁶

Any physical person with a Swedish personal identity number (a unique identification number for Swedish citizens) can obtain an eID. This number appears on the eID and its microchip. Legal entities can also use an eID. Furthermore, Steria has introduced a new type of eIDs in Sweden: organisational certificates for personal use. This type of certificate contains the organisation's number, the name of the organisation, and the name and role of the person. It is worth noting that none of the organisational eIDs contains the personal identity number, which is considered to be sensitive information.¹⁶⁷

¹⁶⁰ European Commission, CyberVote Report (IST-1999-20338), available at http://ec.europa.eu/information_society/activities/egovernment/research/projects/cybervoting/index_en.htm.

¹⁶¹ SFS 2005:837, available in English at http://www.val.se/pdf/2005_elections_act.pdf.

¹⁶² SFS 2005:837, explanatory version of the law available in English at http://www.val.se/pdf/2005_elections_act.pdf.

¹⁶³ SFS 2005:837, *supra*.

¹⁶⁴ The Election Authority, "Voting," at http://www.val.se/in_english/general_information/voting/index.html.

¹⁶⁵ ePractice, eGovernment Factsheet – Sweden – National Infrastructure, *supra*.

¹⁶⁶ *Id.*

¹⁶⁷ *Id.*

EIDs exist as both smart cards and as files stored on the hard disk. Some issuers provide one or the other, whereas some give the option to choose the form of the eID. EIDs are issued in two ways: by ordering and downloading them from the user's Internet bank while logged in (and thus identified by the bank), or by ordering the eID on the Internet. If the eID has been ordered via an Internet bank and is issued on a smart card, the user will need to collect the eID at a bank or post office, showing a physical ID. As eIDs are issued by different suppliers, the authority that provides e-services must be able to authenticate users, verify e-signatures, and apply for revocation checks in different ways and via different eID-suppliers.¹⁶⁸

Several e-Government applications and services require the use of such eIDs. These include: income tax declarations and submissions of tax or VAT returns online; parental services delivered by the Swedish Social Insurance Agency; registration of a new company to the Companies Registration Office; application for and renewal of a driver's licence; and registration and de-registration of vehicles. The Swedish eID is becoming more and more well-known and established as the means to authenticate the user and for the user to sign electronically in e-Government applications.¹⁶⁹

OPEN GOVERNMENT

Sweden is a country that has traditionally adhered to the Nordic tradition of open access to government files. The world's first freedom of information act was the *Riksdag's* (Swedish Parliament's) Freedom of the Press Act of 1766. The Act required that official documents should "upon request immediately be made available to anyone making a request" at no charge. The Freedom of the Press Act is now part of the Constitution and provides that "every Swedish citizen shall have free access to official documents." Restrictions in several situations are stipulated in the Secrecy Act.¹⁷⁰ Decisions by public authorities to deny access to official documents may be appealed to general administrative courts and, ultimately, to the Supreme Administrative Court. The Parliamentary Ombudsman has some oversight functions for freedom of information.

OTHER RECENT FACTUAL DEVELOPMENTS

A new political party, the Pirate Party, dedicated to "reform of copyright laws, the abolishing of patents and working against installing more regulations, and remove the Data Retention Act, that are seriously threatening citizens' privacy" is "making a bid for representation in the Swedish parliament in the upcoming national elections in September."¹⁷¹ After success in the elections for the European Parliament in 2009, the party now aspires to similar results in the national elections. Based on recent experiences

¹⁶⁸ *Id.*

¹⁶⁹ SFS 1980:100.

¹⁷⁰ Piratpartiet, Introduction to Politics and Principles, at http://www.piratpartiet.se/the_pirate_party.

¹⁷¹ However, at the time of writing it seems that a new right-wing populist/extremist party, the Sweden Democrats, will enter the parliament in the 2010 elections.

of the difficulty of establishing new parties in the Swedish party system (such as the poor result of the Feminist Initiative in the 2006 elections and the right-wing populist party New Democracy in the 1990s), this ambition may be difficult to achieve.¹⁷² Without a doubt, the FRA spectacle and the Pirate Bay trial, as discussed above, contributed massively to the good result of the Pirate Party in the EU election. The Swedish debate has, however, cooled off somewhat and the privacy issue has been pushed off the agenda by the current financial crisis and labour market policy.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK ON PRIVACY

No specific information has been provided under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Sweden has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and to its First Optional Protocol that establishes an individual complaint mechanism.¹⁷³

Sweden is a member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁷⁴ It has also signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108)¹⁷⁵ and its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181).¹⁷⁶ Sweden signed, but has not ratified, the Council of Europe Convention on Cybercrime (ETS No. 185).¹⁷⁷ An additional protocol to the Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems was signed on 28 January 2003.

In 2006, the European Court of Human Rights (ECtHR) examined the power of SÄPO (*Säkerhetspolisen*, the Security Police) to compile, register, and save information about individuals.¹⁷⁸ The applicants – a journalist, a peace activist, a political activist, and a

¹⁷² Sweden signed the ICCPR and its First Optional Protocol on 29 September 1967 and ratified the on 6 December 1971. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹⁷³ Signed 28 November 1950, ratified 4 February 1952, entered into force 3 September 1953.

¹⁷⁴ Signed, 28 January 1981, ratified 29 September 1982; entered into force 1 October 1985.

¹⁷⁵ Signed and ratified 8 November 2001, entered into force 1 July 2004.

¹⁷⁶ Signed 23 November 2001.

¹⁷⁷ European Court of Human Rights, App. No. 62332/00, 6 June 2006, *Segersted-Wiber and others v. Sweden*.

¹⁷⁸ European Court of Human Rights, App. No. 62332/00, 6 June 2006, *Segersted-Wiber and others v. Sweden*.

member of the European Parliament – requested access to their files but were refused on the grounds of national security. The ECtHR found that maintaining files on the applicants was in violation of Article 8 (the right to respect for private and family life) because the file was not "necessary in a democratic society." The Court held that SÄPO's refusal to grant the applicants full access to their files did not violate Article 8 and accepted the government's reason citing national security. The ECtHR also held that the registration of the applicant's information violated articles 10 (freedom of expression) and 11 (freedom of association and assembly), since the information concerned political opinion, membership in political parties, and political activities. Lastly, the Court found a violation of Article 13 (the right to an effective remedy) since none of the relevant national authorities were able to order the deletion of the files.

Sweden is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

*Updates to the Swedish Report published in the 2010 edition of EPHR have been provided by: Ola Svenonius, Ph.D student at Södertörn University, Sweden.

SWISS CONFEDERATION (SWITZERLAND)

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 36(4) of the 1874 Constitution guaranteed, "[t]he inviolability of the secrecy of letters and telegrams." This constitution was repealed and replaced by public referendum in April 1999. The new Constitution, which entered into force on 1 January 2000, greatly expanded the older privacy protection provision. Article 13 of the new Constitution states: "All persons have the right to the respect of their private and family life, home, mail and telecommunications. All persons have the right to be protected against abuse of their personal data."¹

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

The Federal Data Protection Act of 1992 (*Loi fédérale sur la protection des données* or LPD) regulates personal information held by federal government and private bodies.² The Act requires that information be legally and fairly collected and places limits on its use and disclosure to third parties. Federal agencies must register their databases. Private companies must register if they regularly process sensitive data or transfer the data to third parties. Transfers to other nations must be registered and the recipient nation must have adequate data protection laws. Individuals have a right of access to correct inaccurate information. There are criminal penalties for violations. In March 2006, the Federal Parliament adopted major revisions to the LPD;³ the revisions came in force on 1 January 2008.⁴

Revisions to the LPD included: elimination of the possibility of justifying a violation of the principles on the basis of an overriding private or public interest; requirement that processors of sensitive data actively notify data subjects; further requirements for controllers to ensure that third party processors have adequate security in place; and

¹ Constitution of Switzerland, 1999, "Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999" (BV, SR 101), <http://www.admin.ch/ch/d/sr/c101.html>. In addition to the Constitution, every federal law and regulation is available in an online directory. In this report, we generally link to the German versions ("Systematische Rechtssammlung" SR: <http://www.admin.ch/ch/d/sr/sr.html>). However, there are versions available in French ("Recueil systématique du droit fédéral" (RS), at <http://www.admin.ch/ch/f/rs/rs.html>) and in Italian ("Raccolta sistematica del diritto federale," at <http://www.admin.ch/ch/i/rs/rs.html>).

² Bundesgesetz über den Datenschutz, DSG vom 19 Juni 1992 (Stand 2006) (Swiss Data Protection Statute from 19 June 1992 (in the updated version of 2006) DSG, SR 235,1), available at <http://www.edoeb.admin.ch/org/00828/index.html?lang=enFDPIC>.

³ David Rosenthal, "Country Q & A – Switzerland," Information Technology 2007-2008, available at http://www.homburger.ch/fileadmin/publications/DAPSWQAC_01.pdf.

⁴ See <http://www.admin.ch/ch/d/sr/2/235,1.de.pdf>.

restriction on the methods of ensuring adequate data protection in transfers to third countries.⁵

Almost all of the 26 Swiss "cantons" (states) have a separate data protection law and their own data protection commissioner. However, as some cantons are small, some data protection commissioners are employed to allocate only 10 percent of their working time for this purpose. In order to exchange opinions and collaborate, the cantonal data protection officers founded the association "PRIVATIM" (formerly DSB+CPD.CH) in March 2000. PRIVATIM created a working group to address questions regarding health privacy, and in June 2007, published a brochure on the rights of individuals concerning their medical data privacy.⁶

In June 1999, the European Union Article 29 Data Protection Working Party determined that Swiss law was adequate under the EU Data Protection Directive.⁷ In July 2000, the European Commission formally adopted this position, thereby approving all future personal data transfers to Switzerland. On 20 October 2004, the Commission confirmed this approval.⁸

In 2008, amendments to the Federal Data Protection Act came into force on 1 January. The new law incorporates the obligation to inform data subjects about the collection and purpose of the information, as well as information about data transfers to third parties.⁹ The new statute also makes a provision for a certification procedure to obtain a data protection quality label, once applicable legal and technical requirements have been met.¹⁰ The new Act modifies the rules applicable to the transfer of personal data abroad and makes it an obligation for data controller transferring personal data to inform the Data Protection Commissioner about contracts and internal data protection regulations in

⁵ *Id.*

⁶ Association of Data Protection Commissioners "PRIVATIM," at <http://www.privatim.ch/>. See "Votre dossier médicale, vos droits", 28 June 2007, available at http://www.privatim.ch/content/pdf/PRIVATIM_Dossier-medical_F.pdf.

⁷ Article 29 Data Protection Working Party, Opinion No. 5/99 on the Level of Protection of Personal Data in Switzerland, 7 June 1999, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp22en.pdf.

⁸ Commission of the European Communities, The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, SEC (2004) 1322, Brussels, 20 October 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1322.... The decision is based on the Commission Decision of 26 July 2000 pursuant to Directive 1995/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304), 2000/518/EC, Official Journal L 215, 25 August 2000, at 1-3. See also European Union Press Release, "Commission Adopts Decisions Recognising Adequacy of Regimes in United States, Switzerland and Hungary," 27 July 2000.

⁹ IWG Country Report – Switzerland, 43rd Meeting of the Working Group, March 2008.

¹⁰ Verordnung über die Datenschutzzertifizierungen, available at <http://www.admin.ch/ch/d/as/2007/5003.pdf>. For more information about the certification procedure mentioned in the text, see <http://www.seco.admin.ch/sas/00026/00059/index.html?lang=en>.

place. The new rules are very similar to the rules of the EU Data Protection Directive and their adoption allowed Switzerland to ratify, on 20 December 2007, the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001.¹¹

Sector-based laws

Besides the Data Protection Act,¹² there are also legal protections for privacy in the Civil Code¹³ and the Penal Code.¹⁴ There are also special rules relating to workers' privacy from surveillance,¹⁵ telecommunications information,¹⁶ health care statistics,¹⁷ professional confidentiality, including medical, and legal data,¹⁸ medical research,¹⁹ and identity cards.²⁰

¹¹ Id. See also Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr (Sammlung der Europaratsverträge SEV-Nr. 181), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=8&DF=06/07/2010&CL=GER>.

¹² For an overview of legal regulations concerning data protection, see <http://www.admin.ch/ch/d/sr/23.html#235>.

¹³ Section 28 of the Zivilgesetzbuch (ZGB, SR 210), Civil Code, 10 December 1907, available at <http://www.admin.ch/ch/d/sr/c210.html>.

¹⁴ Code pénal, Titre troisième: Infractions contre l'honneur et contre le domaine secret ou le domaine privé, Art. 173-179. Schweizerisches Strafgesetzbuch (StGB) vom 21. Dezember 1937 (SR 311,0), available at http://www.admin.ch/ch/d/sr/c311_0.html.

¹⁵ Section 328 of the Obligationenrecht (Code of Obligations), 1 July 1996,, available at <http://www.admin.ch/ch/d/sr/2/220.de.pdf>. See International Labour Organisation, Conditions of Work Digest, Volume 12, 1/1993.

¹⁶ Fernmeldegesetz (Telecommunications Law, LTC) (FMG, SR 784,10), 30 April 1997, available at http://www.admin.ch/ch/d/sr/c784_10.html.

¹⁷ Office fédéral de la statistique, La protection des données dans la statistique médicale, 1997, at http://www.bfs.admin.ch/bfs/portal/fr/index/infothek/erhebungen__quellen/blank/blank/mkh/02.Document.90754.pdf.

¹⁸ Code pénal, Art. 320-322, Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB, SR 311,0), available at http://www.admin.ch/ch/d/sr/c311_0.html.

¹⁹ Verordnung vom 14. Juni 1993 über die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung (VOBG, SR 235,154), available at http://www.admin.ch/ch/d/sr/c235_154.html, Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale (OALSP).

²⁰ Bundesgesetz vom 22. Juni 2001 über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG, SR 143,1), available at http://www.admin.ch/ch/d/sr/c143_1.html, and the corresponding regulation Verordnung vom 20. September 2002 über die Ausweise für Schweizer Staatsangehörige (Ausweisverordnung, VAwG, SR 143,11), available at http://www.admin.ch/ch/d/sr/c143_11.html, replacing the older Ordonnance du 18 mai 1994 relative à la carte d'identité suisse.

DATA PROTECTION AUTHORITY

The LPD created the office of a Federal Data Protection and Information Commissioner (the Commissioner, or FDPIC).²¹ The Commissioner maintains and publishes the Register for Data Files, supervises federal government and private bodies, provides advice, issues recommendations and reports, and conducts investigations. The Commissioner has assumed a new role as mediator relating to transparency and public information.²² The Commissioner also consults with the private sector. The office publishes a detailed annual report, as well as leaflets, summaries of press articles and critical statements, and advice to government agencies on issues of data protection.²³ However, the Commissioner has only limited possibilities for interventions: he can only submit "suggestions" (*Empfehlungen*) or ask the Data Protection Commission to review a case. Decisions of this commission can then be submitted to the Federal Court (*Bundesgericht*). In the FDPIC's 14th Annual Report (2006/2007), the Commissioner addresses issues that range "from military information systems, such as reconnaissance drones, to the planned introduction of the health insurance card, to video surveillance in stores, and to biometric access control in sports stadiums and leisure facilities."²⁴ In the FDPIC's 17th report main topics are "Privacy on Internet" (*Goldgräberstimmung im Internet - das Ende der Privatsphäre?*) dealing with Google, Facebook, Twitter and other online services providers; "Certification of Data Management Systems: Accreditations" (*Zertifizierung von Datenschutzmanagementsystemen: Akkreditierungen*) dealing with the first accreditations of private companies with the Swiss Accreditation Agency (SAS); and "2010 Swiss population Census" (*Volkszählung 2010*).

Annually, the FDPIC deals with 1,500 to 2,000 complaints, investigations, and requests. Among these, there are questions of individuals, media inquiries, long-term supervision of operational proceedings in private enterprises, as much as, in the federal administration, and comments on legislation at the hearing stage. According to the FDPIC, between 1 April 2005 and 31 March 2006 it conducted 63 official investigations, 50 of which concerned access to homeland security files. From 2006 to date there has been any significant change in the number of complaints (page 110 of report). However,

²¹ Official website, at <http://www.edoeb.admin.ch/index.html?lang=en>.

²² 14th Annual Report on Activities, Federal Data Protection and Information Commissioner, 2006-2007, available at <http://www.news-service.admin.ch/NSBSubscriber/message/en/13377#>. A summary of the FDPIC's annual reports is provided in English at <http://www.edoeb.admin.ch/dokumentation/00445/00509/01615/index.html?lang=en>.

²³ 13th Annual Report, Federal Data Protection and Information Commissioner, 2005-2006, available at <http://www.edoeb.admin.ch/dokumentation/00445/00509/00965/index.html?lang=en>.

²⁴ 14th Annual Report 2006-2007, *supra*.

the staff of 25 employees seems not to be sufficient to deal with all complaints in a reasonable time.²⁵

In September 2005, the FDPIC hosted the 27th International Conference of Data Protection and Privacy Commissioners in Montreux. More than 350 participants from all over the world took part, and the Conference adopted two important resolutions: one on the use of biometric data in passports, ID cards, and travel documents, and a second on the use of personal data for political communication.²⁶

The Federal Data Protection and Information Commissioner has been appointed by the *Bundesrat* (the Government), as well as cantonal commissioners have been appointed by their cantonal governments. In order to implement Article 25 of the EU Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters – that states "These authorities [*data protection authorities*] shall act with complete independence in exercising the functions entrusted to them"²⁷ – adaptations in the concerning Swiss regulations are currently under way. All commissioners must be elected by the Parliament, or at least approved by this institution.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

The relevant case law concerning privacy and data protection is discussed *infra* in the text and categorised under the corresponding section.²⁸

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

The Swiss police system is traditionally strongly organised by the 26 cantons. Every canton has its own police force. However, in the last few years there have been substantial efforts to build up a central "Federal Police" corps (Fedpol), based in Berne.²⁹ Fedpol has mainly investigative duties. For this purpose, a Federal Criminal

²⁵ See 17th Annual Report 2009-2010, Federal Data Protection and Information Commissioner, available at <http://www.edoeb.admin.ch/dokumentation/00445/00509/01615/index.html?lan....> See the German full text version at <http://www.edoeb.admin.ch/dokumentation/00445/00509/01615/index.html?lang=de&download=M3wBPgDB/8ull6Du36WenojQ1NTTjaXZnqWfVpzLhmfhnapmmc7Zi6rZnqCkkIN1gnyAbKbXrZ6lhuDZz8mMps2gpKfo>.

²⁶ 13th Annual Report 2005-2006, *supra*.

²⁷ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML>.

²⁸ *Cfr.* Section "Wiretapping, access to, and interception of communications," *infra*.

²⁹ See <http://www.fedpol.ch>, with an impressive organization chart (displayed in German), at http://www.fedpol.admin.ch/content/dam/data/fedpol/visio-fedpol-ab_01012010-d-stand021209.pdf.

Police has been built up since 1994.³⁰ Other duties include the "prevention" of crimes. Fedpol publishes an annual report on "national security."³¹ Most of the expansion of Fedpol has been done in order to "fight against organised crime and terrorism."

Although the cooperation has been extended in various fields, there have been some tensions between Fedpol and cantonal police forces, and also inside governmental agencies. Therefore, the Controlling Commission of the Swiss Parliament (*Geschäftsprüfungsdelegation*, GPDeI) demanded more efficient coordination of the different intelligence agencies of the Swiss Army and the Federal Police.³² With Effect from 1 January 2010, the military and domestic intelligence services are both located in the military department. Fedpol is no longer responsible for this matter.

Legally, the activities of the Fedpol are mainly based on the *Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit* (BWIS).³³ This law was enacted on 1 July 1998 following a scandal in the autumn of 1989, when members of a parliamentary investigative commission (the *Parlamentarische Untersuchungskommission*, or PUK) discovered huge databases of citizens in the premises of the Federal Police (the political police) and the Federal Prosecutor (*Bundesanwaltschaft*).³⁴

Wiretapping, access to, and interception of communications

Whereas until 2003 interception was possible in all investigations relating to crimes and offences (crimes for which a prison sentence can be issued), the Federal Law on the

³⁰ Bundesgesetz über kriminalpolizeiliche Zentralstellen des Bundes vom 7. Oktober 1994 (ZentG, SR 360) available at <http://www.admin.ch/ch/d/sr/c360.html>.

³¹ "Bericht Innere Sicherheit der Schweiz" ("Swiss Domestic Security Report"), Annual Reports from 1999 untill 2008 available at <http://www.fedpol.admin.ch/content/fedpol/de/home/dokumentation/berichte....> The reports are edited by the Fedpol section "Service for Analysis and Prevention," ("Dienst für Analyse und Prävention", DAP), which is the political Swiss "preventive State Security Police," part of the Swiss Federal Police, ex-BUPO, "Bundespolizei".

³² See, e.g., "Für Parlamentarier gar nicht 'hervorragend'" ("For Parliamentarians Not 'Excellent'") NZZ, 22 November 2004, at 13.

³³ Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (Law Concerning Measures to Support Domestic Security), vom 21 März 1997 (BWIS, SR 120), available at <http://www.admin.ch/ch/d/sr/c120.html>.

³⁴ The commission found about 900,000 folders, called "Fichen" (hence "Fichenskandal"), on persons, most of whom were not suspected of having committed any offence. Most of the folders had to be destroyed. At this time, there was no legal basis for the collection of these folders. In 1991, a citizens' committee launched a popular initiative to abolish the political police. Surveillance should only be possible on the grounds of a criminal investigation. The vote on the initiative was postponed by the government for years. In June 1998, nine years after the scandal 75 percent of the voters said no to the initiative. The federal government had saved its political police, which since the beginning of the nineties had been completely modernised and, by 1 July 1998, received for the first time a legal basis with the Law on Measures for Maintaining Internal Security (BWIS).

Surveillance of Mail and Telecommunications (BÜPF)³⁵ prohibits any preventive interception and provides, for the first time, for a catalogue of offences. In the case of investigations of crimes and offences described in the catalogue, the department of public prosecution, with permission from the *Zwangsmassnahmerichter*, can order providers to hand over the archived data.³⁶ The same catalogue is relevant for real-time interception cases. In this case, a judge can compel a provider to install a direct connection of all telecommunications to a specialised agency *Le Service des Tâches Spéciales* the STS.³⁷ In March 2003, the catalogue of criminal offences allowing interception was extended, introducing provisions against the "financing of terrorism."³⁸

On 21 October 2003, the Federal Court decided in a unanimous vote that, in the case of wiretapping, the Federal Prosecutor has the duty to inform the persons observed after

³⁵ Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780,1) (Law on Surveillance of Post and Telephone Services (including Internet), available at http://www.admin.ch/ch/d/sr/c780_1.html (in French, Loi fédérale sur la surveillance de la correspondance postale et des télécommunications, available at www.admin.ch/ch/f/rs/c780_1.html) and its implementing decree, Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780,11), available at http://www.admin.ch/ch/d/sr/c780_11.html (in French, Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT), RS 780,11 from 31 October 2001, available at www.admin.ch/ch/f/rs/c780_11.html).

³⁶ Cfr. Section "Data retention," *infra*.

³⁷ However, this does not include communication by way of ADSL, WLAN, voice-over-IP, MMS and SMS-over-GPRS, see the article "Taube Lauscher", facts 7 October 2007, at 26. While at the beginning of the 1990s about 500 interception orders were issued annually, the number has continuously increased to about 2,000 orders since 1996 (2,138 cases). (Conseil National, Heures de Questions: Session d'hiver 1999, Réponse du Conseil fédéral concernant les écoutes téléphoniques (Answer by the Federal Council, 20 December 1999), available at <http://web.archive.org/web/20041107021645/http://www.parlament.ch/afs/da...>) To these orders, another 2,000 cases of disclosure of traffic data have to be added. Furthermore, Swiss authorities ordered 2,430 telephone taps in 2000 compared with 2,046 the previous year. More than a third of them were ordered in connection with a suspected breach in drugs law, an 18 percent increase ("Phone Tapping on the Increase," 23 July 2003, available at <http://web.archive.org/web/20050112094046/http://www.swissinfo.org/sen/S...>). In 2002, lawful interception concerned 6,646 telephones, two thirds of the mobile phones, that is 1,551 more than in 2001. Almost 3,000 real-time observations were established in 2002. The tariff for lawful interceptions according to BÜPF has been changed for 1 April 2004. For Internet Service Providers, there are only two tariffs since then. One is for requests of past data from log files and it is CHF538 flat (IP address, login number, email log). The other one is CHF1,326 flat for real-time transmission of email messages. Since it is always a flat rate no matter how long the interception (or logs, up to six months) is, some suspect that law enforcement will always opt for the maximum period just in case. Statistics for the years 1998-2003 are available at <http://www.uvek.admin.ch/kommunikation/dba/unterseite2/index.html?lang=de>. In regards to the Internet traffic, the newspaper *Sonntagszeitung* calculated a projection of about 3,000 ex-post requests per year (Michael Soukup: "Sorgen mit dem Datenhunger", *Sonntagszeitung* 30,01,2005, at 102.)

³⁸ See <http://www.admin.ch/ch/d/as/2003/3043.pdf>.

surveillance has been carried out, including information about the reasons of the monitoring.³⁹

National security legislation

After 11 September 2001, the *Bundesrat* (Government) ordered a report on security deficits in Switzerland.⁴⁰ Following this report, the Justice Department has been assigned to prepare a revision of BWIS by the *Bundesrat* on 20 October 2004.

In July 2005, an internal consultation procedure was held with a first draft. One of the addressees was the Federal Data Protection and Information Commissioner.⁴¹ The first draft has been rejected after the internal consultation procedure. A second draft was published on 31 January 2006, and a public consultation procedure was held.⁴² The result of the public consultation procedure was very negative.

In April 2007, at the end of a year-long consultation process, the *Bundesrat* announced its intention to move ahead with a proposal to allow the Swiss secret services to be able to carry out communications surveillance – correspondence, telephone, and email – and observe private areas such as hotel rooms, if necessary by installing bugging devices. Proponents stated that the interception amendment would only concern cases that dealt with terrorism, weapons of mass destruction and spying. They would only be taken as a last resort and their legality checked beforehand. Critics from both the left and the right parties voiced concerns with the proposal, and the Data Protection Commissioner stated that the proposed changes are "dangerous because eavesdropping on citizens within their private sphere could take place without any criminal allegations."⁴³ The revision will allow to spy inside private apartments or to tap telecommunications, even without the specific suspicion of a crime. Further, the discussed revision should include the possibility to operate secret "undercover agents" (*verdeckte Ermittler*), even for the means of "prevention," that is, in cases where no specific crime is under

³⁹ Federal Court, BGE 8G,109/2003 of 21 October 2003.. There have been numerous public revelations of illegal wiretapping. A 1993 inquiry found that phones used by journalists and ministers in the Swiss Parliament were tapped (Statewatch bulletin, Volume 3, Number 1, January-February 1993). The Data Protection Commissioner also accused Swisscom (Telecom PTT at that time), the state telephone company, of illegally wiretapping telephones. In February 1998, an agent for Israel's Mossad Secret Service was arrested by the Swiss authorities for attempting to tap the phone of a Lebanese immigrant whom he believed had links to the Hezbollah. On 7 July 2000 the Swiss court handed down a one-year sentence to be suspended for two years ("Swiss Court Hands Mossad Spy a Suspended One-year Sentence," Associated Press, 10 July 2000). See also the section "National security legislation", *infra*.

⁴⁰ Lage - und Gefährdungsanalyse Schweiz nach den Terroranschlägen vom 11. September 2001, Bericht des Bundesrates an das Parlament vom 26. Juni 2002, available at <http://www.admin.ch/ch/d/ff/2003/1832.pdf>.

⁴¹ At <http://www.edoeb.admin.ch/dokumentation/00445/00509/00965/00978/index.html?lang=de>.

⁴² At http://www.ejpd.admin.ch/content/dam/data/sicherheit/bwis/vorentwurf_bwis_ii.pdf.

⁴³ "Anti-terror Phone Tap Plan to Continue," SwissInfo, 4 April 2007, at <http://www.swissinfo.org/eng/swissinfo.html?siteSect=881&sid=7688550>.

investigation.⁴⁴ The majority of the Parliament accepted the governmental proposal, arguing that this would have been "a necessary tool against organised crime," like terrorism and money laundering.

On 28 April 2009, the revision of BWIS, formally presented to the Parliament on 15 June 2007, was rejected by the Parliament.⁴⁵ However, the *Bundesrat* had already announced a further attempt at the revision. Officially, the events of 11 September 2001 was the reason for the BWIS revision, but the directors of the Federal Police and Intelligence forces demanded more power much earlier than this.

On the legal basis of the BWIS, the government decreed a regulation which compels all institutions "executing an official duty" to report any suspicion of "terrorist activity" to the federal police.⁴⁶ These institutions include universities, hospitals, and train carriers. The regulation was first released on 1 November 2001, in the aftermath of the attacks of 11 September 2001, to sunset after one year. It was extended for another year, and in November 2003 was extended for two more years.⁴⁷ The regulation is now valid until 31 December 2011.⁴⁸

Since 1 January 2005, the police have been allowed to operate as undercover special agents. The law dealing with undercover agents passed Parliament on 20 June 2003 and has been in force since 1 January 2005.⁴⁹ All investigations under this law require advance approval from a judge. Approval is only granted, if specific suspicion of a crime is proven by police. Undercover investigation is only applicable to severe crimes.⁵⁰ From 1 January 2011, the judge for approval of undercover investigation (as well as post-telephone-Internet surveillance and investigative custody) will be the *Zwangsmassnahmenrichter* in all cantons due to the new Criminal Procedure Code.⁵¹

⁴⁴ See, e.g., Markus Steudler: "Der Staat will wieder lauschen" ("The State Plans to Be Big Eared Again"), *NZZ am Sonntag*, 1. Mai 2005, at 11, <http://web.archive.org/web/20060511162756/http://www.nzz.ch/2005/05/01/il/articleCRX8R.html>.

⁴⁵ See <http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2007/2007-06-15.html>.

⁴⁶ Verordnung betreffend die Ausdehnung der Auskunftspflichten und des Melderechts von Behörden, Amtsstellen und Organisationen zur Gewährleistung der inneren und äusseren Sicherheit (SR 120,1) (Regulation on the Extent of Disclosure Requirements and Reporting Laws by Public Officers, Agencies, and Organisations to ensure the Internal and External Security).

⁴⁷ In Switzerland, citizens can demand a referendum on every law regarding domestic politics by collecting 50,000 signatures within 100 days. However, they cannot ask for a referendum in the case of a regulation (Verordnung, decree).

⁴⁸ See http://www.admin.ch/ch/d/sr/c120_1.html.

⁴⁹ Bundesgesetz über die verdeckte Ermittlung (Federal Law on Undercover Investigation), vom 20. Juni 2003, available at <http://www.admin.ch/ch/d/as/2004/1409.pdf>.

⁵⁰ *Id.* and the regulation (decree) Verordnung vom 10. November 2004 über die verdeckte Ermittlung (VVE, SR 312.81), available at http://www.admin.ch/ch/d/sr/c312_81.html.

⁵¹ S Schweizerische strafprozessordnung, vom 5 Oktober 2007, available at http://www.irm.unibe.ch/unibe/medizin/irm/content/e7670/e7868/Eidg.StPO_ger.pdf.

In preparation for the European Football Championship (TM) of 2008 in Switzerland and Austria, the new anti-hooliganism law came into force on 1 January 2007. With a sunset at the end of 2009, it introduced stadium bans, a national hooligan database, travel restrictions for known troublemakers, and increased police powers.⁵² However, critics feared that the term "hooliganism" would not be restricted to football fans, since the law covers all kinds of "large public events", including political demonstrations. The National Swiss Security Strategy for EURO 2008 discussed a number of "risk situations" associated with the event, from terrorism to human trafficking and forced prostitution.⁵³ On 1 January 2010, the *Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen* (Agreement on Measures against Violence linked to Sport Events) came into force. The law carries over the prior regulations against hooliganism.⁵⁴

Data retention

Swiss telecom providers have to keep a log for six months of all communications traffic data to comply with the Federal Law on the Surveillance of Mail and Telecommunications (BÜPF).⁵⁵ This law requires that the respective telephone companies constantly track phones and store the data collected.⁵⁶

In a March 2004 revision of the Penal Code (*Strafgesetzbuch*), commercial companies are allowed to keep logs of phone conversations with their clients, even without their consent, for the purpose of securing evidence. However, they are not allowed to analyse this data for marketing purposes, or to give this data to third parties.⁵⁷

On 19 May 2010 the *Bundesrat* started a consultation procedure for a revision of the BÜPF.⁵⁸ Telephone and Internet data must be stored for 12 instead of six months, Internet hosting providers must keep logs for 12 months, and police will be allowed to install

⁵² "EURO 2008 Tickets Up For Grabs," 28 February 2007, SwissInfo, http://www.swissinfo.org/eng/front/detail/Euro_2008_tickets_up_for_grabs.html?siteSect=105&sid=7574130.

⁵³ The National Swiss Strategy for EURO 2008, Public Authorities Project Organisation, March 2007, available at <http://64,233,169,104/search?q=cache:OlUqnkXffB0J:www.switzerland.com/files/%3Fid%3D2086+switzerland+hooligan+face+surveillance&hl=en&ct=clnk&cd=3&gl=us#24>.

⁵⁴ The National Swiss Security Strategy for UEFA EURO 2008, at http://www.baspo.admin.ch/internet/baspo/de/home/themen/sportanlaesse/euro08_neu/english_documents.parsys.46386.downloadList.99305.DownloadFile.tmp/nationalessicherheitskonzepte.pdf.

⁵⁵ Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780,1), *supra*.

⁵⁶ *Cfr.* Section "Wiretapping, access to, and interception of communications", *supra*.

⁵⁷ Presumably with the exception of giving away such data to investigating police forces, in case a judge ordered it. See: Änderung des Art. 179 quinquies StGB, Abs. 1, Bst. b) vom 1. März 2004 (AS 2004 823). Schweizerisches Strafgesetzbuch (Code pénal) vom 21. Dezember 1937 (SR 311,0), available at http://www.admin.ch/ch/d/sr/c311_0.html, with the new article 179 quinquies, <http://www.admin.ch/ch/d/as/2004/823.pdf>.

⁵⁸ See <http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2010/2010-05-19.html>.

Trojan horses and worms on private computers to gain passwords and monitor encrypted traffic like PGP (email encryption) or Skype (Internet telephony). Furthermore, Internet service providers must be able to assign every transaction to a specific person and the provider of an Internet cafe or a hotel must be able to distinguish between different guests. The consultation ends on 18 August 2010, but there is already significant opposition. As seen in the BWIS case, the *Bundesrat* will forward this revision to the Parliament anyway, but on current indications most probably the bill will not pass.

National databases for law enforcement and security purposes

The former Federal Police, now called the Service for Analysis and Prevention, is part of the Federal Office for Police Matters, which also includes the Federal Criminal Police. It hosts two databanks, ISIS, the Information System for Internal Security, which replaced the old paper files of the federal police, and JANUS.⁵⁹ In April 2004, ISIS contained files on 60,477 persons who are considered terrorists, violent extremists or possible spies.⁶⁰ Files are opened on "preventive" grounds, which means that no criminal investigation is required. However, data resulting from criminal investigations, and thus also from telephone surveillance, can be maintained for preventive purposes, even if the person is acquitted before a court.

After the disclosure of the registration with ISIS of some local parliament members in Basel, as well as reporters and a newspaper, the Committee for Inspection of Special Affairs (*Geschäftsprüfungsdelegation* or GPDel) started an investigation of ISIS in 2008. In its report released on 21 June 2010, the GPDel stated that 200,000 records are stored in ISIS. Many of the records do not comply with legal rules for storage.⁶¹

The other databank, JANUS,⁶² contained files of 62,500 persons in July 2001 and 83,700 in March 2004. Most of them were registered for alleged drug trafficking, since registration of consumers is not allowed. Files in JANUS can be created on the grounds of simple suspicion. In July 2001, the records on the 62,500 suspected target persons

⁵⁹ ISIS: Verordnung über das Staatsschutz-Informationssystem (ISIS-Verordnung) (Regulation for State Security Information System), vom 30. November 2001 (SR 120.3), available at <http://www.admin.ch/ch/d/as/2001/3173.pdf>.

⁶⁰ Heiner Busch, "Das neue Schweizer Wettfichen" ("The New Swiss File Competition"), *WOZ Die Wochenzeitung* nr. 9, 3 March 2005, at 6.

⁶¹ "Datenbearbeitung im Staatsschutzinformationssystem ISIS Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte" ("Report of the Management Delegation of the Federal Assembly on Data Processing in the National Security Information System ISIS"), vom 21. Juni 2010, available at <http://www.parlament.ch/d/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/isis-inspektion/Documents/bericht-gpdel-isis-2010-06-21-d.pdf>.

⁶² Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung) vom 30. November 2001 (Stand am 22. Januar 2002) (SR 360.2), available at http://www.admin.ch/ch/d/sr/c360_2.html. JANUS is the fusion of three information systems that have been built up during the 1990s, and had been maintained separately until 1998: DOSIS, which held data on investigations in drug trafficking; ISOK, the information system on "organised crime"; and FAMP, which includes information about forged money, trafficking in human beings (prostitution), and illicit pornography.

(*Stammpersonen*) also contained 116,500 references to third persons who are not suspected.⁶³ More recent statistics are not publicly available.

The database GEWA of the Fedpol section on money laundering (*Meldestelle Geldwäscherei*) contained 10,884 persons and 4,170 companies in February 2004.⁶⁴ The database for "searched people and objects" (*Fahndungsdatenbank*) RIPOl contained 142,625 entries for persons in January 2004, most of them being searched for minor offences.⁶⁵ In February 2004, the main Fedpol register IPAS (*Personen- und Aktennachweissystem* or People and File Identification System) contained entries on 641,446 persons.⁶⁶ IPAS is organised as an index to other databases, including the database of fingerprints AFIS and of genetic profiles EDNA (see below).⁶⁷

On 31 December 2009 32,343 sets of two fingerprints and 726,347 sets of ten fingerprints as well as 52,069 unidentified samples from crime locations were stored in AFIS.⁶⁸ At the same time 115,000 DNA-profiles were stored.

A draft for a new law on federal information systems for police was published in 2009.⁶⁹ The different data bases for police matters should be linked to a new "police index". The Parliament will discuss this bill in late 2010 or early 2011. There is substantial opposition to the new law.

Finally, the police forces also demanded access to ONYX, the Swiss military satellite telecom interception system similar to ECHELON (see above).

National and international data disclosure agreements

There are several bilateral agreements on police cooperation between Switzerland and many other nations in Europe, which expand the types of collaboration among law enforcement authorities. The Swiss Federal Police is, in this regard, exchanging

⁶³ Among them, 13,500 are so-called "contact persons"; 13,000 are telephone subscribers (with their names and addresses); and about 90,000 are telephone numbers with only fragmentary information@@ to the respective persons. See Conseil national 01-1068 – Question ordinaire de Dardel – Personnes enregistrées dans les systèmes de données JANUS et ISIS – Réponse du Conseil fédéral du 5 septembre 2001.

⁶⁴ Heiner Busch, "Das neue Schweizer Wettfichen," *supra*, at 6.

⁶⁵ The acronym RIPOl stands for "le système de recherches informatisées de police." see Verordnung über das automatisierte Fahndungssystem(RIPOl-Verordnung, SR 172,213.61) vom 19.Juni 1995, see <http://www.admin.ch/ch/d/gg/cr/1995/19950164.html>.

⁶⁶ IPAS is an acronym for "informatisiertes Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei" based on the IPAS-Verordnung vom 21.November 2001 (SR 361,2), see http://www.admin.ch/ch/d/sr/c361_2.html.

⁶⁷ Heiner Busch, "Das neue Schweizer Wettfichen", *supra*, at 6.

⁶⁸ See http://www.ejpd.admin.ch/ejpd/de/home/themen/sicherheit/ref_personenidentifikation/ref_fingerabdruecke/ref_die_datenbank.html.

⁶⁹ Bundesgesetz über die polizeilichen Informationssysteme des Bundes, available at <http://www.admin.ch/ch/d/ff/2006/5093.pdf>.

information and data with other countries.⁷⁰ Concrete collaboration has been tested in the case of international political and economic meetings, like the G8 meeting in Geneva in June 2003 and the World Economic Forum meeting in Davos in January 2004. In January 2005, the Swiss government published an agreement on the collaboration with Europol, signed in September 2004. The agreement allows both parties to establish "exchange officers".⁷¹

Thousands of French and German police supported Swiss police during EURO '08 in June 2008.

Banking records are protected by the Swiss Federal Banking Act of 1934. This act was passed to guarantee strong protections for the privacy and confidentiality of bank customers. However, Switzerland has come under increasing pressure from the European Union and the Organisation for Economic Cooperation and Development (OECD) to weaken these laws and provide greater access to bank records for the purposes of tax collection. In reality, banking data have been transmitted illegally to the US in at least one case described at the end of this section.

On 17 June 2010, the Swiss Parliament approved a US-Swiss Government Agreement, which allows the Swiss Tax Administration to hand over data relating to approximately 4,450 accounts to the US Internal Revenue Service (IRS). This agreement followed a lawsuit concerning Swiss-based cross-border banking services for US private clients by UBS.⁷² On 15 July 2010, the Court for Federal Administration (*Bundesverwaltungsgericht*) rejected a complaint of a private person against a handover of data to the US IRS.⁷³

Switzerland is not a member of the EU, but has some special agreements with the EU. Some of these bilateral agreements were signed in 2000 and 2001. In May 2004, the government decided to sign another set of agreements ("Bilaterale II").⁷⁴ These contracts

⁷⁰ E.g., in April 2002, the Swiss government signed an agreement with Europol on exchanging information as well as police agents. The government promised to submit the agreement to Parliament in a later stage.

⁷¹ See Botschaft, Bundesbeschluss and Abkommen (Agreement, SR 0.360.268.2) in Bundesblatt Nr. 6/2005 of 15 February 2005, at 983ff., available at http://www.admin.ch/ch/d/ff/2005/index0_6.html.

⁷² See the Government's proposal, Botschaft zur Genehmigung des Abkommens zwischen der Schweiz und den Vereinigten Staaten von Amerika über ein Amtshilfegesuch betreffend UBS AG sowie des Änderungsprotokolls, vom 14. April 2010, available at <http://www.admin.ch/ch/d/ff/2010/2965.pdf>; the edict, Bundesbeschluss über die Genehmigung des Abkommens zwischen der Schweiz und den Vereinigten Staaten von Amerika über ein Amtshilfegesuch betreffend UBS AG sowie des Änderungsprotokolls (Federal Decision on the Approval of the Agreement between Switzerland and the United States of America on the request concerning UBS AG and the Protocol of Amendment), vom 17. Juni 2010, available at <http://www.admin.ch/ch/d/as/2010/2907.pdf>.

⁷³ See http://www.bundesverwaltungsgericht.ch/20100719_a40132010.pdf.

⁷⁴ Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen (Bilaterale II) vom 1. Oktober 2004, published in the Bundesblatt nr. 44/09 on 9 November 2004, at 5965-6564, available at http://www.admin.ch/ch/d/ff/2004/index0_44.html.

were approved by referenda, and Switzerland ratified the Schengen and Dublin Conventions on 5 June 2005.⁷⁵ Further, some EU regulations must be implemented "automatically" in the Swiss legal order, like the regulation for passports described below.

The Schengen Convention establishes close cooperation among police forces, in order to combat international "criminal tourism" (*Kriminaltourismus*). The core subject of this agreement is the Schengen Information System (SIS), a pan-European database that records personal information on people who have been arrested, migrants, and missing objects⁷⁶ (*Fahndungsdatenbank*) by the national police forces. In the summer of 2007, SIS consisted of 17 million entries. On 1 January 2010, SIS contained 31,618,951 records.⁷⁷

A second generation database, SIS II has been established in 2006/2007 but it is still not operational.⁷⁸ The SIS database is not only a tool against crime, but also a tool for enforcement of immigration conditions. By joining the Schengen *acquis*, Swiss police officers have full online access to the SIS database. The Swiss Department of Justice and Police (EJPD) calls the SIS "a revolutionary step for police work". Other parts of the Schengen Convention cover cross-border observation by national police forces and the exchange of police officers.

Data of wanted persons are transferred to SIS by the Swiss "Sirene" bureau. In 2009, Swiss police performed 183,000 queries daily in SIS, resulting in 24 hits a day. The reason for the enormous number of queries in SIS is a link from RIPOL to SIS. Every query to RIPOL is automatically passed to SIS.⁷⁹

⁷⁵ A Swiss majority of 55 percent voted to ratify the Schengen and Dublin agreements. See "Vote Takes Switzerland Closer to EU," BBC News, 5 June 2005, available at <http://news.bbc.co.uk/2/hi/europe/4612281.stm>.

⁷⁶ See http://www.fact-index.com/s/sc/schengen_information_system.html. For a critical review of the SIS see e.g. the documentation of the group "Solidarité sans frontières" (SOSF) at <http://www.sosf.ch/publikationen/intro/intro.html>, as well as Heiner Busch "Lieber Pest oder Cholera?" in *WOZ Die Wochenzeitung* Nr. 14/2004, 1 April 2004. For information on SIS in English see e.g. [statewatch.org](http://www.statewatch.org), "From the Schengen Information System to SIS II and the Visa Information (VIS): the Proposals Explained" (48 pages / February 2005), available at <http://www.statewatch.org/news/2005/may/analysis-sisII.pdf>, as well as the 12-page update of May 2005 by Statewatch.org, "SIS II fait accompli? Construction of the EU's Big Brother Database Underway - New Analysis", available at <http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf>. By checking the Governmental Report (Botschaft) on the Schengen Agreement, the data protection officer of the Canton Zug found 233 hits in his quick survey. However, this does not mean that personal data is protected. The Botschaft has been published in the *Bundesblatt* Nr. 44/2004 (9 November 2004), pp. 5965-6564, available at <http://www.admin.ch/ch/d/ff/2004/5965.pdf>. For other agreements in the same context, see http://www.admin.ch/ch/d/ff/2004/index0_44.html.

⁷⁷ See <http://www.statewatch.org/news/2010/feb/eu-council-sis-stats-6162-10.pdf>.

⁷⁸ See "European Union Report" in this survey.

⁷⁹ See <http://www.fedpol.admin.ch/fedpol/de/home/dokumentation/medieninformationen/2009/2009-08-28.html> and <http://www.fedpol.admin.ch/fedpol/de/home/dokumentation/medieninformationen/2010/2010-06-25.html>.

The Dublin Convention, created in 1990, establishes a European cooperation agreement to process applications from asylum seekers. Switzerland is now allowed to access "Eurodac," the pan-European database of fingerprints of asylum seekers and migrants.⁸⁰ According to the Dublin Convention, asylum requests are checked only by one EU member state whose decision becomes binding for all other member states.

Cybercrime

In order to "fight cybercrime" a specific task force was established in 2003, the Coordination Unit for Cybercrime Control (CYCOS).⁸¹ CYCOS was a cooperating project between the Confederation and most of the Swiss Cantons. In 2005, the Canton of Zurich decided to participate as well. According to a newspaper report, CYCOS received about 6,500 hints from the public, most of them regarding child pornography and child abuse. During 2005, CYCOS forwarded 272 cases to the competent cantonal attorneys.⁸² CYCOS has been terminated, and Fedpol is now responsible for cybercrime.⁸³

In December 2004, the Swiss government opened the consultation process on a revision of the Penal Code (*Strafgesetzbuch*, StGB),⁸⁴ which consists mainly of regulating the criminal liability of Internet providers, stating: content providers should be fully liable for documents which are prohibited by law; hosting providers should not be liable at all; while access providers should be liable only if they participate actively in offering such documents. A second consultation process has been opened on a bill aiming at centralising the investigation of cybercrime cases at the Federal Police.⁸⁵

⁸⁰ See http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_en.htm. After a revision of the regulation *Verordnung über die Bearbeitung erkennungsdienstlicher Daten* by the Swiss Government on 12 May 2004, from 1 June 2004 the Swiss border police are allowed to collect fingerprints of all persons they expect to be illegally trying to immigrate to Switzerland, and to store these data in the national database called AFIS. The revision has to be regarded as preparation for joining the Eurodac database. See *Verordnung über die Bearbeitung erkennungsdienstlicher Daten* vom 21. November 2001 (SR 361.3), available at http://www.admin.ch/ch/d/sr/c361_3.html.

⁸¹ Koordinationsstelle zur Bekämpfung der Internetkriminalität, KOBik (Coordination Unit against Cybercrime), at <http://www.kobik.ch/index.php?language=en>.

⁸² Niels Anner, "Erfolge der Internet-Polizei," *NZZ am Sonntag*, 6 February 2005.

⁸³ *Cfr.* Fedpol Annual Report 2009, available in German at http://www.fedpol.admin.ch/content/dam/data/migr_new/sicherheit___jahresbericht/jabe-2009-d.pdf.

⁸⁴ Swiss Penal Code, *Strafgesetzbuch*, SR 311.0, available in German, French, and Italian at http://www.admin.ch/ch/d/sr/311_0/index.html.

⁸⁵ See media release by the Federal Justice Departement (EJPD): "Die Netzwerkkriminalität verstärkt bekämpfen. EJPD schickt zwei Gesetzesentwürfe in die Vernehmlassung" ("Stronger Fight against Cybercrime – Justice Department Starts Consultation Procedure for Two Drafts of New Law"), 10 December 2004, <http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2004/2004-12-10.html>.

On 1 July 2008, some minor changes in the Federal law on Copyright and Related Rights came in force.⁸⁶ Private download of music and movie files is still allowed. A revision of the Penal Code concerning hacking of computers is currently under way. The handover of data gained from telephone and Internet surveillance to foreign authorities should become possible in a very early stage of investigation with the same revision.⁸⁷

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

No specific information has been provided under this section.

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

No specific information has been provided under this section.

TERRITORIAL PRIVACY

Video surveillance

More and more public transport companies are introducing CCTV in their vehicles. After a pilot test in 2002 and 2003, the Swiss Federal Railway company (SBB, now a private company, but still owned by the state) announced a large project to install surveillance cameras in trains.⁸⁸ Until 2003, such surveillance was not allowed by law, neither was the operation of CCTV systems in train stations. In December 2003, a regulation was

⁸⁶ Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, vom 9. Oktober 1992, available at <http://www.admin.ch/ch/d/sr/2/231.1.de.pdf>.

⁸⁷ See <http://www.news.admin.ch/message/index.html?lang=de&msg-id=33758>.

⁸⁸ See media release http://web.archive.org/web/20040815083056/http://www.sbb.ch/gs/press/press_0303_d.htm#210303Kameraüberwachung.

subsequently introduced, allowing the SBB to operate CCTV systems in train stations and inside trains.⁸⁹

The city police of Zurich bought a new mobile camera system with capabilities for automatic car plate recognition (AFNES) to be operated in Zurich. It will be able to identify car plates and compare the results with the national database RIPOL. Since 12 December 2008, all queries to RIPOL trigger a query in the European database SIS automatically. With effect from 1 October 2008, the guidelines for speed measurement by police have been extended to allow average speed measuring (*Abschnittsgeschwindigkeitskontrolle*).⁹⁰ A system with a set of two cameras installed along a fixed route records all front number plates using automatic number plate recognition and calculates the average speed of each vehicle. A first test system will start operation in September 2010; a second will follow later in the year.⁹¹ This pilot project is supervised by the Data Protection Authority, and no data may be used for any other purpose than speed measurement and fining of speeding drivers.

The growth of video surveillance in Switzerland is helped by the cameras getting smaller, cheaper and more sophisticated. This is especially true for the systems operated by private entities, such as shopkeepers or house owners. Also, more sport stadiums are installing CCTV cameras. However, opposition to camera surveillance is growing as well. The committee of the Swiss "Big Brother Awards" has organised several "excursions" on the subject of surveillance cameras in Zurich and released a map with camera locations in a city district of Zurich, as well as in the Zurich Main Train Station.⁹² The Federal Data Protection Commissioner published a leaflet explaining the legal conditions for private individuals to operate video surveillance cameras.⁹³

The Swiss Air Force started operating Unmanned Aerial Vehicles (*Drohnen*, UAV) of the type "ADS 95 Ranger." They are produced in Switzerland by the company RUAG in Emmen (Lucerne), in collaboration with Israeli companies. On 6 January 2004, on a test flight, a military UAV observed a civilian car driving into a forest near Lucerne. The operators informed the local police patrol, who apprehended the car's passengers for

⁸⁹ Verordnung über die Videoüberwachung durch die Schweizerischen Bundesbahnen SBB (Videoüberwachungsverordnung SBB, VüV-SBB) SR 742.147.2, http://www.uvek.admin.ch/imperia/md/content/gs_uvek2/d/verkehr/schienenverkehr/vuev/1.pdf.

⁹⁰ Weisungen über polizeiliche Geschwindigkeitskontrollen und Rotlichtüberwachung im Strassenverkehr, available at http://www.astra.admin.ch/dokumentation/00117/00208/01640/index.html?lang=de&download=NHZLpZeg7t,lnp6I0NTU042I2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDd4R3gGym162epYbg2c_JjKbNoKS6A.

⁹¹ See <http://www.astra.admin.ch/00638/index.html?lang=de&msg-id=34214>.

⁹² See <http://www.bigbrotherawards.ch/kameras/>.

⁹³ See <http://web.archive.org/web/20050208162644/http://www.edsb.ch/e/doku/merkblaetter/video.htm>.

smoking marijuana.⁹⁴ According to a media report, the Swiss Air Force is operating one to four UAV test flights every day. The images of the cameras are recorded and stored for up to six months. During the 2008 European Football Championship, drones were used for traffic and crowd control. No attempts at face or car plate recognition were made.⁹⁵ In total, 37 operations over 100 hours were performed in Basel, Bern, and Zürich. There were some complaints due to noise.⁹⁶

In honour of this privacy invasion, the Air Force received one of four Swiss "Big Brother Awards 2004".⁹⁷ On Easter Holiday 2005, the Army offered their UAVs to cantonal police forces in order to observe north-south traffic on the Gotthard route. For the celebration of International Worker's Day on 1 May 2004, the Zurich police asked the Air Force about using UAVs to observe the rally in Zurich from the air. These examples show strengthened collaboration between military and police forces.

For many years there has been no formal legal basis governing the use of army reconnaissance drones by the border police. At the request of the Commissioner, the Federal Council finally agreed to remedy this legal shortcoming and to also regulate the use of surveillance equipment for civilian purposes. The Commissioner has pointed out that the legal rules covering military information instruments need to be highly specific, and should cover not just the actual surveillance devices, but also the type and purpose of the surveillance.⁹⁸ Since 1 January 2010 the Federal Law on Military Information Systems (*Bundesgesetz über die militärischen Informationssysteme* or MIG) is in force. Its article 180 is the legal basis for drones.⁹⁹

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this section.

⁹⁴ See "Von der Luftwaffe beim Kiffen erwischt" ("Caught Smoking Shit by the Air Force"), *NZZ am Sonntag* on 23 May 2004, at <http://www.nzz.ch/2004/05/23/il/page-article9M50A.html> (in German). During the Olympic Games in Athens, Greece in the summer 2004, Swiss surveillance "Zeppelins" were used to observe the city.

⁹⁵ See the Final Report of the Organisation Committee, at 48, at http://www.baspo.admin.ch/internet/baspo/de/home/das_baspo.html.

⁹⁶ "Drohnen waren über 100 Stunden in der Luft" ("Drones were flying for 100 hours"), *NZZ Online*, 1 June 2008, at http://www.nzz.ch/nachrichten/schweiz/armee_zieht_bilanz_ueber_drohnenfluege_waehrend_der_euro_08_ueber_host_cities__1.773617.html.

⁹⁷ See <http://www.bigbrotherawards.ch/2004/>.

⁹⁸ 14th Annual Report 2006-2007, *supra*.

⁹⁹ Bundesgesetz über die militärischen Informationssysteme (MIG), vom 3. Oktober 2008, available at <http://www.admin.ch/ch/d/sr/5/510.91.de.pdf>. See also http://www.admin.ch/ch/d/sr/510_91/a180.html.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

The identity card is machine-readable, as is the new passport, which became effective on 1 January 2003. On 15 September 2004, the Swiss government decided that the next edition of Swiss passports should include a chip with biometric data. The decision was based on a feasibility study by the Federal Police "Fedpol," commissioned in September 2003. This should allow Swiss citizens to fulfil the requests introduced by the US government after 11 September 2001 requiring that every visitor without a visa be able to present a passport with a biometric identity tag.¹⁰⁰ In April 2005, the Swiss government declared that such a passport would not be available until September 2006 or later, due to the coordination of similar efforts of the European Union (EU).¹⁰¹ In September 2006 Switzerland issued its first biometric passports as part of a five-year pilot project. However, during the pilot phase, facial images were the only biometric data stored on the passports.¹⁰² The FDPIC reviewed and commented on draft revisions to the identity documents law and decree and was very critical of the plan to store biometric data in a central database.

This project has been terminated due to the new passport 2010. However, passports issued during the duration of this project remain valid.¹⁰³

Since 1 March 2010, all new Swiss passports contain two fingerprints of the holder on their chips. This change was made in accordance with the Council Regulation (EC) No. 2252/2004 of 13 December 2004 on Standards for Security Features and Biometrics in Passports and Travel Documents issued by Member States. Additionally, fingerprints are stored in a central database located at the federal police (Fedpol) office in Bern. The whole electronic data transfer must be encrypted. Data of fingerprints are available for federal and cantonal police for identification of persons only. However, no biometric data

¹⁰⁰ "Pilotprojekt für Biometrie-Pässe," ("Pilot Project for Biometric Passports"), Media release of the Justice and Police Department EJPD of 15 September 2004, available at http://web.archive.org/web/20050306192615/http://www.ejpd.admin.ch/doks/mm/content/mm_view-d.php?mmID=2192&mmTopic=Ausweise.

¹⁰¹ "Biometrischer Schweizer Pass: Einführung frühestens im September 2006" ("Swiss Biometric Passports: Launch in September 2006 or Later"), Media release of the Swiss Justice and Police Department EJPD of 13 April 2005, available at http://www.schweizerpass.admin.ch/pass/de/home/dokumentation/medienmitteilungen/2005/ref_2005-04-130.html.

¹⁰² "Introduction of Biometric Data in the New Swiss Passport," Federal Data Protection Commissioner, July 2006, <http://www.edoeb.admin.ch/dokumentation/00445/00509/00965/00980/index.html?lang=en>.

¹⁰³ See http://www.schweizerpass.admin.ch/pass/de/home/ausweise/aeltere_paessee/p... official 10-point FAQ on biometrical data in the Swiss passport is available at <http://www.schweizerpass.admin.ch/pass/de/home/dokumentation/faq.html>.

are transferred from the database. A Boolean number (true or false) is sent after a query with passport number and fingerprints has been performed.¹⁰⁴

Documents for foreigners with residency in Switzerland (*Ausländerausweis*) will contain data chips with fingerprints from 1 January 2011.¹⁰⁵

The Schengen Agreement¹⁰⁶ aims at creating a pan-European Security Zone, thus shifting the borders between European nations to the external borders of Europe. Inside Europe, people would be able to travel without the traditional border police control, while travellers from and to Europe would face strengthened border controls. However, the national police forces will be allowed to execute "mobile controls" in the 30km range along the borders, as well as in train stations, inside of trains, and at airports. The Schengen Agreement came in force on 12 December 2008. Even if the federal border police (*Grenzwachtkorps*) are allowed to perform "mobile controls", Swiss citizens are not obliged to carry a ID card.¹⁰⁷

National ID & smart cards

In May 2004, the National Council began to debate the revision of the Law on Foreigners.¹⁰⁸ The larger chamber of the Federal Parliament decided to include biometric data in foreigners' identity documents. The law would also provide a definite legal basis for the Central Register of Foreigners, which now holds data on about 4.5 million persons. In order to avoid so-called "faked marriages" (*Scheinehen*), the law provides that marriage officers (*Zivilstandsbeamte*) would be allowed to investigate the "honesty" of bi-national marriages. In June 2004, the National Council passed the law, despite strong opposition in the parliamentary commission concerned. The second chamber (*Ständerat*)

¹⁰⁴ Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Federal law on identity cards for Swiss citizens), vom 22. Juni 2001, available at <http://www.admin.ch/ch/d/sr/1/143.1.de.pdf>; Verordnung über die Ausweise für Schweizer Staatsangehörige (Regulation on the cards for Swiss citizens), vom 20. September 2002, available at <http://www.admin.ch/ch/d/sr/1/143.11.de.pdf>.

¹⁰⁵ Press release of the federal police department, 26 May 2010, at http://www.bfm.admin.ch/bfm/de/home/dokumentation/medienmitteilungen/2010/ref_2010-05-260.html. Draft of the new regulation, Verordnung vom 24. Oktober 2007 über Zulassung, Aufenthalt und Erwerbstätigkeit (Regulation of 24 October 2007 on admission, residence and work), available at http://www.bfm.admin.ch/content/dam/data/migration/rechtsgrundlagen/gesetzgebung/biometrie_auslaenderausweis/anpassung_verordnungen/vo-ent-vzae-d.pdf. A sample of the new ID Card for foreigners is available at http://www.bfm.admin.ch/content/dam/data/migration/aufenthalt/prospekt_ausauswd.pdf.

¹⁰⁶ See "Solidarité sans frontières" (SOSF), available at <http://www.sosf.ch/publikationen/intro/intro.html>.

¹⁰⁷ See "Festnahmen im Basler Bahnhof" ("Arrests in Basel train station"), Basler Zeitung, 24 July 2010, at <http://bazonline.ch/basel/stadt/Festnahmen-im-Basler-Bahnhof/story/23470640>. This rule is most likely against a 1983 decision by the Swiss federal court, which held that identity controls are only allowed in case of a disruptive situation ("situation troublée"). Bundesgerichtesentscheid BGE 109 Ia 146, available at http://grundrechte.ch/2010/BGE_109_Ia_146.pdf.

¹⁰⁸ Ausländergesetzrevision, Dossier <http://web.archive.org/web/20071024141931/http://www.parlament.ch/do-auslaendergesetz> and the Bundesgesetz über die Ausländerinnen und Ausländer (AuG, Entwurf) (Federal Law on Foreigners), at <http://www.admin.ch/ch/d/ff/2002/3851.pdf> (Parliamentary nr. 02.024).

discussed the bill in March 2005 and introduced even more severe restrictions for foreigners.¹⁰⁹ The bill now goes back to the National Council. On 24 September 2006, the new law passed a referendum; it has been in force since 1 January 2008.¹¹⁰

According to a vote of the National Council in 2008, Switzerland's national identity card will be similar to biometric passports and introduced by 2010; the ID cards will include an electronically encoded photo and fingerprints on a chip. They will be in the "credit card" format already used for Swiss ID documents. They are to be provided at "family-friendly" prices.¹¹¹

Sports facilities in Switzerland have begun using biometric access control systems. The FDPIC has conducted inspections of the systems and asked that biometric data, in this case digital fingerprints, be stored on the individual membership cards and not in a central database. At the Commissioner's request, the sports facilities inspected agreed to provide customers who refuse the registration of their biometric data with alternative solutions at the same price.¹¹²

RFID tags

No specific information has been provided under this section.

BODILY PRIVACY

At the Zurich "Unique" airport, the cantonal Police of Zurich tested a pilot system for automatic face recognition between February and June 2003. Officially, the Face Recognition system (*Farec*) mainly aims at recognising people trying to immigrate without identity documents. This is the first test worldwide of face recognition in the context of boarder controls. During the test phase, 1,003 passengers from 277 flights were registered by *Farec*. In 81 cases, a search in the database followed, with ten hits and 17 misses. In December 2004, the Zurich Cantonal Government (*Regierungsrat*) provided a legal regulation (decree, *Verordnung*), extending the test phase until the end of

¹⁰⁹ Discussion in the Parliament (Ständerat) available at http://www.parlament.ch/ab/data/d/s/4707/122615/d_s_4707_122615_122623.htm.

¹¹⁰ Bundesgesetz über die Ausländerinnen und Ausländer (AuG) (Federal Law on Foreigners), vom 16. Dezember 2005, available at <http://www.admin.ch/ch/d/ff/2005/7365.pdf>.

¹¹¹ ePractice, eGovernment Factsheet – Switzerland – Infrastructure (May 2010), available at <http://www.epractice.eu/en/document/288426>.

¹¹² 14th Annual Report 2006-2007, *supra*.

2006.¹¹³ Although quite sceptical about the usefulness of the system, the data protection officer of the canton Zurich accepted the decree.¹¹⁴

In November 2005, a pilot project using facial recognition for security during sport events started in Berne. One hundred season ticket holders at the local ice-hockey club were registered with a photograph on a voluntary basis. Cameras at the entrance and in the stadium were tested. The company responsible dubbed this pilot project a success, but there were no further projects.¹¹⁵

On 27 August 2008, the "round table against violence in sport" (*Runder Tisch zur Gewaltbekämpfung im Sport*) proposed to use facial recognition in train stations and stadiums. A project with one dedicated system was planned for 2009. Tests with biometric cameras were expected in all football stadiums of the highest league. However, there have been no tests so far. The new regulation for measures and data systems of Fedpol, in force since 1 January 2010, allows the handover of photographs from the hooligan database HOOGAN to the private security forces of sport events for their use in automatic face recognition.¹¹⁶

WORKPLACE PRIVACY

No specific information has been provided under this section.

HEALTH & GENETIC PRIVACY

Medical records

The Federal Office of Public Health plans to implement voluntary storage of medical information on new health insurance cards. However, the Commission asked the Federal Office of Public Health to forego storing medical data on the health insurance card, because Public Health had not yet defined the purpose of this storage, nor shown the necessity of implementing such a scheme. Without a clearly set-out purpose, it was impossible to determine whether the storage was appropriate and respected the principle of proportionality.

¹¹³ Verordnung über den Einsatz eines biometrischen Gesichtserkennungssystems am Flughafen Zürich vom 8. Dezember 2004, (Nr. 551.113, available at http://www.sk.zh.ch/internet/sk/de/mm/mm_2004_quartal_4/285_gesichtserkennung.ContentList.0002.Document.tmp/Verordnung%20FCber%20den%20Einsatz%20eines%20biometrischen%20Gesichtserkennungssystems%20a). See also the media release issued by the Regierungsrates on 16 December 2004 (http://www.sk.zh.ch/internet/sk/de/mm/mm_2004_quartal_4/285_gesichtserkennung.html). See also Marcel Gyr, "Weiterer Test des Gesichtserkennungssystems" (Further Test of the Facial Recognition System), *Neue Zürcher Zeitung NZZ*, 17 December 2004, at 53.

¹¹⁴ See e.g., *Neue Zürcher Zeitung*, 23. August 2002, No. 194, at 37, and id., and Stefan Hohler, "Phase 2 für 'Frühwarnsystem'" (Phase 2 for 'early warning'), *Tages-Anzeiger* 17 December 2004.

¹¹⁵ See http://www.unisys.ch/clients/featured__case__studies/casestudy_biometrie.htm.

¹¹⁶ Verordnung über verwaltungspolizeiliche Massnahmen und über Informationssysteme des Bundesamtes für Polizei, vom 4. Dezember 2009 available at http://www.admin.ch/ch/d/sr/120_52/index.html.

Since 1 January 2010, the new health insurance cards are mandatory.¹¹⁷

Genetic identification

In July 2000, a regulation on the collection and storage of genetic profiles was introduced, allowing the Swiss administration – by way of a new Agency called AFIS Services – to establish and operate a centralised database with DNA profiles of persons and stains.¹¹⁸ The Federal Office has collected data for the police since 1 August 2000. All samples taken by the police are given a unique identifier, so that the name of the suspect is never disclosed to laboratory employees. The regulation states that police forces are allowed to collect DNA samples only in case the offence committed is listed in a catalogue.¹¹⁹ However, this catalogue not only includes crimes like murder, sexual offences, life endangerment, and rape, but also theft (*Diebstahl*). Further, there are reports (and lawsuits) of cases where the police have taken DNA samples of persons who did not commit any of these offences.¹²⁰ By the end of 2003, EDNA contained 45,313 DNA profiles. One year later, it had almost 60,000.¹²¹ On 1 January 2005, the EDNA regulation was replaced by a formal law,¹²² which does not have a catalogue of offences at all.

In March 2004, the majority of the National Council decided to allow life insurance companies to review previous DNA analyses of persons in case they want to sign a contract with a life or a voluntary insurance company against invalidity. The bill was approved by the smaller chamber (*Ständerat*) in June 2004 and again in October 2004.

¹¹⁷ *Id.*

¹¹⁸ Verordnung über das DNA-Profil-Informationssystem(EDNA, SR 361.1) (Regulation of the DNA profile information system), vom 31.Mai 2000, available at <http://www.admin.ch/ch/d/as/2000/1715.pdf>.

¹¹⁹ EDNA, Article 5, for details on the procedure see also W.Bär, Adelgunde Kratzer & M. Strehler, "Swiss Federal DNA Profile Information System – EDNA," available at <http://www.promega.com/geneticidproc/ussymp12proc/abstracts/bar.pdf>.

¹²⁰ See, e.g., Heiner Busch, "Die Wattestäbchenattacke," *WOZ Die Wochenzeitung*, Nr. 26/2004, available at <http://www.woz.ch/artikel/archiv/10141.html>, as well as reports at <http://switzerland.indymedia.org/demix/2004/11/28078.shtml>. For a critical comment on DNA samples See also Markus Hofmann "DNA-Profil - die Lieblinge der Polizei," in: *Neue Zürcher Zeitung NZZ*, 4 March 2005, at 13. According to this article, every sample costs about CHF 295.

¹²¹ Heiner Busch, "Das neue Schweizer Wettfischen" in *WOZ Die Wochenzeitung* nr. 9, 3 March 2005, at 6.

¹²² Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen (DNA-Profil-Gesetz, SR 363 available at <http://www.admin.ch/ch/d/sr/c363.html>, as well as the corresponding regulation (decree) (DNA-Profil-Verordnung, SR 363.1 http://www.admin.ch/ch/d/sr/c363_1.html). For the discussion in the Parliament see (Nationalrat, Amtliches Bulletin, 20.06. 03-08h00) http://www.parlament.ch/ab/data/d/n/4619/86799/d_n_4619_86799_86951.htm. In September 2002, the majority of the National Council decided, against the recommendation of the preparing commission, not to include any catalogue in the new law on DNA profiles. After the tsunami disaster in December 2004 in Southeast Asia, a lot of DNA samples of Swiss relatives of missing tourists were taken.

The deadline for a referendum passed on 27 January 2005 without a request for a public ballot.¹²³

FINANCIAL PRIVACY

As already reported, banking records are protected by the Swiss Federal Banking Act of 1934. This act was passed to guarantee strong protections for the privacy and confidentiality of bank customers. However, Switzerland has come under increasing pressure from the European Union and the Organisation for Economic Cooperation and Development (OECD) to weaken these laws and provide greater access to bank records for the purposes of tax collection.¹²⁴

E-GOVERNMENT & PRIVACY

The SuisseID provide an electronic proof of identity in Switzerland, supporting both a legally binding electronic signature as well as a method for secure authentication. Available in form of a USB key or as smart card, the SuisseID allows for conducting business online in a secure manner. By means of SuisseID, private persons are able to sign contracts with companies as well as with the public authorities directly via Internet; in addition, private companies are able to sign contracts with each other.¹²⁵

OPEN GOVERNMENT

In July 2006, the Freedom of Information Act (*Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung* or BGÖ) came into effect.¹²⁶ The FDPIC is responsible for Advisory, Conciliation, and Arbitration Service related to the new Act. The FDPIC has already made several recommendations, and the number of requests for arbitration is increasing.¹²⁷

In some cantons, the data protection law is at the same time a "Freedom of Information Law" (*Öffentlichkeitsgesetz*), and the data protection officer has the duties of a Freedom of Information Protection Officer as well. According to such laws, all official documents should be publicly available and citizens have a legal right to receive information – except if a document is declared as confidential. Other cantons and the Confederation are

¹²³ Bundesgesetz über genetische Untersuchungen beim Menschen (Parliamentary number 02.065, SR 814.02, Bundesblatt Nr. 41, 19 October 2004, at 5483ff, available at <http://www.admin.ch/ch/d/ff/2004/5483.pdf>). For a summary of the parliamentary discussion see http://www.parlament.ch/afs/data/d/rb/d_rb_20020065.htm (in German).

¹²⁴ *Cfr.* Section "National and international data disclosure agreements," *supra*.

¹²⁵ ePractice, eGovernment Factsheet – Switzerland – Infrastructure, *supra*.

¹²⁶ See http://www.admin.ch/ch/d/sr/c152_3.html.

¹²⁷ 14th Annual Report 2006-2007, *supra*.

preparing a similar law.¹²⁸ However, the first consultations among interested parties are revealing considerable opposition, e.g. in the canton of Zurich.

In 2009, the FDPIC dealt with 41 requests for arbitration (25 in 2008); 65 percent of the cases resulted in a success for the requester.

In April 2005, a revision of the regulation (decree) on Land Registers (*Grundbuchverordnung*), dating back to 1910, was put into force by the Government.¹²⁹ The cantons are now allowed to publish parts of the register on the Internet.

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

No specific information has been provided under this section.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Switzerland acceded to the 1966 UN International Covenant on Civil and Political Rights (ICCPR) but it is not party to its First Optional Protocol, which establishes an individual complaint mechanism.¹³⁰

Switzerland is a member of the Council of Europe (CoE) and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).¹³¹ Switzerland has signed and ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108)

¹²⁸ For the Confederation, see the proposal for a Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.), published in the *Bundesblatt* 2004, at 7269ff. (<http://www.admin.ch/ch/d/ff/2004/7269.pdf>) and the corresponding governmental report (Botschaft). The delay for a referendum was passed on 7 April 2005 without any request for it was presented. For an overview of this law, see <http://web.archive.org/web/20051118210014/http://www.ofj.admin.ch/themen/oeffprinzip/intro-d.htm> (in German). Critics of the new law argue that it contains too many exceptions.

¹²⁹ Grundbuchverordnung, (GBV; SR 211.432.1, available at http://www.admin.ch/ch/d/sr/c211_432_1.html). The changes have been published in the official publication of laws (AS), available at <http://www.admin.ch/ch/d/as/2005/1343.pdf>. For an overview in English, see <http://web.archive.org/web/20050920110715/http://www.ofj.admin.ch/themen/gba/intro-e.htm>.

¹³⁰ Switzerland acceded to the ICCPR on 18 June 1992. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

¹³¹ EMRK, signed in Rome on 4 November 1950, accepted by the Parliament on 3 October 1974, ratified on 28 November 1974 http://www.admin.ch/ch/d/sr/0_101/index.html.

in 1997.¹³² It has signed and ratified the Additional Protocol to the above mentioned Convention No. 108 as well.¹³³ In November 2001, Switzerland signed the CoE Convention on Cybercrime, but has not ratified it.¹³⁴

It is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

As reported above, Switzerland is not a member of the EU, but has some special agreements with the EU. Some of these bilateral agreements were signed in 2000 and 2001. Further some EU regulations must be implemented "automatically" in the Swiss legal order, like the regulation for passports previously described.

*Updates to the Swiss Report published in the 2010 edition of EPHR have been provided by: Christian Thommen, Grundrechte.ch, Switzerland; Christoph Mueller, University of Zurich, Switzerland; Heinrich Busch, Switzerland.

¹³² Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Abgeschlossen in Strassburg am 28. Januar 1981. Von der Bundesversammlung genehmigt am 5. Juni 1997. Schweizerische Ratifikationsurkunde hinterlegt am 2. Oktober 1997. Für die Schweiz in Kraft getreten am 1. Februar 1998 (Übersetzung des französischen Originaltextes, Translation of the original in French, RO 2002 2847). SR 0.235.1) <http://www.admin.ch/ch/d/as/2002/2847.pdf>. Signed 2 October 1997; ratified 2 October 1997; entered into force 1 February 1998.

¹³³ Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr, available (in German) at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=7&D...> signed the Additional Protocol on 17 October 2002 and ratified it on 20 December 2007. With regard to Switzerland the Additional Protocol entered into force on 1 April 2008.

¹³⁴ Signed 23 November 2001.

REPUBLIC OF TURKEY

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

Article 20 of the Turkish Constitution deals with individual privacy and states, "Everyone has the right to demand respect for his private and family life. Privacy of individual and family life cannot be violated."¹ Article 20 prohibits the search or seizure of any individual, his private papers, or his belongings unless there exists a decision duly passed by a judge in cases explicitly defined by law, and, in cases where delay is deemed prejudicial, that there is an order by an agency authorised by the law. Article 22 preserves the secrecy of communication and states that, "Communication shall not be impeded nor its secrecy be violated, unless there exists a decision duly passed by a judge in cases explicitly defined by law, and unless there exists an order of an agency authorised by law in cases where delay is deemed prejudicial."² In October 2001, in a move aimed at improving its chances of joining the European Union, Turkey passed the Constitutional Amendment Bill, containing 34 proposed amendments to the Constitution.³ Several of the proposals strengthen the basic rights and freedoms of individuals, including increased protection for privacy of the person and the home.⁴

Subsequently, the Turkish Government presented a new constitutional amendment package (*Anayasa Değişiklik Paketi*) to Parliament in March 2010, which included proposed changes to 26 articles of the 1982 Constitution.⁵

A new section will be added to Article 20 regarding privacy and data protection issues. Pursuant to the proposed amendments, obtaining, storing, and using personal data for any means shall require the data subject's prior and explicit consent. It shall also grant every person the right to access related data without any delay or obstacle, and shall provide the right to demand a high level of protection for stored data and to have full control over one's personal data. The proposed amendment package was accepted by the Parliament and approved by the President in May 2010. However, because it was accepted without the three-fifths or two-thirds qualified majority according to Article 175 of the Constitution, a nationwide referendum will be held to approve the amendment package in September 2010.

¹ Constitution of the Republic of Turkey (as amended on 7 October 2001), Art. 20, available at http://www.anayasa.gov.tr/images/loaded/pdf_dosyalari/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_TURKEY.pdf.

² *Id.*, Art 22.

³ Nick Thorpe, "Mixed Reactions to Turkey's Reforms", BBC News, 5 October 2001, available at http://news.bbc.co.uk/1/hi/english/world/europe/newsid_1580000/1580238.stm.

⁴ US Department of State, Country Reports on Human Rights Practices - 2001, 4 March 2002, available at <http://www.state.gov/g/drl/rls/hrrpt/2001>.

⁵ Text available in Turkish at <http://www.akparti.org.tr/media/www/Anayasa%20teklif%20metni.pdf>.

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

As part of Turkey's 2005 Accession Partnership with the European Union, Turkey is required to "[a]dopt a law on protection of personal data" and "establish an independent supervisory authority."⁶ According to the European Commission's latest progress report in late 2006, there have been no developments in Turkey regarding the protection of personal data.⁷ The EU partially suspended accession negotiation with Turkey in December 2006.⁸

Thus the situation is as follows. The 2003 Draft Data Protection Act (DDPA) has been sent to the relevant legislative commission at the Parliament; it is pending and has not yet been adopted.⁹ The draft establishes the protection of privacy in the public and private sphere on a new legal basis. It protects the personal data handled either by persons or entities, with the aim of protecting natural persons. The law will be applicable to both automated and manual data processing. It aims to protect the right of personhood and the fundamental rights of persons who are the subjects of data processing. The draft addresses the following: general conditions for the legal standard of data processing; rules regarding the rights of personal data subjects; rules for data processing under private and public law; the establishment, structure, membership and obligations of the supervisory authority; data registry; registration of data collection; data transfers to other countries; the obligation to register data transmission; and penal provisions. Regarding the last, the legislature intends to regulate offences against privacy, which will be subject to civil, administrative and criminal sanctions.¹⁰

This draft is in accordance with the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which Turkey signed but has not yet ratified. Its crucial sections, regarding data processing, transfer, and storage are very much in line with Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.¹¹ The OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data are also taken under consideration. Though there are still some loopholes

⁶ European Commission, Council Decision of 23 January 2006 on the principles, priorities, and conditions contained in the Accession Partnership with Turkey (2006/35/EC), available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32006D0035&model=guichett.

⁷ European Commission, Turkey 2006 Progress Report, 8 November 2006, available at http://ec.europa.eu/enlargement/pdf/key_documents/2006/nov/tr_sec_1390_en.pdf.

⁸ European Commission, Questions and Answers – Turkey, available at http://ec.europa.eu/enlargement/questions_and_answers/turkey_en.htm.

⁹ Turkish text at <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf>.

¹⁰ *Id.*

¹¹ See <http://www2.tbmm.gov.tr/d23/1/1-0576.pdf> (in Turkish).

in the Draft Act, it can be considered an important step toward Turkey's harmonisation with EU legislation in terms of data protection and privacy.

Sector-based laws

For the time being, the protection of personal rights within the Turkish national legislation is regulated in the Civil Code. Pursuant to Article 24 of the Civil Code, an individual whose personal rights are unjustly violated has a right to civil action. Furthermore, disclosing, transferring, or misusing personal or confidential data in any way is deemed an invasion of personal privacy, and consequently, as an infringement of personal rights. Any unlawful invasion of an individual's privacy, including personal or confidential information, will incur legal consequences. The scope of personal or confidential data is determined by a court under its sole discretion, unless such scope is defined within the terms of a confidentiality agreement or any other agreement between the parties, or is specified by a special regulation. As consequence of such act, an aggrieved party may receive indemnification of their material and immaterial damages pursuant to Article 49 of the Code of Obligations (*Borçlar Kanunu*).¹² However, there is little criminal liability for such violations of personal rights.

The 2005 Criminal Code regulates felonies against the private life and the private sphere. These felonies may be pursued *ex officio*, where the offences concern the storage, illegal transfer or retention of data. The following felonies on data protection are established in Section 9 of the Turkish Criminal Code: violation of the secrecy of a communication; wire-tapping; storage of personal data; and illegal transfer of personal data.¹³

A Turkish law extending the state press restrictions to the Internet was passed amid much opposition in May 2002.¹⁴ The law, called the Supreme Board of Radio and Television Bill No. 4676,¹⁵ places the Turkish Internet under the regulatory authority of the Supreme Radio and Television Board (*Radyo ve Televizyon Üst Kurulu* or RTÜK).¹⁶ Former Turkish President Ahmet Necdet Sezer has expressed disapproval of the provisions.¹⁷ The President first rejected the law and sent it back to the Parliament, and proclaimed the law to be unjust and unfair supporting his opinion with a long list of motivations.¹⁸ The Parliament insisted on the necessity of such legislation and the President had

¹² Turkish text available at <http://www.mevzuat.adalet.gov.tr/html/407.html>.

¹³ *Id.*

¹⁴ Jonathan Evans, "Turkey Passes Strict Net Law," Wired News, 15 May 2002, available at http://www.wired.com/news/politics/0,1283,52558,00.html?tw=wn_story_related.

¹⁵ Yaman Akdeniz, Internet Governance and Freedom in Turkey 3 (2003). available at http://www.cyber-rights.org/documents/osce_turkey_paper.pdf.

¹⁶ Dorian Jones, "Turkey Tightens Controls on the Net", BBC News Online, 28 May 2002, available at <http://news.bbc.co.uk/1/hi/sci/tech/2006759.stm>.

¹⁷ *Id.*

¹⁸ See http://www.turkhukuk sitesi.com/makale_38.htm (in Turkish).

compulsorily to undersign it, according to the Constitution. However, having declared his disapproval, he has taken the law to the Constitutional Court for annulment. This situation caused great discontent among the public and put pressure on the highest Court. Eventually, the number of the Bill changed to 4756 but most of the critical articles – such as Article 31, which gives authority to the RTÜK for regulating dissemination on the Internet – remained unchanged. In particular, Article 26 of the Bill No. 4756, which integrated Article 9 at the current RTÜK Bill No. 3984 – has inserted a very debatable provision to the Press Law (with this article the provisions regarding the defamatory claims in the RTÜK Bill, shall cover the actions that will be taken via the Internet). Fortunately, these particular controversial provisions have not been used very often by the prosecutors since they were adopted.

The Electronic Signature Act came into force on 23 July 2004. The Act was prepared under the guidance of the EU Directive and took into account the practice of member states such as Germany, France, Austria, and Belgium. The Electronic Signature Act mainly provides that e-signatures have the same value and effect as actual written signatures and thus validate proceedings concluded in the electronic environment. With regards to the privacy and data protection, Article 12 of the Act regulates data collection and data processing and Article 16 underlines the importance of express consent from the provider and penalises contrary receipt of data without the consent.

In addition, the E-signature Regulation and Communiqué entered into force on 6 January 2005.

According to its provisions, e-signature certificate providers are commissioned to issue such electronic documents by fulfilling certain conditions stated in the law, and they are subject to the following obligations related to data protection: (a) The certification service provider may collect personal data only to the extent necessary for the purpose of issuing a certificate. Sharing data with a third party is permissible only with the consent of the person whose personal data is being processed; (b) The certification service provider may not disclose the certificate to third parties without the consent of the certificate owner; and, (c) The certification service provider has to prevent third parties from collecting personal data without the written consent of the owner of such personal data. The certificate service provider may transfer/use personal data only with consent of the owner of such data.¹⁹

The Telecommunications Council, established in 2000, is the main institution responsible for data protection and privacy issues in the telecoms sector. It has been authorised by the Turkish Government. Under the supervision of the Council, a regulation was enacted in 2004 by the Parliament in terms of data protection in the telecommunication sector as Regulation on Personal Data Processing and the Protection in Telecommunication Sector (Regulation). The Regulation is in principle a summary of the European Union's

¹⁹ *Id.*

Directive 2002/58/EC on data protection in electronic communications.²⁰ It regulates the following topics: security of communication; duty to disclose the risks with regard to network security; privacy of communication; processing of data; call number display; lists of participants; and spamming. In Article 20 of the Regulation, it is clearly stated that "you shall not obtain any personal data without the data subject's express consent; and process it in terms of communicating by telephone, fax, mobile phone and electronic mailing or any other electronic communication device." It has also been stated that the data subject should always have easy access to an option to opt in or opt out whenever he or she wants.

In the light of the above, it can be deduced that there currently is no comprehensive regulation concerning data protection and privacy in Turkish law. There is not a concrete definition for "personal data" either. Only Article 3 of the Regulation on Personal Data Processing and the Protection in Telecommunication Sector gives a framework definition of "personal data" as "any kind of information such as ID number, any other direct and/or indirect physical, sociological, cultural, economical, ethnical, political information, and also other additional explanatory information regarding her/his genetic, religious and family status." So, in light of this very general and vague definition, in practice the name, postal address, email account information, phone numbers, age, and sex of a person are generally accepted as personal information. According to the abovementioned Regulation, digital information such as computer IP addresses, might also be considered indirect or direct information in the event of damage and loss. But this definition as such will be slow in coming, and shall definitely be at the discretion of the relevant courts. Moreover, there are more solid definitions in the key sectors like the banking and finance.

MAJOR PRIVACY & DATA PROTECTION CASE LAW

Relevant case law concerning privacy and data protection is cited *infra* in the text and categorised under the corresponding section.²¹

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

Wiretapping, access to, and interception of communications

Despite the existing laws and regulations, the right to privacy of private communications is immature in Turkey. According to Human Rights Watch, human rights defenders are

²⁰ Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002, OJ L 201, 31 July 2002, at 37-47, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML>.

²¹ *Cfr.* Sections "Cybercrime," and "International Obligations & International Cooperation," *infra*.

routinely placed under surveillance, often prevented from holding public events, and routinely prosecuted for various speech and assembly offences.²²

Articles 195-200 of the Turkish Criminal Code govern freedom of communication through letters, parcels, telegram, and telephone. Government officials are required, subject to various exceptions, to obtain a judicial warrant before monitoring private correspondence.

In a letter that was leaked to the media in early 2007, the National Intelligence Agency Undersecretary complained about the difficulties the national intelligence community was facing because of existing legislation against phone tapping and eavesdropping; he requested an amendment in the law to enhance the agency's eavesdropping powers.²³

National security legislation

In 2006, the government adopted amendments to its Antiterrorism Law. The amendments have been highly criticised for placing further restrictions on the already censored media. Editors that disclose the identities of public personnel fighting terrorism may be fined, and a judge may order the closure for up to one month of a publication that "makes propaganda for terrorist organisations." During the year there was an increase in the number of cases against the press under the Antiterrorism Law. The Turkish Publishers Association and human rights groups reported that the law contains an overly broad definition of what constitutes an offence that allows ideologically and politically motivated prosecutions.²⁴

Immediately following deadly bombings in Ankara in May 2007, the government proposed another amendment to the Police Task and Authority Bill, (*Polis Vazife Ve Selahiyet Kanunu*)²⁵ that will allow police to take fingerprints of anyone applying for a gun licence, driving licence, passport, or Turkish citizenship. This amendment was adopted swiftly in June 2007. It also provides the police with a larger authority to stop, search, and demand identification from individuals. The amended Bill also enables the police to use anyone to collect information. Some lawyers say it represents the largest expansion of police authority ever.²⁶

²² Human Rights Watch 2006 Report – Turkey, at <http://www.hrw.org/wr2k7/wr2007master.pdf>.

²³ Yusuf Kanli, Informatics Crimes, 17 January 2007, *Turkish Daily News*, available at <http://www.hurriyetdailynews.com/h.php?news=informatics-crimes-2007-01-17>.

²⁴ US State Department 2009 Human Rights Report: Turkey, 11 March 2010, available at <http://www.state.gov/g/drl/rls/hrrpt/2009/eur/136062.htm>.

²⁵ Turkish text at <http://www.mevzuat.adalet.gov.tr/html/569.html>.

²⁶ Onur Burcak Belli, "Advocacy Groups Alarmed at Proposed Police Powers," *Turkish Daily News*, 29 May 2007, available at <http://www.hurriyetdailynews.com/h.php?news=advocacy-groups-alarmed-at-proposed-police-powers-2007-05-29>.

Data retention

In the Telecommunications Council's 2007 work plan, the Authority stated that it plans to review the Regulation on Personal Data Processing and the Protection in Telecommunication Sector (Regulation) in order to suggest methods of harmonising it with the European Union's 2006 Data Retention Directive.²⁷ No further information has been provided.

National databases for law enforcement and security purposes

The Ministry of Justice has recently established a National Judiciary Informatics System (*Ulusal Yargı Ağı Projesi* or UYAP),²⁸ which is to implement a very ambitious information system between the courts and all other institutions of the Ministry, including prisons. UYAP equipped these institutions with computers with networking and Internet connections, allowing them access to all legislation, decisions of the Supreme Court, judicial records, judicial data of the police, and army records. Thus, UYAP established an electronic network covering all courts, offices of public prosecutors and law enforcement offices together with the Central Organisation of the Ministry of Justice.

It is also planned to set up integration with the databases of national and international institutions and organisations in the course of progress towards accession to the European Union. In this context, it is also aimed at establishing links to the central databases of the European Union and EU member countries' systems.²⁹

National and international data disclosure agreements

No specific information has been provided under this section.

Cybercrime

Under the current Turkish Criminal Code, computer-related offences can be prosecuted pursuant to Amendment No. 3756, "Crimes on Informatics."³⁰

Just before the 2007 elections, the Government rushed to enact the infamous Law No. 5651 entitled Regulation of Publications on the Internet and Suppression of Crimes Committed by means of such Publication.³¹ Law No. 5651 regulates the legal responsibilities of various actors including content providers, hosting companies, Internet service providers (ISPs), and Internet cafés. It also addresses how the current regulatory systems work and how websites, predominantly situated outside the Turkish jurisdiction, will be blocked by court and administrative proceedings. This has raised the issue of

²⁷ Republic of Turkey Telecommunications Authority Workplan 2007, available in English and Turkish at http://www.tk.gov.tr/Yayin/Is_Planlari/2007_is_plani.pdf.

²⁸ UYAP, website in English at <http://www.uyap.gov.tr/english/index.html>.

²⁹ See <http://www.uyap.gov.tr/genelbilgi/genel.html> (in Turkish).

³⁰ Turkish Criminal Code, Amendment No. 3756 14 June 1991.

³¹ Turkish text at <http://www.tbmm.gov.tr/kanunlar/k5651.html>.

censorship of Internet content and drawn attention to the Telecommunication Communication Presidency (*Telekomünikasyon İletişim Başkanlığı* or TİB). TİB is the organisation responsible for executing blocking orders issued by the courts, and has been given authority to issue administrative blocking orders with regard to certain Internet content hosted in Turkey, and to websites hosted abroad, in terms of crimes listed in Article 8 of Law No. 5651.

Thus, censorship of ISPs, and eventually of user-generated content, is a long-lasting issue in Turkey. It started with a court order in Ankara stemming from ten video clips consisting of defamatory statements and images about the founder/pioneer of Turkish Republic, Atatürk. These clips were deemed to be illegal by the court pursuant to Law No. 5816 titled Crimes Against Atatürk, and access to these clips are blocked in accordance with the Law No. 5651, which came into force in November 2007 as aforementioned.

The attitude of the Government, and TİB gradually grew less tolerant such that it is estimated that 5,000 websites are currently blocked in Turkey. This grave situation reached its climax when TİB requested that some ISPs in Turkey block access to specified IP addresses used by YouTube. As a result of this demand and action, a number of Google services – including Google Analytics, Translate, Docs, Books, Maps, and Earth – have been heavily affected since 4 June 2010. These Google services were not blocked, but access to them has become a painstaking and time-consuming effort. Some users have even reported that they cannot access the aforementioned sites. To defend itself from the resulting public annoyance, TİB blamed Google as the parent company of YouTube, and held it responsible by using the same blocked IP addresses for the disrupted Google-related services.

Nonetheless, there is another side of the coin. According to Law No. 5651, a valid court order is essential for blocking access to a website. Some exceptions to this rule are provided in specific cases such as child pornography and crimes against Atatürk. Even for these exceptions, an administrative proceeding should be sought. However, neither was done in TİB's latest action. Therefore, this action can be considered absolutely unlawful.³² Once again, the basic constitutional right to "communication and access to information" was violated.

On the other hand, the reason behind the government's actions against YouTube was revealed and alleged to be financial. Google has no legal entity in Turkey and therefore has no tax liability. The government claims that Google should be registered and should pay its levies as any other foreign company operating in Turkey. However, this should not be accepted as an excuse, this is totally a different issue and no such financial or tax based provision has been stated in Law No. 5651 as reason for justifying blocking access.

³² See <http://privacy.cyber-rights.org.tr/?cat=21> (in Turkish).

Critical infrastructure

No specific information has been provided under this section.

INTERNET & CONSUMER PRIVACY

E-commerce

The Internet and e-commerce industries are booming in Turkey. With a very young population (the median age is 28.8) of circa 75 million, Turkey is the second in EU for Facebook penetration and has more than 30 million Internet users, a jump from 4 million seven years ago.

With these promising figures, Turkey is in the verge of an Internet era. However, it is obvious that current legislation is not in line with international standards and their present implementation runs counter to basic human rights such as freedom of expression and freedom of information. Therefore, reforms urgently need to be carried out in order to provide conditions that allow the Turkish public to exercise their rights. As reported above, Law No. 5651 considerably limits freedom of expression and severely restricts citizens' right to access information.

Cybersecurity

No specific information has been provided under this section.

Online behavioural marketing and search engine privacy

No specific information has been provided under this section.

Online social networks and virtual communities

No specific information has been provided under this section.

Online youth safety

No specific information has been provided under this section.

TERRITORIAL PRIVACY

Video surveillance

No specific information has been provided under this section.

Location privacy (GPS, mobile phones, location based services, etc.)

No specific information has been provided under this section.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

No specific information has been provided under this section.

NATIONAL ID & SMART CARDS

According to a Prime Minister's department Circular, issued on 4 July 2007, on an electronic citizenship card pilot project, electronic citizenship cards will be exclusively used for ID verification purposes.³³ The Circular specifies both the characteristics of the card as well as the project's implementation process.³⁴

The citizenship card, which is actually a smart card, will exclusively contain static information necessary to perform ID verification, but no dynamic data such as health information, address, etc. The card will enable ID verification with different credentials such as visual security elements, pin code and biometric data (fingerprint). The biometric data will be held exclusively on the card and will not be stored in a central database. The card is going to replace the currently used national identity cards. In addition, the characteristics of the card enable its usage in any service requiring secure ID verification, such as online e-government services, financial transactions, etc.³⁵

In accordance with the Circular, a three-stage pilot implementation project has already been initiated in the area of social security and health. The second phase of the pilot implementation was completed and third and last phase which includes the dissemination of 300,000 ID cards to citizens has been started by August 2009. Pilot implementation will be completed by 2010 and ID cards will be distributed all over the country in 2011.³⁶

Religious affiliation is listed on national identity cards. A few religious groups, such as the Baha'i, are unable to state their religion on their cards because it is not included among the options; they have made their concerns known to the government. In April 2006, the government adopted legislation allowing persons to leave the religion section of their identity cards blank or change the religious designation by written application. However, according to the US State Department, the Turkish government continued to restrict applicants' choice of religion.³⁷

RFID tags

No specific information has been provided under this section.

BODILY PRIVACY

No specific information has been provided under this section.

³³ *Cfr. "E-government & Privacy," infra.*

³⁴ ePractice, eGovernment Factsheet – Turkey – National Infrastructure (August 2010), available at <http://www.epractice.eu/en/document/288418>.

³⁵ *Id.*

³⁶ *Id.*

³⁷ US State Department Human Rights Report 2009, *supra*.

WORKPLACE PRIVACY

No specific information has been provided under this section.

HEALTH & GENETIC PRIVACY

Medical records

No specific information has been provided under this section.

Genetic identification

No specific information has been provided under this section.

FINANCIAL PRIVACY

Pursuant to the Debit and Credit Cards Law which was enacted in 2006, prior written consent of the cardholder is vital, and personal data such as name, address, phone numbers, emails, and any other relevant financial information, should not be disclosed, sold, exchanged, or transferred to third parties without the written and undersigned consent of the data subject.³⁸ Both banks and transaction affiliates are liable and are obligated to take the required precautions in order to protect the cardholder/consumer from any harm.

E-GOVERNMENT & PRIVACY

The Ministry of Finance prepared and issued a Communiqué on Electronic Invoice and Electronic Commercial Books in 2008. However, it is not yet commonly used by Turkish companies because of a complicated IT infrastructure that is still in an integration phase.

The Ministry of Finance has also implemented a nationwide communications network to streamline administrative workflows and allow citizens to submit their tax returns online.³⁹ The system connects 599 offices – including tax offices, regional finance offices, and tax inspector offices – of the Revenue Administration. Citizens can submit tax returns via the Internet and can call up their tax file online whenever they want. All tax data is centrally stored in a data warehouse system, and access to the system is secured by the use of digital signatures and encrypted data transfer via a Public Key Infrastructure. The project also stipulates establishing the necessary IT infrastructure for the creation of a call centre.⁴⁰

Other infrastructure related to the Ministry of Finance includes the "e-Declaration" application, which provides acceptance of declarations, announcements and appendices via the Internet. Integration and data exchange with external systems such as banks is also provided. Another application is the "Internet Tax Office" of the Revenue Administration, which enables taxpayers to follow their tax transactions such as accrual

³⁸ Turkish text available at <http://www.mevzuat.adalet.gov.tr/html/26831.html>.

³⁹ ePractice, eGovernment Factsheet – Turkey – National Infrastructure, *supra*.

⁴⁰ *Id.*

tax, payments in, etc. These applications are all parts of the Tax Offices Automation Project (VEDOP).⁴¹

In line with the Electronic Signature Act, the Ministry of Justice declared that documents will no longer be circulated physically among the judicial units after 1 July 2008. All documents are required to be sent in the electronic environment, signed by e-signature.

There is a project, carried out within UYAP, called "Expert System Portal Development Project" which aims to develop a web-based expert system portal.⁴² In this Project, the user will be able to access information about which route to follow, how much to pay in fees, and what the costs will be during the course of the lawsuit. It enables the user to access the decisions of similar cases when she/he enters the keywords and the required parameters that will appear on the screen concerning the law suit involved. Reports of similar cases will be extracted together with related statistical information; the number of lawsuits filed according to the topics; the duration of lawsuits; the number of claims that are accepted, partially accepted, and rejected; the legal costs, the quantity of amendments, the amount of money paid to defendants, etc.

In a quite recent development, after reaching an agreement with the GSM operators, text messages containing information about the case files can be sent to the parties who need to be warned when to attend the court. In order to subscribe to this service, citizens should send a SMS with their ID number, type the required word "abone" and then send it to tel. No. 4060.

In addition to this, after completing the test stage, courts and other judicial units were equipped with "video and audio recording," and "video conferencing systems". These systems were tested in Ankara Courthouse, the biggest court in Turkey, and were rolled out in 225 "heavy" criminal courts. "Heavy" Criminal courts consist of a presiding judge and two members with a public prosecutor. Offences and crimes involving a penalty of over five years of imprisonment are under the jurisdiction of these courts, of which there is at least one in every city. The court is sometimes divided into several branches according to need and population.

OPEN GOVERNMENT

A Law on the Right to Information⁴³ was officially published in October 2003 and went into effect on 24 April 2004.⁴⁴ The law allows the public to request information from government agencies. It provides for the withholding of confidential private information, and the review of disputed information requests by a Turkish Right to Information

⁴¹ *Id.*

⁴² See UYAP, *supra*.

⁴³ Law on the Right to Information (No. 4982), available at http://www.bilgiedinmehakki.org/en/index.php?option=com_content&task=view&id=7&Itemid=8.

⁴⁴ "Turkey Enacts Freedom of Information Law," BilgiEdinmeHakki, http://www.bilgiedinmehakki.org/en/index.php?option=com_content&task=view&id=4&Itemid=5.

Review Council (*Bilgi Edinme Değerlendirme Kurulu*, or BEDK), as well as a right to sue for any losses deriving from the illegal action.

Appeals of withholdings are made to the BEDK; its jurisdiction was originally limited to cases relating to national security and state economic interests but the law was amended in November 2005 to allow appeals in all cases. BEDK received 2,475 appeals through March 2007. Due to the efforts of Turkish pressure group *BilgiEdinmeHakki.org*, BEDK began publishing its decisions as of April 2007.⁴⁵ Appeals can then be made to the administrative courts.

The Law on the Right to Information was amended in 2006 to enable citizens to dispute all decisions of state agencies regarding denials of requests for information. Public organisations are making use of the new legislation.

A total of 1,886,962 right to information requests were made between 2004 and 2006 in Turkey.⁴⁶ In fact, the overall number of applications in Turkey is higher than most countries in the world.⁴⁷ The application process is gradually evolving and it indicates the sensitivity of Turkish people to the issue of open government.

In 2006, Turkey adopted a law for the establishment of an Ombudsman that the European Union believed would help fight corruption, increase transparency, and allow better control of military spending; however, President Sezer vetoed the law before its enactment in July 2006.⁴⁸ Following Turkey's election on 22 July 2007, the EU stated that passage of the Ombudsman's bill should be a top priority of the new government.⁴⁹

The pressure on government seems to have finally paid off and the recent Constitution package, which will be held in referendum, has made the ombudsman institution a priority.

OTHER RECENT FACTUAL DEVELOPMENTS

No specific information has been provided under this section.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

No specific information has been provided under this section

⁴⁵ Turkish Right to Information Assessment Council started to publish its decisions," March 14, 2007, available at <http://www.bilgiedinmehakki.org/en/>.

⁴⁶ Dr. Yaman Akdeniz, "Freedom of Information in Turkey," May 2008, at 23, at http://www.bilgiedinmehakki.org/doc/Turkey_FOI_2008_Report.pdf.

⁴⁷ *Id.*

⁴⁸ "Sezer Vetoes EU-Backed Ombudsman Law," *Turkish Daily News*, 2 July 2006, available at <http://www.hurriyetdailynews.com/h.php?news=sezer-vetoes-eu-backed-ombudsman-law-2006-07-02>.

⁴⁹ "Relieved EU Urges the New Government to Resume Reforms," *Turkish Daily News*, 24 July 2007, <http://www.hurriyetdailynews.com/h.php?news=relieved-eu-urges-the-new-government-to-resume-reforms-2007-07-24>.

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

Turkey has signed and ratified the 1966 UN International Covenant on Civil and Political Rights (ICCPR) and its First Optional Protocol that establishes an individual complaint mechanism.⁵⁰

Turkey is member of the Council of Europe and has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁵¹ It signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108) in 1981 but has not yet ratified it.⁵² On a positive note, the Ministry of Transport stated that a delegate from the government will soon be heading to Strasbourg to sign the Convention on Cybercrime and that the Government is willing to ratify the Convention rapidly, in order to maintain and sustain cross-border co-operation on cybercrime.⁵³

In November 2006, the European Court of Human Rights ruled that Turkey infringed the right to privacy of a human rights defender whose premises were searched and whose private professional materials were seized without the requisite authorisation. Taner Kılıç is a board member of the Izmir branch of the Association of Human Rights and Solidarity for Oppressed Peoples (MAZLUM-DER). In June 1999 the now-defunct Ankara State Security Court issued a warrant authorising the search of the headquarters and branches of MAZLUM-DER in order to collect evidence concerning certain acts by the association, allegedly carried out against the "integrity of the country and the secular regime." Maintaining that the situation was urgent, the public prosecutor extended the scope of the search warrant and ordered the search of the homes and offices of the association's general director and board members.⁵⁴

Subsequently, when communicating the search orders issued by the State Security Court and the public prosecutor to the governors, the undersecretary of the Ministry of the Interior specified that not only the homes and offices of the general director and board members should be searched but also the premises of all branch board members. During the search of Kılıç's home, the police confiscated two videotapes and photocopied various

⁵⁰ Turkey signed the ICCPR on 30 April 1968 and ratified it on 18 March 1969. It signed the First Optional Protocol to ICCPR on 3 February 2004 and ratified it on 24 November 2006. The texts of the Covenant and of its First Optional Protocol are available at <http://www2.ohchr.org/english/law/index.htm>.

⁵¹ Signed Rome, 11 November 1950; ratified 18 May 1954, entered into force 18 May 1954, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

⁵² Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 29 January 1981, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

⁵³ "Yıldırım: Siber suç anlaşması imzalanacak," NTVMSNBC, 16 June 2010, <http://www.ntvmsnbc.com/id/25106705>.

⁵⁴ "Rights Defender Wins Case Against Turkey," Turkish Daily News, 5 November 2006, available at <http://www.hurriyetdailynews.com/h.php?news=rights-defender-wins-case-against-turkey-2006-11-05>.

documents taken from his office. Kılıç complained about the search and the seizure of his property.⁵⁵ According to Orhan Kemal Cengiz, lawyer for the applicant, "[t]his case shows that it is high time to think about the rights of human rights defenders", and the decision urges Turkey to revise practices such as frequent house and office searches and property seizure used against human rights defenders.⁵⁶

Turkey has been a member of the Organisation for Economic Co-operation and Development since 1961.

Turkey has signed and ratified the International Covenant on Civil and Political Rights⁵⁷ and adopted the UN Convention on Fight against Corruption, which entered into force in May 2006.

With the motivation and the back wind of EU accession talks in the mid 2000's, the Turkish government accelerated its legalisation actions and drafted several laws, based on related EU regulations such as the Commercial Code, the Data Protection Code, and others. Even though these codes have not yet been enacted, they can be seen as an "alternative" adaptation of EU laws into the Turkish legal system by making the required modifications.

*Updates to the Report published in the 2010 edition of EPHR have been provided by:
Emre Berk, Attorney-at Law at Bener Law Office, Turkey.

⁵⁵ *Id.*

⁵⁶ "Human Rights Defender Wins Case," Turkish Daily News, 5 November 2006, available at <http://www.hurriyetdailynews.com/h.php?news=human-rights-defender-wins-case-2006-11-05>.

⁵⁷ Signed 15 August 2000, ratified 23 September 2003, available at <http://www2.ohchr.org/english/law/ccpr.htm>.

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND*

I. PRIVACY AND DATA PROTECTION FRAMEWORK

CONSTITUTIONAL PRIVACY AND DATA PROTECTION FRAMEWORK

The United Kingdom (UK) does not have a written constitution. There is a growing consensus among the political parties that a more formal constitution and bill of rights is necessary.¹ In the spring of 2010 the Equality and Human Rights Commission, a non-departmental public body established by the Equality Act 2006, published a detailed report investigating the key principles that should underpin a bill of rights, and the policy implications that this would likely entail. The report notes that the circumstances for creating a UK bill of rights are currently unfavourable, citing lack of understanding and enthusiasm among the general public as major obstacles.²

The Human Rights Act 1998 provides for a limited incorporation of the European Convention on Human Rights (ECHR) into domestic law, including the right of privacy.³ The Act came into force on 2 October 2000. Thus far, the courts have cautiously implemented this legislation. A common law right of privacy is slowly emerging in the courts from the law of confidence that has been used as far back as 1849 to protect the unauthorised disclosure of personal data.⁴ The UK House of Lords ruled in October 2003 that there is no general common law tort for invasion of privacy and that the ECHR does not require the UK to adopt one.⁵ However, the Lords ruled in May 2004 that a tabloid newspaper violated model Naomi Campbell's privacy under Article 8 by publishing that she was undergoing drug treatment and printing pictures of her leaving the treatment centre.⁶ The courts have ruled in a series of cases for privacy rights for public figures in their private lives.⁷ However, more recently, courts have shown a willingness to rule in

¹ See Joint Committee on Human Rights, *A Bill of Rights for the UK?* Twenty-ninth Report of Session 2007–08, August 2008.

² Equality and Human Rights Commission, *Developing a Bill of Rights for the UK*, spring 2010, available at http://www.equalityhumanrights.com/uploaded_files/research/developing_a_bill_of_rights_for_the_uk_report_51.pdf.

³ Human Rights Act 1998 (c. 42), available at <http://www.hms0.gov.uk/acts/acts1998/19980042.htm>.

⁴ *Prince Albert v. Strange*, (1849) 1 Mac & G 25.

⁵ *Wainwright and another v. Home Office*, (2003) UKHL 53, (2003) 4 All ER 969, 16 October 2003.

⁶ *Campbell v. MGN Ltd*, (2004) UKHL 22, 2 WLR 1232; see also Information Commissioner – Annual report and accounts for the year ending 31 March 2003, July 2003, available at <http://www.informationcommissioner.gov.uk/>.

⁷ *Douglas v. Hello*, (2005) EWCA Civ 595. Also see *Mosely v. News Group Newspapers*, (2008) EWHC 1777 (QB); *Murray v Big Pictures*, (UK) Ltd (2008) EWCA Civ 446; *McKennitt v Ash*, (2008) QB 73.

favour of the publication of intrusive material if a strong public interest can be shown to exist.⁸

There is a long history of recognising the right to privacy from government intrusion in the UK. The statesman William Pitt in the 18th century said, "The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter, the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement!"⁹

Although the Conservative-Liberal coalition government has indicated an intention to unveil measures that promote privacy, the overall trend during the past ten years has been a steady encroachment upon privacy rights. The UK has been a leader in adopting intrusive surveillance technologies such as biometrics, surveillance cameras, computer databases, and DNA testing, largely implemented without effective public consultation.¹⁰ A recent and widely publicised ranking of 47 countries by the privacy rights watchdog Privacy International found the UK's level of surveillance to be "endemic", worst among EU countries and on par with Russia, China, and Singapore.¹¹ The previous Labour government's tough crime policy and its large parliamentary majority resulted in an unprecedented number of new laws limiting human rights, including freedom of assembly, privacy, freedom of movement, the right of silence, and freedom of speech, leading the former Information Commissioner to warn that the UK was "sleepwalking into a surveillance society".¹²

The privacy picture has improved somewhat under the newly-instituted Conservative-Liberal coalition government. The coalition has taken steps to roll back many of the former government's initiatives. Most notably, the coalition has published a bill intended to cancel the controversial ID cards program, along with the National Identity Register, a proposed central repository for personal data about every British citizen, and the next

⁸ Application by Guardian News and Media Limited and others in *HM Treasury v Mohammed Jabar Ahmed and others*, (2010) UKSC 1; *John Terry v Persons Unknown* (2010) EWHC 119.

⁹ William Pitt, Earl of Chatham, Speech on the Excise Bill in *Bartlett's Familiar Quotations*, 10th ed. (1919); see also e.g. *Entick v. Carrington*, 95 Eng. Rep., (1765), 807 K.B.

¹⁰ For a comprehensive overview of recent developments in the deployment of surveillance technologies in the UK, see FIPR, Technology development and its effect on privacy & law enforcement, February 2004, available at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/technology_and_privacy.pdf, House of Lords Select Committee on the Constitution's, Surveillance: Citizens And The State, HL 18-I & HL 18-II, 6 February 2009, available at <http://www.parliament.the-stationery-office.co.uk/pa/ld/ldconst.htm>.

¹¹ Privacy International, Leading surveillance societies in the EU and the World, September 2006-2007, [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559597](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597); [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-545269](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269).

¹² Information Commissioner's Office, e-newsletter, 3rd edition, November 2006.

generation of biometric passports.¹³ The bill is currently being debated and is almost certain to become law, given the widespread support it enjoys among members of the coalition, and the fact that both coalition partners appeared clearly committed to its aims in their respective election manifestos.¹⁴

PRIVACY AND DATA PROTECTION LAWS AND REGULATIONS

Comprehensive law

Parliament approved the Data Protection Act ("DPA") in July 1998 to implement Directive 95/46/EC.¹⁵ The legislation, which came into force on 1 March 2000, applies to personal data held by government agencies and private organisations. The obligations for entities subject to the DPA, or "data controllers," are enshrined in eight data protection principles. These principles cover, *inter alia*, the obligation to (i) ensure that personal data are used for specific and legitimate purposes, (ii) permit individuals access to their personal data, (iii) provide adequate technical and organisational security for personal data, and (iv) prevent the international transfer of personal data to jurisdictions not recognised to have adequate data protection laws, unless legally recognised mechanisms are deployed to protect the personal data both during and following the transfer. Data controllers are also required to register their processing activities with the Information Commissioner's Office (ICO).

The DPA is quite complex. It has been described by the courts as a "cumbersome and inelegant piece of legislation."¹⁶ The former Information Commissioner observed that it "is not the most elegant or easily understood statute" and "is not written for the casual reader."¹⁷ Its complexity results in it being often incorrectly (and sometimes cynically) cited as a justification for the mishandling of data by public and private authorities.¹⁸ The ICO has criticised organisations for using it as a "duck out" to avoid disclosing information.¹⁹ In June 2010, the European Commission issued a "reasoned opinion" to

¹³ Identity Documents Bill 2010, available at <http://www.publications.parliament.uk/pa/cm201011/cmbills/001/11001.1-4.html>.

¹⁴ The Conservative Party, The Conservative Manifesto 2010, available at http://media.conservatives.s3.amazonaws.com/manifesto/cpmanifesto2010_lowres.pdf; The Liberal Democrats, The Liberal Democrat Manifesto 2010, available at <http://issuu.com/libdems/docs/manifesto?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Fflight%2Flayout.xml&showFlipBtn=true&proShowMenu=true>.

¹⁵ Data Protection Act 1998 (c. 29), available at <http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>.

¹⁶ *Campbell v. MGN Ltd*, Court of Appeal (Civil Division), (2002) EWCA Civ 1373, (2003) QB 633

¹⁷ Information Commissioner's Office, Annual Report, 2004.

¹⁸ See Final Report of the Bichard Inquiry regarding problems of police understanding the DPA rules (2004), available at <http://www.bichardinquiry.org.uk/>; "Couple with No Gas Found Dead," BBC News Online, 22 December 2003, available at http://news.bbc.co.uk/2/hi/uk_news/england/london/3342059.stm.

¹⁹ See http://www.ico.gov.uk/for_organisations/topic_specific_guides/get_clued_up.aspx.

the UK government, which outlined the defects of the UK's data protection framework. In particular, the opinion criticised the difficulty of enforcing the right to have personal data rectified or erased, and the difficulty of claiming compensation for moral damage arising from inappropriate use of personal data.²⁰ A previous notice issued by the European Commission in 2004 also expressed concerns about the UK's insufficient implementation of Directive 95/46/EC in a number of areas.²¹

There has been some confusion about what constitutes "personal data" under UK data protection rules. The UK Court of Appeal issued a controversial decision in December 2003 narrowing the definition of information protected under the Act and limiting individuals' right of access to personal data held in manual files.²² The court took the view that the data must "focus" on a particular individual, and not merely "relate" to an individual in order to constitute personal data protected by the DPA. This decision was criticised by the European Commission in 2004 in the formal notice mentioned above. In 2007, the Article 29 Working Party adopted an opinion setting out a definition of personal data that was clearly wider than the one taken by the UK Court of Appeal.²³ Following this, the ICO issued a guidance note attempting to reconcile the decision of the Court of Appeal with the opinion of the Article 29 Working Party.²⁴ Although the ICO guidance note is observed by most practitioners, a 2008 ruling from the Information Tribunal affirmed that the narrower view of personal data taken by the Court of Appeal remains good law.²⁵

The Isle of Man, Guernsey and Jersey each have data protection laws that are based on the Data Protection Act 1998, and their own independent data protection authorities.

The Isle of Man Data Protection Act 2002 came into force in April 2003. The Office of the Data Protection Supervisor is responsible for enforcement and overseeing compliance.²⁶ The European Commission has declared the Isle of Man an adequate data protection regime.²⁷

²⁰ European Commission, Press Release IP/10/811, 24 June 2010, available at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/811&format=HTML&aged=0&language=EN&guiLanguage=en>.

²¹ "European Commission suggests UK's Data Protection Act is deficient," Out-Law, 15 July 2004, <http://www.out-law.com/page-4717>.

²² *Durant v. Financial Services Authority*, (2003) EWCA Civ 1746.

²³ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

²⁴ Information Commissioner's Office, Determining what is personal data, August 2007, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf.

²⁵ *Tony Harcup and Yorkshire Forward v Information Commissioner*, EA/2007/0058, 5 February 2008.

²⁶ See <http://www.gov.im/odps/>.

²⁷ Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, available at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

The Data Protection (Bailiwick of Guernsey) Law of 2001 was approved in March 2002.²⁸ The Isle of Guernsey Data Protection Commissioner is responsible for enforcement and overseeing compliance.²⁹ The European Commission has declared Guernsey an adequate data protection regime.³⁰

In Jersey, the Data Protection (Jersey) Law went into effect in December 2005.³¹ The Data Protection Commissioner is responsible for enforcement and overseeing compliance.³² The European Commission has also declared Jersey an adequate regime for the protection of personal data.³³

In June 2010, the European Commission issued a reasoned opinion that the Data Protection Act 1998 regime should be amended to better implement Directive 95/46/EC (Data Protection Directive), including as regards the monitoring and enforcement powers of the Information Commissioner's Office. One of the areas of criticism is the fact that the ICO does not have the authority to perform random checks on those using or processing personal data, or to enforce penalties following such checks.

The ICO has released a statement confirming that it will discuss the Commission's concerns with the Ministry of Justice and that it plans to provide input into the UK government's response. The UK now has two months to inform the Commission of measures taken to ensure full compliance with the Directive.

Sector-based laws

There are also several other laws that impact privacy, most notably those governing medical records³⁴ and consumer credit information.³⁵ Other laws with privacy components include: the Rehabilitation of Offenders Act 1974, the Police Act 1997, the Broadcasting Act 1996 (Part VI), the Protection from Harassment Act 1997, and the Human Tissue Act 2004. The House of Commons Culture, Media, and Sport Committee recommended the adoption of a privacy law covering the media in June 2003, but the

²⁸ The Data Protection (Bailiwick of Guernsey) Law, 2001, available at <http://www.dpcommission.gov.gg/2001%20Law/2001%20Law.htm>.

²⁹ At <http://www.dpcommission.gov.gg/>.

³⁰ Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, available at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

³¹ See Office of the Data Protection Commissioner, Legislation <http://www.dataprotection.gov.je/cms/Legislation/>.

³² Homepage <http://www.dataprotection.gov.je/>.

³³ Commission Decision of 8 May 2008 on the adequate protection of personal data in Jersey, available at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

³⁴ Access to Medical Reports Act 1988 and the Access to Health Records Act 1990. The Health and Social Care Act 2001. Mostly repealed by the Data Protection Act 1998.

³⁵ Consumer Credit Act, 1974. Replaced by Consumer Credit Act 2006, available at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060014_en.pdf.

Government immediately rejected the proposal.³⁶ Since then, the court decisions on privacy have led to additional debate on adopting a law but without significant developments.

DATA PROTECTION AUTHORITY

The Information Commissioner's Office is an independent agency that maintains a public register of data controllers and enforces the DPA, the Privacy and Electronic Communication Regulations, and the Freedom of Information Act.³⁷ A new Commissioner, Christopher Graham, was appointed in 2009. As of April 2010, there were 328,164 data controllers registered with the ICO.³⁸ It received 33,234 requests for advice and complaints in 2009-2010, up 30 percent from the previous year. There were nine prosecutions for failure to respond to enforcement notices or for failure to register a database. A significant case from 2009 involved the shutting down of an industry employee blacklist of 3,200 people that had operated for 15 years. However, the conviction resulted in only a £5,000 fine. The ICO has taken enforcement action against 14 companies that paid thousands of pounds for subscription to the blacklist, prohibiting them from using the data for commercial purposes.³⁹

On 6 April 2010, the ICO was granted new powers to impose penalties of up to £500,000 for serious breaches of the data protection principles, strengthening its relatively limited enforcement powers. The ICO has issued guidance on the circumstances under which the new fining powers may be exercised.⁴⁰ According to the guidance, the ICO will need to be satisfied that there has been a serious breach, meaning it is likely to cause substantial damage or distress to the data subject and was either deliberate or negligent. Moreover, the organisation must have failed to take reasonable steps to prevent it. Additionally, the ICO has been granted new powers to audit government departments without consent.⁴¹ There is scope for this audit power to be extended to public authorities and certain private sector data controllers. A code of practice has been published that sets out the new audit

³⁶ House of Commons Culture, Media, and Sport Committee, Privacy and Media Intrusion, Fifth Report of Session 2002–03, June 2003.

³⁷ Information Commissioner's Office, <http://www.ico.gov.uk/>.

³⁸ See Information Commissioner – Annual Report 2009-2010, July 2010, available at <http://www.ico.gov.uk/>.

³⁹ "Blacklisting: ICO bans 14 firms from using data," Construction News, 4 August 2009, available at <http://www.cnplus.co.uk/hot-topics/legal/blacklisting-ico-bans-14-firms-from-using-data/5206177.article>.

⁴⁰ Information Commissioner's Office, Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C(1) of the Data Protection Act 1998, January 2010, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf.

⁴¹ Part 8, Coroners and Justice Act 2009 (c. 25), available at <http://www.legislation.gov.uk/ukpga/2009/25/contents>.

powers.⁴² It remains to be seen whether the ICO's new powers will translate into more numerous and stringent enforcement actions.

The Information Tribunal (formerly the Data Protection Tribunal) can hear appeals of decisions and notices issued by the ICO. Most tribunal decisions relate to the Freedom of Information Act 2000,⁴³ with only a handful relating to the DPA. Of these, the more recent decisions have considered whether information requested by data subjects is personal data capable of being disclosed under the DPA.⁴⁴

MAJOR PRIVACY & DATA PROTECTION CASE LAW

II. FOCUS AREAS

NATIONAL SECURITY, GOVERNMENT SURVEILLANCE & LAW ENFORCEMENT

The Police and Criminal Evidence Act 1984 (PACE) allows the police to enter and search homes without warrant following an arrest for any offence. The police also have the right to stop and search any person on the street where they have a suspicion against the individual. The police stopped and searched over 1.1 million persons and vehicles in England and Wales in 2008-09, up 10 percent from the previous year.⁴⁵

The Office of the Surveillance Commissioners reviews other investigatory techniques under RIPA Part II and the Police Act 1997.⁴⁶ Official figures give an insight into the extent of surveillance operations in the UK. There were 2,681 authorisations including 384 for "intrusive" authorisations for break-ins into homes under the Police Act 1997 and Part II of RIPA over 2008-09.⁴⁷ There were 16,118 authorisations by law enforcement and 9,894 from other public bodies for directed surveillance in the same period. The Commissioners have expressed concern about local authority use of surveillance powers, describing a "serious misunderstanding" of proportionality, inexperience of officers compounded with poor oversight, and "an increasing temptation to use innovative

⁴² Information Commissioner's Office, Assessment Notices Code of Practice, April 2010, available at http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/assessment_notices_code_of_practice.pdf.

⁴³ Freedom of Information Act 2000 (c.36), available at <http://www.legislation.gov.uk/ukpga/2000/36/data.pdf>.

⁴⁴ *Michael O'Connell v Information Commissioner*, EA/2009/0010, 17 September 2009; *Tony Harcup and Yorkshire Forward v Information Commissioner*, EA/2007/0058, 5 February 2008.

⁴⁵ Home Office, Police Powers and Procedures, England and Wales 2008/09, June 2010; See also Anti-terrorist Stop and Searches Target Muslim Communities, but Few Arrests, *Statewatch Bulletin*, Vol. 13 No. 6, November-December 2004.

⁴⁶ Homepage <http://www.surveillancecommissioners.gov.uk/>.

⁴⁷ Annual Report of the Chief Surveillance Commissioner for 2008-09.

technology without properly considering the application of the legislation."⁴⁸ They have also stated that they have concerns about new technologies not yet addressed by Parliament including tracking devices, Automatic Number Plate Recognition (ANPR), covert cameras, and special identification dyes.

Wiretapping, access to, and interception of communications

Interception of communications is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA).⁴⁹ Part I authorises the Home Secretary to issue warrants for the interception of communications and requires providers of "public telecommunications services"⁵⁰ to provide a "reasonable interception capability" in their networks. The Home, Northern Ireland, or Foreign Secretaries of State and the Scottish First Minister normally authorise telephone taps for national security purposes. It further allows any public authority designated by the Home Secretary to access "communications data" without a warrant. This data includes the source, destination, and type of any communication, such as mobile phone location information and partial web browsing logs (note that the full URL is considered content subject to a warrant). Part III of RIPA allows senior members of the civilian and military police, customs, and members of the judiciary to demand that users hand over the plaintext of encrypted material or, in certain circumstances, the decryption keys. Part II sets rules on other types of "human intelligence" powers that had not been previously regulated under UK law. Many legal experts believe that a number of RIPA's provisions violate the ECHR. The Home Office has issued dozens of codes and regulations on its use in the past five years.⁵¹ Currently, evidence obtained from interceptions is not admissible in court although there is a vigorous debate about changing this.

Over 200 agencies, police forces, and prisons are now authorised to intercept communications. Official figures give some indication of how frequently communications are intercepted. In 2009, there were 1,706 warrants for interceptions of telephone and mail issued in England and Scotland under RIPA (down marginally from 1,712 in 2008) and 5,267 modifications (down from 5,334).⁵² The government refuses to

⁴⁸ Annual Report of the Chief Surveillance Commissioner for 2007-08.

⁴⁹ Regulation of Investigatory Powers Act 2000. (c. 23), available at <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>, replacing Interception of Communications Act, 1985 (c. 56), see Y. Akdeniz, N. Taylor, C. Walker, Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights, *Criminal Law Review* 73-90 (February 2001) available at <http://www.cyber-rights.org/documents/crimlr.pdf>.

⁵⁰ "Public telecommunications service" means any telecommunications service that is offered to a substantial section of the public in the UK. These may, and in most cases will, include services offered by private companies.

⁵¹ See Home Office RIPA pages <http://security.homeoffice.gov.uk/ripa/>.

⁵² Report of the Interception of Communications Commissioner for 2009, July 2010. For a historical overview, see Statewatch, Telephone Tapping and Mail-opening Figures 1937-2008, available at <http://www.statewatch.org/uk-tel-tap-reports.htm>.

disclose the number of national security interceptions, claiming that releasing this information could undermine public security.

Requests for communications data are very common, and do not require the grant of a warrant. In 2009, there were over 500,000 such requests. A revised code of practice on acquisition and disclosure of communications data was adopted in October 2007.⁵³ All police forces, intelligence, and security agencies, 474 local authorities, and 110 other public authorities have the authority to obtain access to communications data. There is evidence that RIPA has been used to obtain information unrelated to serious crimes, which has caused heated controversy.⁵⁴ In August 2010, for example, a council in Dorset was revealed to have spied on a family to see if it lived in the right school catchment area.⁵⁵ The Conservative-Liberal coalition has indicated that it will not permit local authorities to exercise powers under RIPA unless they are approved by a magistrate and required for preventing serious crime.⁵⁶ At the time of writing, these changes have not been implemented.

Requests for interceptions and communications data are reviewed by the Interception of Communications Commissioner, a former high court judge who acts more as a cheerleader than a watchdog for the process.⁵⁷ A new Commissioner was appointed in April 2006. Every year the Commissioner has found errors in the process but has also decreed that they were not deliberate and were appropriately remedied. Examples included tapping wrong numbers or monitoring domestic targets using the intelligence services. 36 interception-related errors were recorded in 2009. In one notable case from 2008, using IP data, a person was misidentified as being involved in a paedophile ring and was arrested.

The Investigatory Powers Tribunal hears complaints from individuals who allege that they have been subject to illegal surveillance. It received 157 complaints in 2009, up

⁵³ Home Office, Acquisition and Disclosure of Communications Data Code of Practice, October 2007. Available at <http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop>. FIPR Response to the Home Office, "Consultation on the Revised Statutory Code for Acquisition and Disclosure of Communications Data – Chapter II of Part I of the Regulation of Investigatory Powers Act 2000," September 2006, available at <http://www.fipr.org/060901commsdata.pdf>.

⁵⁴ See The Grim RIPA, Big Brother Watch, May 2010, available at <http://www.statewatch.org/news/2010/may/uk-bbw-grim-ripa-reort.pdf>.

⁵⁵ "Poole council loses school catchment 'spying' tribunal," BBC News, <http://www.bbc.co.uk/news/uk-england-dorset-10839104>.

⁵⁶ HM Government, The Coalition: our programme, May 2010, available at <http://programmeforgovernment.hmg.gov.uk/files/2010/05/coalition-programme.pdf>.

⁵⁷ He noted in his 2003 report that, "I have been impressed by the quality, dedication and enthusiasm of the personnel carrying out this work on behalf of the Government and the people of the United Kingdom." Similar language is found in the 2008 report at 2.2-2.4. See also correspondence between Commissioner and PI, available at

from 136 complaints in 2008. In 2009, the Tribunal found in favour of one complainant for unauthorised interception.

There is a long history of illegal wiretapping of political opponents, labour unions, and others in the UK.⁵⁸ In the late 1970s and 1980s, MI5, Britain's security service, tapped the phones of many left-leaning activists including current MPs and members of the government. Following strong criticism from the European Court of Human Rights (ECtHR), several changes were introduced. In 1985, the ECtHR ruled that police interception of individuals' communications was a violation of Article 8 of the ECHR,⁵⁹ which resulted in the adoption of the Interception of Communications Act 1985. The ECtHR ruled in 1997 that police eavesdropping on a policewoman violated Article 8, which resulted in the adoption of RIPA.⁶⁰ The ECtHR ruled in April 2007 that monitoring an employee's telephone, email, and Internet usage violated Article 8.⁶¹ In July 2008, the Court ruled that the bulk "strategic monitoring" of all communications between the UK and Ireland violated Article 8.⁶² There has also been considerable controversy about the legality of ISPs using a system to monitor the traffic of their users for advertising purposes.⁶³

National security legislation

The United Kingdom has an extensive system of anti-terror legislation that has developed over the past 100 years. Five major anti-terrorism statutes have been introduced in the last ten years.

In December 2001, Parliament approved the Anti-terrorism, Crime and Security Act (ATCS).⁶⁴ ATCS allows the Home Secretary to issue a code of practice for the "voluntary" retention of communications data by communications providers for the purposes of protecting national security or preventing or detecting crime that relates to national security.⁶⁵ Under ATCS, some communications data can be retained for up to a year. An opinion commissioned by the ICO found that access to information retained

⁵⁸ See, e.g., Patrick Fitzgerald & Mark Leopold, *Stranger on the Line*, Bodley Head 1987.

⁵⁹ *Malone v. United Kingdom*, (Application 8691/79), 27 June 1984.

⁶⁰ *Halford v. United Kingdom* (Application 20605/92), 25 June 1997.

⁶¹ *Copland v. United Kingdom* (Application 62617/00), 3 April 2007.

⁶² *Liberty v. United Kingdom* (Application 58243/00), 1 July 2008.

⁶³ "Phorm fires privacy row for ISPs, *The Guardian*," 6 March 2008; Open Letter to the Information Commissioner, 17 March 2008; "EU tells UK to deal with Phorm - or else," *The Register*, 16 July 2008, http://www.theregister.co.uk/2008/07/16/eu_warns_uk_over_phorm/.

⁶⁴ Anti-terrorism, Crime and Security Act 2001 (c.24), available at <http://www.hmso.gov.uk/acts/acts2001/20010024.htm>.

⁶⁵ The Retention of Communications Data (Code of Practice) Order 2003, SI 2003 No. 3175, December 4, 2003; Retention of Communications Data Under Part 11: Anti-Terrorism, Crime & Security Act 2001 - Voluntary Code of Practice, available at <http://www.legislation.hmso.gov.uk/si/si2003/draft/5b.pdf>.

under ATCS for non-national security purposes would violate human rights and would be unlawful.⁶⁶

The Terrorism Act 2000 allows the police to stop and search individuals where there is a "reasonable suspicion" that such individuals are involved in terrorist activities.⁶⁷ Up until July 2010, the police were able to obtain authorisations to stop and search individuals and vehicles without suspicion in certain designated areas (including the whole of London). In a landmark ruling from the ECtHR, the power to stop and search individuals without suspicion was declared a violation of Article 8 of the ECHR.⁶⁸ Following this decision, Home Secretary Theresa May announced in July 2010 that the police would no longer be able to obtain authorisations to search individuals without suspicion, and that vehicles may only be searched where there is "reasonable suspicion" that the relevant individuals are involved in terrorist conduct.⁶⁹ It is important to note that the power to stop and search individuals without suspicion will remain law until the relevant provision is repealed or amended, and could be reinstated by a decision of the Home Secretary in the future.⁷⁰

Official figures show the extent to which stop and search powers under the Terrorism Act have been used in the past few years. There were over 210,000 stops in 2008-09, an increase of 66 percent from the previous year. Less than 1 percent of these stops resulted in an arrest.⁷¹ The NGO Statewatch estimates that many of these stops are made under other legislation and that the official figures represent only half of actual incidents. Individuals of Asian origin are 30 percent more likely to be stopped than other races in London, but thousands have been stopped without reason in an attempt to try and balance the statistics.⁷²

Additional legislation was adopted following the London bombings in July 2005. This focused on other aspects including detention periods, "control orders", and increasing

⁶⁶ Opinion of Ben Emmerson QC and Helen Mountfield, Matrix Chambers, July 2002, available at <http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opinion.htm>.

⁶⁷ Terrorism Act 2000 (c.11), available at http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_5#pt5-pb2-l1g44.

⁶⁸ *Gillian and Quinton v. United Kingdom*, (Application 4158/05), 12 January 2010.

⁶⁹ Statement of Home Secretary Theresa May to the House of Commons, 8 July 2010, available at <http://www.statewatch.org/news/2010/jul/03uk-terr-powers.htm>.

⁷⁰ "It's not the end for stop and search", The Register, 12 July 2010, http://www.theregister.co.uk/2010/07/12/section_44_police/.

⁷¹ Home Office, Police Powers and Procedures, England and Wales 2008/09, June 2010.

⁷² "Terror law used to stop thousands 'just to balance racial statistics'," *The Guardian*, 17 June 2009.

penalties for "encouraging" terrorism.⁷³ The Counter-Terrorism Act 2008 extends the possibilities for collecting DNA and fingerprints.⁷⁴

Data retention

The provisions of the EU Data Retention Directive have been implemented into UK law by the UK's Data Retention (EC Directive) Regulations 2009 ("Retention Regulations"), which came into force in April 2009. The Retention Regulations require that all traffic data, including Internet usage data and mobile location data, be kept for one year. Previous legislation only covered traffic data generated by telephony services. RIPA (see above) sets out which bodies may access retained communications data. A proposal for creating a national database of all communications data was withdrawn after widespread public opposition, although the former government offered companies £2 billion to maintain the capability themselves.

The Home Office then set out proposals in April 2009 to extend requirements on Communications Service Providers (CSPs) to collect, retain, and use communications data. This initiative, known as the Interception Modernisation Programme (IMP), would have required CSPs to collect and retain even more communications data than they do at present. The scope of the data collection and retention obligations under IMP were wide, and would have included data that were not processed for business purposes, such as data relating to Internet-based services, and data that were not subject to the Retention Regulations. CSPs would have been required to organise and process these additional communications data, matching their own data to those of third parties where they had features in common (for example, where they related to the same person or to the same communications device). The government's stated objective was to keep up with developments in communications technology and "to find ways both (i) to ensure that all the potentially relevant data is collected and retained; and (ii) that it is done in a way that allows public authorities to put together an increasing number of fragments to make a coherent whole."⁷⁵ The government framed IMP as an attempt to "maintain" the existing capability of public authorities to access and use communications data. The ICO certainly did not accept that IMP was merely about preserving the status quo; on the contrary, it expressed in stark terms that the proposals would "represent a step change in the relationship between the citizen and the state."⁷⁶ IMP was reported to have been shelved

⁷³ See Clive Walker, "Clamping Down on Terrorism in the United Kingdom," *Jnl of Intl Crim Justice* 4 (2006).

⁷⁴ Counter-Terrorism Act 2008 (c.28), available at http://www.opsi.gov.uk/acts/acts2008/ukpga_20080028_en_1.

⁷⁵ Home Office Consultation, *Protecting the Public in a Changing Communications Environment*, April 2009, available at <http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf>.

⁷⁶ Information Commissioner's Office, *Information Commissioner's response to "Protecting the Public in a Changing Communications Environment"*, 15 July 2009, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_response_home_office_consultation_20090715.pdf.

in autumn 2009. The largest organisation of ISPs condemned this initiative as intrusive and illegal.⁷⁷

National databases for law enforcement and security purposes

The previous Labour government demonstrated an inclination towards the creation of large databases as repositories of information to be used in the fight against crime and in the promotion of wider security. There are indications that the current Conservative-Liberal coalition does not agree with this approach. However, some concerning initiatives are still ongoing. The National Health Service has been in the process of creating a national database of patient records that will have few limits on access. Civil society and doctors' groups have been urging patients to opt out of the system.⁷⁸ The project has had significant technical problems and the government remains locked in a £700 million legal dispute following the withdrawal of a major supplier in 2008.⁷⁹ There have been reports of officials attempting to coerce patients to stay on the system.⁸⁰

Among the initiatives introduced by the former Labour government was a national database of 11 million children under the Children Act 2004.⁸¹ Under this initiative, over 300,000 people had access to children's personal data. Children's advocates and the Parliamentary Joint Committee on Human Rights rightly expressed their concern that the tool violated Article 8 of the ECHR.⁸² This database was shut down by the Conservative-Liberal coalition government in August 2010.⁸³

The UK has the largest per capita DNA database in the world. It has grown rapidly in the last ten years to contain over 5 million samples.⁸⁴ The law was amended in 2001 to allow for the inclusion of samples from individuals who have been acquitted and who have not been charged with an offence (except in Scotland). The law was further amended in 2003 to permit requests for samples in any arrest, no matter how minor or dubious the crime. Over 7 percent of the population is now included in the system and this includes over 800,000 people who have never been convicted of a crime. A number of judges and senior police officers have called for the expansion of the database to cover the entire

⁷⁷ "Internet firms resist ministers' plan to spy on every email," *The Times*, 2 August 2009.

⁷⁸ See Moritz Y. Becker, A formal Security Policy for an NHS Electronic Health Record Service, University of Cambridge, Computer Laboratory, March 2005, available at <http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-628.html>.

⁷⁹ "NHS faces £700m legal action over IT project," *The Independent*, 30 August 2008.

⁸⁰ "Patients 'forced to stay on NHS database'," *The Guardian*, 11 March 2009.

⁸¹ Children Act 2004, (c. 31), available at <http://www.hms0.gov.uk/acts/acts2004/20040031.htm>.

⁸² Joint Committee On Human Rights, Nineteenth Report, 8 September, 2004.

⁸³ "ContactPoint child database scrapped," *The Daily Telegraph*, 6 August 2010.

⁸⁴ The National DNA Database Annual Report 2006-2007; Genewatch, The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy, January 2005 <http://www.genewatch.org>.

population.⁸⁵ The House of Lords ruled in 2004 that DNA and fingerprints could be retained even if there was no conviction.⁸⁶ However, following a public inquiry, the Human Genetics Commission opposed the retention of samples of unconvicted persons.⁸⁷ It was revealed in 2006 that a private company, involved in testing DNA for the government, had been retaining samples secretly, and that the Home Office had given permission for a separate study to investigate whether ethnic backgrounds could be determined by the database.⁸⁸ There are also proposals to keep genetic profiles in the national health database currently being constructed.⁸⁹ Going forward, the government is likely to face pressure to significantly reform these and other similar information repositories.

In a key decision in December 2008, the Grand Chamber of the European Court of Human Rights unanimously ruled that the UK's system of retaining DNA profiles, samples and fingerprints violated Article 8 of the ECHR. The decision rejected the UK's DNA retention policy in strong terms, stating that it was "entirely improper and prejudicial" for samples to be retained where there was no "reasonable relationship of proportionality to the purported aim of crime prevention."⁹⁰ The government responded to this by launching a consultation recommending the retention of information relating to unconvicted persons for six to 12 years. The Association of Chief Police Officers (ACPO) has also urged senior police officials not to follow the ruling and deny requests from those asking to be removed from the database.⁹¹ There is some evidence, however, that the new Conservative-Liberal coalition is willing to more closely align current policy with the Grand Chamber decision. The coalition intends to adopt protections for the DNA database that are similar to those in place in Scotland, where DNA samples from people arrested but not convicted of any other offence must be destroyed after a maximum of five years.⁹²

⁸⁵ "All UK 'must be on DNA database'," BBC, 5 September 2007.

⁸⁶ *Regina v. Chief Constable of South Yorkshire Police*, (2004) UKHL 39.

⁸⁷ Human Genetics Commission, Citizens' Inquiry into the Forensic Use of DNA and the National DNA Database, July 2008. Available at <http://www.hgc.gov.uk/UploadDocs/DocPub/Document/Citizens%20Inquiry%20-%20Citizens%20Report.pdf>.

⁸⁸ "Police DNA database 'is spiralling out of control'," *The Observer*, 16 July, 2006.

⁸⁹ "We'll store DNA samples on a new NHS computer system, admits Department of Health," *Daily Mail*, 31 January 2009.

⁹⁰ *S. and Marper v. the United Kingdom*, (Application 30562/04), 4 December 2008, available at <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>.

⁹¹ "Police told to ignore human rights ruling over DNA database," *The Guardian*, 7 August 2009.

⁹² HM Government, *The Coalition: our programme*, May 2010, available at <http://programmeforgovernment.hmg.gov.uk/files/2010/05/coalition-programme.pdf>.

National and international data disclosure agreements

Nothing to report.

Cybercrime

Nothing to report.

Critical infrastructure

Nothing to report.

INTERNET & CONSUMER PRIVACY

E-commerce

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PEC Regulations") came into force in December 2003.⁹³ The PEC Regulations implement Directive 2002/58/EC on Privacy and Electronic Communications into UK law. The PEC Regulations impose rules on the use of cookies and require opt-in for most email and SMS advertising. The ICO issued guidance in 2007 that messages sent over Bluetooth were not covered by the PEC Regulations.⁹⁴ Overall, the PEC Regulations are not regarded as an effective instrument against the unwanted distribution of spam. A recent survey of UK businesses found that 30 percent do not observe the requirements of the PEC Regulations.⁹⁵ There have also been very few enforcement cases against illegal spamming. In one of the few cases of its kind, in 2007, a spammer who was found to have contravened the requirements of the PEC Regulations was fined £270.⁹⁶ Several UK bodies have signed a Memorandum of Understanding with the US Federal Trade Commission and the relevant Australian government bodies in order to facilitate cooperation in anti-spam efforts. Under a 2005 EU agreement, the Office of Fair Trading (OFT) obtained the power to investigate and seize equipment in spam investigations.⁹⁷

Cybersecurity

The UK has not been successful in fostering a culture of security for personal data. Personal data from government computers are regularly disclosed inadvertently or for

⁹³ The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003 No. 2426, September 18, 2003, available at <http://www.hmso.gov.uk/si/si2003/20032426.htm>; The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004, available at <http://www.opsi.gov.uk/si/si2004/20041039.htm> ; see also "Spam": Report of an Inquiry by the All Party Internet Group, October 2003, available at http://www.apig.org.uk/spam_inquiry.htm.

⁹⁴ Information Commissioner's Office, Bluetooth spam not covered by ICO guidance, 11 October 2007, available at <http://www.ico.gov.uk/upload/documents/pressreleases/2007/bluetooth.pdf>.

⁹⁵ "UK companies 'flouting spam laws'," Silicon.com, 8 January 2007, <http://www.silicon.com/management/cio-insights/2007/01/08/uk-companies-flouting-spam-laws-39165003/>.

⁹⁶ "Court victory hailed as spam stopper," *The Guardian*, 28 December 2005.

⁹⁷ "OFT gains powers to seize spammers' PCs," ZDNet, 28 February 2007, <http://www.zdnet.co.uk/news/security-threats/2007/02/28/oft-gains-powers-to-seize-spammers-pcs-39286106/>.

profit-making purposes. The ICO released two reports in 2006 revealing an extensive illegal trade in personal data among police and private detectives who obtain information through bribery or impersonation.⁹⁸ There have been a series of major losses of personal data in recent years, mostly by government bodies. In one of the most high profile cases, HM Revenue and Customs (HMRC) lost 25 million records belonging to 7.25 million UK families receiving child benefit.⁹⁹ Other major cases include a contractor in Iowa, USA, losing 3 million UK driver records,¹⁰⁰ the Ministry of Defence losing a laptop with the personal data of 600,000 recruits,¹⁰¹ and PA Consulting, a major contractor for the National ID system, losing 377,000 information records that included 84,000 UK prisoners in August 2008.¹⁰² The National Health Service has been a particularly bad culprit, responsible for more than 300 breaches between November 2007 and June 2010.¹⁰³ There have also been numerous incidents in the financial services sector, resulting in large monetary sanctions from the Financial Services Authority. Overall, the ICO received reports of over 400 breaches over the 2009-2010 period. These incidents have led to increased calls for the adoption of a national breach notification law, under which organisations would be compelled to report the loss or misuse of personal data. To date, only a few European Member States, including Germany and Austria, have enacted breach notification legislation.

Online targeted advertising and search engine privacy

Nothing to report.

Online social networks and virtual communities

Nothing to report.

Online youth safety

Nothing to report.

⁹⁸ Information Commissioner's Office, *What Price Privacy?: The unlawful trade in confidential personal information*, May 2006; *What price privacy now? The first six months' progress in halting the unlawful trade in confidential personal information*, December 2006. Available at <http://www.ico.gov.uk/>. See also "Officer jailed for leaking police records to violent criminal," *Out-Law*, 13 April 2007, <http://www.out-law.com/page-7956>.

⁹⁹ "UK's families put on fraud alert," *BBC News*, 20 November 2007, http://news.bbc.co.uk/2/hi/uk_news/politics/7103566.stm.

¹⁰⁰ "No cover-up' on lost driver data," *BBC News*, 22 August 2008,

¹⁰¹ "MoD admits loss of secret files," *BBC News*, 18 July 2008, http://news.bbc.co.uk/2/hi/uk_news/7514281.stm.

¹⁰² "Home Office data loss included drug records," *ZDNet UK*, 27 August 2009, <http://www.zdnet.co.uk/news/security-management/2009/08/27/home-office-data-loss-included-drug-records-39730190/>.

¹⁰³ "NHS top culprit as UK data breaches exceed 1,000", *ZDNet UK*, 1 June 2010, <http://www.zdnet.co.uk/news/compliance/2010/06/01/nhs-top-culprit-as-uk-data-breaches-exceed-1000-40089098/>.

TERRITORIAL PRIVACY

Video surveillance

There has been a proliferation of CCTV cameras throughout Britain. It is estimated that there are over 4 million cameras in Britain, and that the average citizen is recorded over 300 times each day.¹⁰⁴ The camera networks can be operated by police, local authorities, or private companies. Their original purpose was crime prevention and detection, though in recent years the cameras have become important tools for city centre management and the control of "anti-social behaviour". Many of the systems have been enhanced with technology for facial recognition but the agencies that have installed the systems admit that the technology has yet to result in an arrest. It is understood that most CCTV cameras are not operated in compliance with requirements of the DPA.¹⁰⁵

More concerning for the ordinary citizen is the fact that CCTV systems are now being used in connection with other databases. In London, a system for "congestion charging" uses a sophisticated number plate recognition system to charge motorists who drive into central London during business hours. It was revealed that the system was organised in cooperation with the intelligence services, who use it with facial recognition systems to monitor drivers.¹⁰⁶ The NGO No CCTV has also revealed via freedom of information requests that the police intend to make ANPR a "core policing tool".¹⁰⁷ Traffic cameras have also spread across the country. In 2009, the Information Tribunal rejected an application by Privacy International to review the waiver of data protection rights for all number plate identification cameras in central London.

There is a growing body of research demonstrating that these cameras are not very effective as crime prevention tools.¹⁰⁸ The Metropolitan Police have revealed that only 3 percent of crimes are solved using CCTV.¹⁰⁹ An internal report released in 2009 found that only one crime was solved per 1,000 cameras.¹¹⁰ An earlier Home Office study had

¹⁰⁴ Surveillance Studies Network, A Report on the Surveillance Society, September 2006, available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

¹⁰⁵ "Nearly all cameras illegal, says watchdog," *The Times*, 31 May 2007.

¹⁰⁶ "Security Role for Traffic Cameras," *The Observer*, 9 February 2003.

¹⁰⁷ Association of Chief Police Officers (ACPO), ANPR Strategy for the Police Service 2007/2010, available at http://www.no-cctv.org.uk/blog/anpr_-_policing_by_consent.htm.

¹⁰⁸ See The Campbell Collaboration, Effects of Closed Circuit Television Surveillance on Crime, 2 December 2008, available at http://www.campbellcollaboration.org/news_/CCTV_modest_impact_on_crime_printer.shtml.

¹⁰⁹ "CCTV boom has failed to slash crime, say police," *The Guardian*, 6 May 2008, at <http://www.guardian.co.uk/uk/2008/may/06/ukcrime1>.

¹¹⁰ See "1,000 CCTV cameras to solve just one crime, Met Police admits," *Daily Telegraph*, 25 August 2009, available at <http://www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html>.

also identified many problems with these systems. In all but one area studied, crime did not show a statistically significant decrease and even increased in a majority of areas. CCTV also did not improve perceptions about safety significantly and did not change behaviour. In nearly half of the areas, support for CCTV and its perceived effectiveness declined once it was installed.¹¹¹ The ECtHR ruled in January 2003 that a Council's release of CCTV footage of an attempted suicide for a campaign on CCTV violated the relevant person's Article 8 right to privacy.¹¹²

Video surveillance has become more intrusive. Some cameras are fitted with facial recognition technology to identify suspects, and in the last few years there has been a vast rise in the number of cameras incorporating automatic car number plate recognition software (ANPR). In February 2010, the Association of Police Chief Officers revealed that 10,502 ANPR-enabled cameras were passing information to the National ANPR Data Centre.

Between 10 and 14 million photographs are being processed every day, many of which contain images of the vehicle's driver and front-seat passengers. These images will be retained for at least two years. Law enforcement agencies in other EU member states can use the database under the Prüm Treaty, and in April 2008 it emerged that the government has also granted access to the USA.

In January 2010, an *Independent on Sunday* report revealed that police are using the technology to meet government performance targets and raise revenue. The report also said that records stored on the ANPR database are "at least 30 percent inaccurate" leading to wrongful arrests and car seizures.¹¹³

In June 2010, an investigation by *The Guardian* revealed that 150 ANPR cameras, 40 of them "covert", have been installed in predominantly Muslim areas of Birmingham's suburbs to monitor individuals suspected by security agencies of being "extremist".¹¹⁴ Local councillors and members of the Muslim community had been told it was to tackle vehicle crime, drug-dealing, and anti-social behaviour. On 17 June 2010, use of the cameras was temporarily suspended pending a "full and in-depth consultation".

¹¹¹ Home Office Research, Development and Statistics Directorate, "Home Office Research Study 292 Assessing the impact of CCTV," February 2005, available at <http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>.

¹¹² *Peck v. the United Kingdom* (Application 44647/98), January 2003, available at <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=peck&sessionid=57939349&skin=hudoc-en>.

¹¹³ "The laughing policeman: 'Inaccurate' data boosts arrest rate," *The Independent on Sunday*, 17 January 2010, <http://www.independent.co.uk/news/uk/crime/the-laughingpolicemen-inaccurate-data-boosts-arrest-rate-1870416.html>.

¹¹⁴ "Surveillance cameras spring up in Muslim areas – the targets? Terrorists," *The Guardian*, 4 June 2010, at <http://www.guardian.co.uk/uk/2010/jun/04/birmingham-surveillance-cameras-muslim-community>

Location privacy (GPS, mobile phones, location based services, etc.)

Nothing to report.

Travel privacy (travel identification documents, biometrics, etc.) and border surveillance

Nothing to report.

NATIONAL ID & SMART CARDS

The Conservative-Liberal coalition government has announced its intention to cancel the controversial ID cards programme. Parliament is currently discussing a bill intended to repeal legislation implementing ID cards along with the National Identity Register and the next generation of biometric passports.¹¹⁵ Given the widespread support the bill enjoys amongst members of the coalition, its passage into law is highly likely, although the legislation implemented by the former government remains in effect at the time of writing.

There has been no national ID card in the UK since 1952, when the House of Lords ruled that requiring the disclosure of the card was not lawful and the National Registration Act was repealed.¹¹⁶ Since that time, the issue came up every few years and was soundly rejected each time due to public opposition. After 11 September 2001, a series of Home Secretaries proposed the card as a solution while at the same time admitting that it would not stop terrorism, and it was adopted as a government position in 2004.

The Identity Cards Act was approved in March 2006 after years of contentious debate and heated opposition from various parties.¹¹⁷ The Act requires the creation of a central National Identity Register and the issuing of "voluntary" ID cards that will include biometric identifiers. The legislation includes heavy penalties for a large number of new offences including failing to register to receive a biometric scan, and to update a home address. It gives the Home Secretary the power to issue regulations to vastly expand the scope of the scheme, including making the ID card mandatory for certain classes of people and extending use of the register and the types of information held in it. As indicated above, legislation is pending to repeal these proposals.

The bill was only adopted in the face of a constitutional crisis after the Lords refused five times to agree to the bill as adopted by the House of Commons. The bill was strongly opposed by a wide variety of groups including the Conservative party (the official

¹¹⁵ Identity Documents Bill 2010, available at <http://www.publications.parliament.uk/pa/cm201011/cmbills/001/11001.1-4.html>.

¹¹⁶ *Willcock v. Muckle*, June 26, 1951; See Privacy International UK ID Card Page for more details.

¹¹⁷ Identity Cards Act 2006, available at <http://www.opsi.gov.uk/ACTS/acts2006/20060015.htm>.

opposition which initially supported it), the Liberal Democrat party (the third largest political party), the Law Society, and the Information Commissioner.¹¹⁸

The Act called for phasing in the National Identity Scheme over ten years or more years starting in 2008 with biometric visas for non-EEA nationals followed by young people in 2010. Most other implementations have been delayed until 2011 or later. Documents released by the Labour government in March 2007 indicate that they planned to make the scheme universally compulsory by 2014 if the Labour Party were to win the 2010 election. Progress in implementing the scheme was due to technical issues, and by 2008 a number of the major technology companies had withdrawn from the project.¹¹⁹ The first contract was issued in August 2008 to defence contractor Thales.¹²⁰

Estimates suggested that the scheme could cost at least £15 billion to implement, and billions more to integrate with existing public and private sector systems, but the government refused to release many details of the costings claiming reasons of commercial confidentiality.¹²¹

There was continued opposition to the scheme even after its adoption. Public support dropped from 80 percent to around 50:50 for and against, and 82 percent of the public believe there is a danger their personal information will be divulged improperly from the ID database.¹²² Polling from the Home Office estimated that at least 15 million people would refuse to register for the database.¹²³ The Conservative Party announced it would cancel the scheme when next elected into power. The Foundation for Information Policy Research (FIPR) estimates that more than 200,000 illegal requests for information are made each year by private investigators under false pretences.

RFID tags

Nothing to report.

BODILY PRIVACY

Nothing to report.

WORKPLACE PRIVACY

Nothing to report.

¹¹⁸ Heated Debate on ID Cards in the UK," EDRI-gram newsletter, June 29, 2005, number 3.13, available at <http://www.edri.org/edriagram/number3.13/>.

¹¹⁹ Companies abandon ID card project, *The Financial Times*, 23 January 2008.

¹²⁰ Defence group awarded £18m identity card contract, *The Financial Times*, 1 August 2008.

¹²¹ See The Identity Project: as assessment of the UK Identity Cards Bill and its implications, London School of Economics, June 2005. <http://identityproject.lse.ac.uk/>.

¹²² See UK Polling Report, Support for ID Cards <http://ukpollingreport.co.uk/blog/issues/id-cards>. *Daily Telegraph* poll, 12 December 2006

¹²³ Millions to rebel over ID cards, *The Times*, April 8, 2007.

HEALTH & GENETIC PRIVACY

Health privacy

The British Medical Association, amongst others, has already expressed concern that the Spine database system is being rolled out too quickly and there have been recent media reports to the effect that an NHS Trust in Wales is failing to ensure that proper restrictions are being placed on hospital staff accessing patient data.

The police have been criticised for building up a database of protesters. In the case of *Wood v. Commissioner for Police of the Metropolis* (2009),¹²⁴ the Court of Appeal found that the Metropolitan Police had acted unlawfully when it retained photographs which it had taken of an anti-arms trade campaigner.

In March 2009, the Joseph Rowntree Reform Trust published its report "The Database State" which considered 46 databases across the major government departments including the national DNA database, the national pupil database, the NHS detailed care record system, and the automatic number-plate recognition system.

In summary, the report concluded that: a quarter of the 46 databases reviewed were "almost certainly illegal under human rights or data protection law; that they should be scrapped or substantially redesigned" (including, for example, the Contactpoint index of all children in England and the national DNA database); "more than half have significant problems with privacy or effectiveness and could fall foul of a legal challenge" (including, for example, the NHS Summary Care Record and the National Pupil Database); fewer than 15 percent were "effective, proportionate, and necessary with a proper legal basis for any privacy intrusions"; Britain was generally out of line with other developed countries as a result of its comparably greater tendency to centralise and share records on sensitive matters like healthcare and social services; that "the benefits claimed for data sharing are often illusory".

Genetic privacy

Under a voluntary moratorium agreed by the former Labour government and the insurance industry in 2001 and renewed in March 2005 and June 2008, insurance companies will not demand or use the results of genetic tests for policies under £500,000 unless approved first by the Genetics and Insurance Committee. The moratorium lasts until 2014. Tests done for research studies do not have to be disclosed.¹²⁵ The level of protection for employees is less clear.¹²⁶ Certain groups had demanded legal protections

¹²⁴ EWCA Civ 414.

¹²⁵ Concordat and Moratorium on Genetics and Insurance, March 2005, available at http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4106050.pdf.

¹²⁶ See Genewatch, "Genetic Testing in the Workplace," June 2003, available at <http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/GeneticTesting.pdf>.

against genetic discrimination in the Equality Bill, but these were not included in the final draft of the legislation.¹²⁷

FINANCIAL PRIVACY

Nothing to report.

E-GOVERNMENT & PRIVACY

An extensive pilot of e-voting took place in the 2007 elections. A review of the process found that the systems were poorly designed and insecure. There were numerous problems including unreliable registers, incorrect ballot displays, and poorly designed cryptographic receipts.¹²⁸ Some electronic counts had to be abandoned while others had significant delays in counting or severe discrepancies between the counts. The former government rejected suggestions from the Electoral Commission to conduct further pilots before widespread adoption of e-voting.¹²⁹ There is some indication that public support for e-voting is increasing, however. Widespread problems at polling stations in the 2010 elections prompted calls for reform of the voting system, and recent research conducted by Cisco indicates that two-thirds of voters expect to vote online by the time of the next elections.¹³⁰

OPEN GOVERNMENT

The Freedom of Information (FOI) Act was enacted in November 2000.¹³¹ However, its full implementation was delayed until 2005, the slowest implementation of any FOI law in the world. There were over 34,000 requests to central government bodies in 2008, a slight increase from 2007.¹³² A full report for 2009 has not been published at the time of writing, though a statistics bulletin from the Ministry of Justice indicates that central government bodies received 6,857 requests in the first quarter of 2010, an increase of 14

¹²⁷ Equality Act 2010 (c.15), available at http://www.opsi.gov.uk/acts/acts2010/ukpga_20100015_en_1.

¹²⁸ Open Rights Group, May 2007 Election Report, July 2007 <http://www.openrightsgroup.org/e-voting-main/>.

¹²⁹ The Government's response to the Electoral Commission's recommendations on the May 2007 electoral pilot schemes, October 2007, available at <http://www.justice.gov.uk/docs/gov-response-elec-comm.pdf>.

¹³⁰ See <http://www.publicnet.co.uk/news/2010/07/15/study-shows-big-rise-in-demand-for-online-voting/>.

¹³¹ Freedom of Information Act 2000 (c.36), available at <http://www.cfoi.org.uk/foiact2000.html>. For detailed information on the Act, see the Campaign for Freedom of Information's website <http://www.cfoi.org.uk>.

¹³² Ministry of Justice, Freedom of Information Act 2000: 4th Annual Report on the Operation of the FOI Act in Central Government 2008, June 2009.

percent over the first quarter of 2009.¹³³ One notable request on the expenses of MPs led to the resignation of the Speaker of the House and many other MPs.

Appeals against denials of information are to the Information Commissioner and then, until 18 January 2010, the Information Tribunal. On that date the Information Tribunal ceased to exist and all its work was transferred to the new General Regulatory Chamber. From 18 January, all FoI appeals will be heard either in the First-tier Tribunal (Information Rights) or in the Upper Tribunal.¹³⁴

The utility of the Act has been limited by extensive delays in responding by public bodies and to appeals by the Information Commissioner, many of which can last up to five years. In June 2002, the Scottish Parliament approved a Freedom of Information Act¹³⁵ that is regarded as somewhat stronger than the UK Act. It also went into effect in January 2005.

It is also limited by the breadth of the exemptions on which a public body may rely in denying access to information. In the recent case of *BBC v. Sugar*, the Court of Appeal held that for the purposes of the Freedom of Information Act 2000 Sch.1, information that was established to have been held for a genuine journalistic purpose was effectively exempt from production under the Act even if it had also been held for other purposes. Where the exemption is qualified, however, it may be possible to argue that the public authority has reached the wrong conclusion. The Information Commissioner recently decided that the Cabinet Office was wrong to rely on the exemptions contained in sections 37(1)(b) (the conferring of honours), 40(2) (personal data) and 41 (breach of confidence) in refusing to disclose whether Lord Ashcroft had given an undertaking.¹³⁶ In the Commissioner's view, the public interest in transparency in the honours system outweighed the Cabinet Office's claim that disclosure would be "unwarranted and prejudicial to the rights and legitimate interests" of Lord Ashcroft.

The Act is also fundamentally undermined by the existence of the Ministerial veto. The Labour government relied on the veto to avoid having to publish the minutes of cabinet meetings at which the 2003 invasion of Iraq was discussed. Labour had argued that doing so would damage cabinet government and invoked section 53 of the Act to veto first the Information Commissioner's decision that the public interest should prevail, and later that of the Information Tribunal, which upheld the Commissioner's decision.¹³⁷

¹³³ Ministry of Justice, Freedom of Information Act 2000 – Statistics on implementation in central government Q1: January – March 2010, 24 June 2010, available at <http://www.justice.gov.uk/foi-quarterly-stats-jan-mar-2010a.pdf>.

¹³⁴ Transfer of Functions Order 2010 (SI 2010/22).

¹³⁵ See <http://www.scotland.gov.uk/consultations/government/dfib-00.asp>.

¹³⁶ Cabinet Office Ref: FS50197952 28/01/2010)

¹³⁷ Cabinet Office and Dr Christopher Lamb v IC (EA/2008/0024 & 0029 27 January 2009)

The Commissioner said at the time: "Anything other than exceptional use of the veto would threaten to undermine much of the progress towards greater openness and transparency in government since the FoI Act came into force."

Despite this, on 10 December 2009, Straw announced that he was exercising his powers of veto for a second time – this time to prevent disclosure of minutes of the Cabinet Ministerial Committee on devolution to Scotland and Wales and the English regions in 1997.¹³⁸

The coalition government have committed themselves to increased transparency in government, to "throwing the doors open of public bodies" and to creating a new "right to data". It remains to be seen what these commitments will mean in practice.

In the draft of their Freedom Bill they proposed that the Information Commissioner be given greater powers to ensure that all data controllers, both in the public and private sector, are complying with the Act and punish those who are not. This would mean giving the Commissioner the same power to inspect private companies as public bodies.

The Ministry of Justice have recently announced that they intend to amend the FOIA by November 2011 to incorporate further organisations.

OTHER RECENT FACTUAL DEVELOPMENTS

Nothing to report.

III. NON-GOVERNMENTAL ORGANISATIONS' ADVOCACY WORK

The Foundation for Information Policy Research (FIPR)'s highest-impact activity between 2008 and 2010 was the 2009 report "Database State"¹³⁹ that examined a number of government systems that hold information on many citizens. The report found that 11 of them almost certainly infringed the ECHR. It was extensively covered in the media. The opposition parties, the Conservatives and the Liberal Democrats, who now form the Government, adopted its arguments and a number of its ideas. The new government abolished a number of systems, including the proposed ID card and the ContactPoint children's database. The debate continues on health systems.¹⁴⁰

Another of the Foundation for Information Policy Research's high-impact campaign in 2008 was against the behavioural advertising system devised by the commercial company Phorm. FIPR documented how it worked and demonstrated that it was illegal. The government disagreed, but FIPR convinced the European Commission to intervene, which it eventually did by taking the view that if Phorm was legal in the United Kingdom, the country's implementation of the *acquis communautaire* was defective. It

¹³⁸ Cabinet Office FS50100665 23/6/09)

¹³⁹ See <http://www.lightbluetouchpaper.org/2009/03/23/database-state/>.

¹⁴⁰ See also <http://www.lightbluetouchpaper.org/2010/06/17/database-state-latest/> and <http://www.lightbluetouchpaper.org/2010/09/13/research-public-opinion-and-patient-consent/>.

subsequently threatened legal action. The United Kingdom is now changing its regulations.¹⁴¹

IV. INTERNATIONAL OBLIGATIONS & INTERNATIONAL COOPERATION

The UK is a member of the Council of Europe (CoE) and has signed and ratified the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108)¹⁴² and the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁴³ In November 2001, the UK signed the CoE Convention on Cybercrime but is yet to ratify this instrument.¹⁴⁴ The UK is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

* We are grateful to the assistance and guidance of the contributors to the update of this report for the 2010 edition: Anna Mazzola, Hickman & Rose, United Kingdom; Daniel Cooper, Mark Young, Shamma Iqbal, and Philip Christofides, Covington & Burling, United Kingdom; Ross Anderson, Computer Laboratory, Cambridge University, United Kingdom.

¹⁴¹ See <http://www.lightbluetouchpaper.org/2008/04/04/the-phorm-webwise-system/> and <http://www.lightbluetouchpaper.org/2008/04/22/stealing-phorm-cookies/>.

¹⁴² Signed 14 May, 1981; ratified 26 August 1987; entered into force December 1, 1987.

¹⁴³ Signed 4 November, 1950; ratified 8 March 1951; entered into force September 3, 1953.

¹⁴⁴ Signed 23 November 2001.

EUROPEAN UNION

I. PRIVACY AND DATA PROTECTION IN THE EU

OVERVIEW OF THE LEGAL AND INSTITUTIONAL FRAMEWORK

The European Union (EU) is an economic and political union of 27 member states. Its structure, as well as the ways in which it ensures the protection for fundamental rights, have been profoundly affected by the entry into force on 1 December 2009 of the Lisbon Treaty,¹ with significant implications for the insurance of the right to privacy and the right for the protection of personal data.

Currently, fundamental rights are protected in the EU legal framework through three complementary perspectives: (a) as general principles of the EU derived from the European Convention of Human Rights (ECHR) and the constitutional traditions common to member states;² (b) as defined by the Charter of Fundamental Rights of the European Union³ (hereafter, "the Charter");⁴ and (c) as protected by the European Convention on Human Rights, to which the EU shall accede.⁵

The Charter, which is now generally binding in the EU, was originally proclaimed in 2000. It introduced then as a major novelty the separate recognition of a fundamental right to privacy, in its Article 7,⁶ on the one hand, and a fundamental right to the protection of personal data, in its Article 8,⁷ on the other. This latter right establishes that data concerning individuals must be processed fairly, for specified purposes, and on the basis of their consent or a legitimate basis laid down by law, that everyone has a right to

¹ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, OJ C 306, 17 December 2007, at 1-271. EU treaties and relevant adopted or under adoption legislation as well as other official documents are also available online at http://europa.eu/documentation/legislation/index_en.htm.

² Art. 6(3) of the Consolidated Version of the Treaty on European Union (TEU). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 83, 30 March 2010, at 1-388.

³ Charter of Fundamental Rights of the European Union, OJ C 83 30 March 2010, at 389-403.

⁴ Art. 6(1) TEU.

⁵ Art. 6(2) TEU.

⁶ Art. 7 of the Charter, "Respect for private and family life," reads: "Everyone has the right to respect for his or her private and family life, home and communications".

⁷ Art. 8 of the Charter, "Protection of personal data," reads: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

access and rectify the data collected concerning them,⁸ and that compliance with these rules shall be subject to control by an independent authority.⁹

In turn, the European Court of Justice (ECJ), which is based in Luxembourg and is the highest court for the interpretation of EU law, began acknowledging the existence of a European right to the protection of personal data.¹⁰

The Lisbon Treaty put an end to the division of the EU into three pillars, which during decades had determined the development of EU law, and thus of EU data protection law. Since the entry into force of the Lisbon Treaty, the EU has in Article 16 of the Treaty on the Functioning of the European Union (TFEU) a new legal basis for the regulation of data protection, which is applicable to all processing of personal data, be it in the private or the public sector, including the processing in the area of police and judicial cooperation.¹¹ This new legal basis could be used in the context of the revision of what is currently the main EU legal instrument for the protection of personal data, i.e., the Data Protection Directive.

THE DATA PROTECTION DIRECTIVE

Directive 1995/46/EC, known as the Data Protection Directive,¹² defines the basics of personal data protection that EU member states have to transpose into national law, where the actual regulation and enforcement are taking place. The provisions of the Directive can be invoked in the national courts against member states' data protection rules in order to oust the application of rules contrary to those provisions.

⁸ Art. 8(2) of the Charter.

⁹ Art. 8(3) of the Charter.

¹⁰ ECJ, Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, Judgment of the 16 December 2008; Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, Judgment of 29 January 2008, § 63.

¹¹ Art. 16 TFEU reads: "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the member states when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union." Art. 16 TFEU also applies to processing in the area of Common Foreign and Security Policy (CFSP), as far as EU institutions process personal data (Art. 39 TEU provides for a specific legal basis for data processing by the member states in the second pillar; it reads: "In accordance with Article 16 of the Treaty on the Functioning of the European Union and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the member states when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities").

¹² Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23 November 1995, at 31-50.

The Data Protection Directive applies to any automated processing of personal data and any other handling of personal data that form part of a filing system.¹³ Personal data is defined as any information that relates to an "identified or identifiable natural person".¹⁴ Processing operations concerning public security, defence, state security, and activities of the member states in areas of criminal law were left outside the scope of the Directive. Data processing by a natural person in the course of purely private and household activities is exempted as well.¹⁵

The Directive provides a list of legitimate reasons allowing for the processing of personal data¹⁶ and mandates that the person responsible for determining the purposes and means of the processing of personal data, referred to as the "data controller", ensures compliance with principles relating to data quality.¹⁷ The data controller has also information duties toward the person whose data are processed, who is designated the "data subject", applicable whenever personal data is collected directly from the person,¹⁸ but also when obtained otherwise.¹⁹ Strengthened protection is foreseen for the use of sensitive personal data relating, for example, to health, sex life, or religious or philosophical beliefs.²⁰ The data controller is additionally mandated to implement appropriate technical and organisational measures against unlawful destruction, accidental loss, or unauthorised alteration, disclosure, or access.²¹

Data subjects' individual rights, as established by the Directive, are: the right to access, which includes the right to acquire from the data controller confirmation as to whether or not data relating to them are being processed and information on the purposes of the processing, the categories of data concerned, and the recipients to whom the data are disclosed, as well as the right to obtain the rectification, erasure, or blocking of data the processing of which does not comply with the provisions of the Directive;²² a right to

¹³ *Id.*, Art. 3(1).

¹⁴ *Id.*, Art. 2(a).

¹⁵ *Id.*, Art. 3(2).

¹⁶ *Id.*, Art 7.

¹⁷ *Id.*, Art. 6(1).

¹⁸ *Id.*, Art. 10.

¹⁹ *Id.*, Art. 11.

²⁰ *Id.*, Art. 8.

²¹ *Id.*, Art. 17.

²² *Id.*, Art. 12. The ECJ clarified the meaning of this Article in: Case C 553/07, *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer*, Judgment of 7 May 2009.

judicial remedy;²³ and the right to object to certain data processing practices.²⁴ Any person who has suffered damage as a result of an unlawful processing operation is entitled to receive compensation from the data controller.²⁵

In line with the fundamental right to data protection as established by Article 8 of the Charter,²⁶ the Data Protection Directive requires member states to ensure that independent supervisory authorities monitor the application of its provisions.²⁷ The ECJ recently clarified the meaning of the requirement of "complete independence" of data protection supervisory authorities, emphasising that is not compatible with being subject to State oversight.²⁸ Supervisory authorities must be endowed with investigative powers and effective powers of intervention, such as powers to order blocking, erasure, and destruction of data, or to impose a temporary or permanent ban on processing.²⁹

The Data Protection Directive set up a consultative body called the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, or Article 29 Data Protection Working Party (hereafter, WP29).³⁰ This body is made up of representatives of member states' supervisory authorities, and welcomes also a representative of the European Data Protection Supervisor (EDPS), a supervisory authority put in place in 2004 (more information below).

The Data Protection Directive provides a mechanism by which transfers of personal data outside the territory of the EU have to meet a level of processing "adequate" to the one prescribed by the Directive's provisions.³¹ A finding by the European Commission of an adequate level of protection in a country outside the EU effectively clears the transfer of personal data to that third country. European Commission's decisions on the adequacy of the protection of personal data in third countries presently cover Argentina, the Canadian Personal Information Protection and Electronic Documents Act, Andorra, the Bailiwick of Guernsey, the Bailiwick of Jersey, the Isle of Man, the Faeroe Islands, and

²³ Directive 1995/46/EC, *supra* at Art. 22.

²⁴ *Id.*, Art. 14.

²⁵ Unless the data controller proves he is not responsible for the event given rise to the damage, *Id.*, Art. 23.

²⁶ Art. 8(3) of the Charter, *supra*.

²⁷ Directive 1995/46/EC, *supra* at Art. 28.

²⁸ ECJ, Case C-518/07, European Commission v. Federal Republic of Germany, Judgment of 9 March 2010.

²⁹ Directive 1995/46/EC, *supra* at Art. 28(3).

³⁰ *Id.*, Art. 29.

³¹ *Id.*, Art. 25. This is however not the only possibility for transfers to third countries to take place (see, in particular, Art. 26 of Directive 1995/46/EC).

Switzerland.³² Commercial transfers of EU data to the US can take place under the so-called Safe Harbour Agreement.³³

The ECJ establishes the interpretation of EU law that member states' courts must take into account when applying national law in order to stay in line with EU law. The ECJ has ruled on the Data Protection Directive in a number of instances. In a 2003 judgment, it made it clear that the Directive's wide scope applies also to processing of personal data within the public sector, and confirmed that the Directive can be invoked by interested parties in national courts.³⁴ In another 2003 ruling, the ECJ established that the Directive applies to websites, and that the uploading of personal information to the Internet does not trigger the provision for transfers of personal data to third countries even though the web page is universally accessible.³⁵

REVIEW OF THE DATA PROTECTION DIRECTIVE

EU institutions are currently considering the possibility to review the Data Protection Directive. In 2009, the European Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data, opening the way to such a revision. In late 2010 the Commission released a Communication on outlining its plans for changes.³⁶

The WP29 publicly expressed its support for the revision of the Directive, notwithstanding the fact that it considers that existing data protection principles are still relevant. In an *ad hoc* document,³⁷ it advanced substantive suggestions, such as: to clarify some key notions of data protection law (notably, "consent" and "transparency");³⁸ to

³² Updated decisions on adequacy findings are published at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

³³ Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), OJ L 215, 25 August 2000, at 7–47.

³⁴ ECJ, Joined Cases C-465/00, C-138/01 and C-139/01, Rechnungshof, Judgment of 20 May 2003.

³⁵ RCJ, Case C-101/01, Bodil Lindqvist, Judgment of 6 November 2003.

³⁶ European Commission, 'A comprehensive approach on personal data protection in the European Union, Brussels, 4 November 2010, COM(2010)609Final.

³⁷ The Article 29 Data Protection Working Party and the Working Party on Police and Justice, "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to the protection of personal data," 1 December 2009, Brussels.

³⁸ In addition, the complex interplay between the roles of "data controllers" and "data processors" in a globalised world had been tackled in a previous Opinion: The Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010, Brussels.

introduce some additional principles (such as "privacy by design"³⁹ and "accountability",⁴⁰ to modernise some arrangements (e.g. by limiting bureaucratic burdens, but also by improving the protection of data subjects⁴¹); to establish a comprehensive legal framework, applying also to police and judicial cooperation in criminal matters; and to improve the conditions for data transfers to third countries, promoting international standards and new rules on applicable law, as well as regulating by law the use of Binding Corporate Rules (BCRs).

PRIVACY AND ELECTRONIC COMMUNICATIONS

The EU has taken specific measures to ensure the protection of privacy and personal data in the field of telecommunications. In 1997 the Telecommunications Privacy Directive (Directive 1997/66/EC) was adopted, replaced in 2002 by the e-Privacy Directive (Directive 2002/58/EC),⁴² then amended in 2006⁴³ and in 2009.⁴⁴

The e-Privacy Directive applies to publicly available electronic communications services in public telecommunications networks in the EU. It regulates the processing of so-called "traffic" and "location data" ("traffic data" being the data necessary for the provision of communications, and "location data" being the data giving the geographic position of terminal equipment), as well as unsolicited communications ("spam"), cookies, and spyware, among other things.

³⁹ Encouraging the integration of data protection and privacy requirements since the early design and creation of the technology, especially in risky areas. See also EDPS, Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 19 March 2010, Brussels.

⁴⁰ Defined as the data controllers' ability to demonstrate that they have taken all the necessary data protection measures. See, on this subject, The Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010, Brussels.

⁴¹ For instance, via the introduction of class actions, or by providing easier and more affordable complaint procedures.

⁴² Directive 1997/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, OJ L 24, 30 January 1998, at 1–8. The Directive required member states to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector, and introduced provisions on security (Ar. 4), the confidentiality of the communications (Art. 5); traffic and billing data (Art. 6); itemised billing: (Art. 7); the presentation and restriction of calling and connected line identification (Art. 8); automatic calling forwarding (Article 10); directories of subscribers (Art. 11); unsolicited calls (Art. 12); and technical features and standardisation (Art. 13).

⁴³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), OJ L 201, 31 July 2002, at 37–47.

⁴⁴ *Cfr.* Section "The data retention directive," *infra*.

The 2009 review of the e-Privacy Directive⁴⁵ modified the previous text in various ways. First, it laid down a legal definition of data breaches.⁴⁶ Providers of communications services falling under the scope of the Directive are obliged to notify breaches to the competent national authorities, as well as to subscribers or customers likely to be adversely affected by the breach (i.e. by identity theft, reputational loss, etc.), and unless they can demonstrate that they have implemented appropriate security measures to protect the data. Such notification shall be accompanied by a list of the measures suggested to counter the breach, and an inventory of all breaches that have happened should be created.⁴⁷ To this end, supervisory authorities were granted extended competences. They gained the necessary investigative powers and resources to monitor service providers, stop infringements, and enforce the Directive's provisions. In addition, they acquired the means to pursue effective cross-border cooperation.⁴⁸

Second, the revision strengthened measures on spyware and cookies, as well as spam. The former can be installed in the terminal equipment of subscribers, to gain access to information already stored in them, only with the explicit consent of the subscriber or the user, given after having been provided with clear information, in accordance with Directive 1995/46/EC, and after having been offered the right to refuse such access, unless such access is needed for the strict purposes of transmission of a communication or to provide an explicitly requested service.⁴⁹ As for spam, infringements of the provisions on unsolicited communications can now be remedied via legal proceedings, by both individuals and legal persons.⁵⁰

THE DATA RETENTION DIRECTIVE

In 2002, the e-Privacy Directive had introduced the possibility for member states to pass laws mandating the retention of communications data for security purposes.⁵¹ In 2006,

⁴⁵ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18 December 2009, at 11-36 (to be transposed into national laws by 25 May 2011).

⁴⁶ Art. 2(2)(c) of Directive 2009/136/EC: "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

⁴⁷ *Id.*, Art. 2(4).

⁴⁸ *Id.*, Art. 2(10).

⁴⁹ *Id.*, Art. 2(5) (resulting in the amended Art. 5(3) of Directive 2002/58/EC). See, on the issue: The Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, 22 June 2010, Brussels.

⁵⁰ *Id.*, Art. 2(7).

⁵¹ Art. 15(1) of Directive 2002/58/EC.

the EU amended the e-Privacy Directive by enacting the Data Retention Directive (Directive 2006/24/EC),⁵² which obliges member states to require communications providers to retain communications data for a period of between six months and two years. Member states had until September 2007 to transpose the requirements of the Directive into national laws, but were entitled to postpone implementation regarding Internet access, Internet telephony, and Internet email until March 2009. At the beginning of 2010, seven member states had not yet adopted relevant national legislation.⁵³ Implementations of the Data Retention Directive vary per member state. The most remarkable differences concern the retention period, the data to retain, the types of crimes that would justify access to the data, and the methods for law enforcement to access the data. The European Commission has brought action against various member states for failing to satisfactorily transpose the Data Retention Directive into their legal frameworks, in some cases already resulting in judgments confirming the failure to duly transpose its provisions.⁵⁴

At the time of its adoption, the WP29 issued an opinion on the Data Retention Directive in which it asserted that "[t]he decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish".⁵⁵ The WP29 further noted that the Directive lacked some adequate and specific safeguards as to the treatment of communication data and left room for diverging interpretation and implementation by the member states in this respect.

Ireland brought an action seeking the annulment of the Data Retention Directive directly before the ECJ,⁵⁶ based on the argument that it had not been adopted on an appropriate

⁵² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-63.

⁵³ Austria, Belgium, Greece, Ireland, Luxembourg, Poland, and Sweden. *Cfr.* The Article 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action: compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, WP 172, 13 July 2010, Brussels.

⁵⁴ See, notably: ECJ, Case C-189/09, *European Commission v Republic of Austria*, Judgment of 29 July 2010; Case C-185/09, *European Commission v Kingdom of Sweden*, Judgment of 4 February 2010; Case C-202/09, *European Commission v Ireland*, Judgment of 26 November 2009; Case C-211/09, *European Commission v Hellenic Republic*, Judgment of 26 November 2009; Case C-394/10, *European Commission v Grand Duchy of Luxembourg*, action brought on 4 August 2010.

⁵⁵ The Article 29 Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, WP 119, 25 March 2006, Brussels, at 2.

⁵⁶ ECJ, Case C-301/06, *Ireland v Council of the European Union*, European Parliament, available from <http://curia.europa.eu/>.

legal basis. More than 40 civil liberties NGOs and professional associations based in different countries took the opportunity to submit a letter to the ECJ with a petition for the annulment of the Directive.⁵⁷ In February 2009, the ECJ established that the Directive was adopted on the correct legal basis and, without further analysis on the issue of privacy, dismissed the action seeking annulment.⁵⁸

At national level, different legal actions have attacked national laws transposing the Data Retention Directive. Digital Rights Ireland filed a lawsuit against the Irish Government to the High Court in September 2006.⁵⁹ The case argues that the Irish data retention law breaches fundamental principles of human rights and is therefore contrary to the Irish Constitution as well as Irish and EU data protection laws.⁶⁰ In Germany, 34,000 individual citizens challenged the German transposition of the Data Retention Directive at the German Federal Constitutional Court, making it the largest legal action before this court ever.⁶¹ The final judgment of the German Federal Constitutional Court was delivered on 2 March 2010.⁶² Additional relevant case law was pronounced by the Romanian Constitutional Court, on 8 October 2009,⁶³ and by the Bulgarian Administrative Court on 11 December 2008.⁶⁴ In accordance with the provisions of the Data Retention Directive,⁶⁵ the European Commission has carried out an evaluation of its application and impact in autumn 2010.

PERSONAL DATA PROTECTION AND ACCESS TO EU DOCUMENTS

In 2001, a Regulation was adopted to make applicable the content of the Data Protection Directive for data processing undertaken by the institutions of the European Communities

⁵⁷ Arbeitskreis Vorratsdatenspeicherung, "European NGOs Ask Court to Annul Data Retention Directive", 8 April 2008, available at http://www.vorratsdatenspeicherung.de/content/view/216/79/lang,en/#_note-0.

⁵⁸ ECJ, Case C-301/06, *Ireland v European Parliament*, Council of the European Union, Judgment of 10 February 2009.

⁵⁹ Digital Rights Ireland, "DRI Brings Legal Action over Mass Surveillance," 14 September 2006, available at <http://www.digitalrights.ie/2006/09/14/dri-brings-legal-action-over-mass-surveillance/>.

⁶⁰ *Id.*

⁶¹ Arbeitskreis Vorratsdatenspeicherung, "Constitutional Complaint Filed against German Telecomms Data Retention Act," 31 December 2007 available at <http://www.vorratsdatenspeicherung.de/content/view/184/79/lang,en/>.

⁶² Vorratsdatenspeicherung(Data retention) BVerfG 2 March 2010, 1 BvR 256/08, available at http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

⁶³ Decision No. 1258, Romanian Constitutional Court, 8 October 2009, published in the Romanian Official Monitor, No. 789, 23 November 2009.

⁶⁴ Decision No. 13627, Bulgarian Supreme Administrative Court (Върховния административен съд), 11 December 2008.

⁶⁵ Directive 2006/24/EC, *supra* at Art. 14.

(EC), namely Regulation (EC) No. 45/2001.⁶⁶ This Regulation did not only establish the EDPS, but is also relevant, *inter alia*, in reference to the access to documents held by EU institutions.

Access to documents held by EU institutions is governed by Regulation (EC) No. 1049/2001.⁶⁷ The relation between access to documents and the protection of personal data has been clarified by the ECJ in the context of a case that opposed the European Commission, on the one hand, to a private company (The Bavarian Lager Co.) supported by the EDPS.⁶⁸ In its judgement on the case, the ECJ confirmed the applicability of EU data protection provisions in this field, and underlined that the application of such data protection provisions cannot be reduced to a mere examination of whether an interference in the sense of Article 8 of the ECHR has taken place.⁶⁹

THE AREA OF FREEDOM, SECURITY AND JUSTICE (AFSJ)

The former "third pillar" of the EU generally covered cooperation in the fields of justice and home affairs. The protection of personal data processed in the context of activities in this area, which had been left unregulated by the Data Protection Directive, were addressed through a number of different EU data protection provisions. These were commonly adopted in relation with the many specific information systems or agencies set up in the area, creating a sort of legislative patchwork. Usually, these legal instruments refer to the Council of Europe's Convention No. 108 as the benchmark for their data protection provisions.

After many years of discussions on the possibility to establish a horizontal data protection instrument for the whole "third pillar",⁷⁰ the Council Framework Decision 2008/977/JHA was adopted on 27 November 2008.⁷¹ The scope of application of this Framework

⁶⁶ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12 January 2001, at 1- 22.

⁶⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31 May 2001, at 43-48.

⁶⁸ ECJ, Case C-28/08 P, *European Commission v. The Bavarian Lager Co. Ltd*, Judgment of 29 June 2010.

⁶⁹ *Id.*, § 58-59.

⁷⁰ The EDPS issued three Opinions on the subject: EDPS, Third opinion of 27 April 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ C 139, 23 June 2007, at 1; Second Opinion of 29 November 2006 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ C 91, 26 April 2007, at 9; Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final), OJ C 47, 25 February 2006, at 27.

⁷¹ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ 350, 30 December 2008, at 60–71.

Decision is however extremely limited. In fact, it is exclusively concerned with the protection of personal data exchanged between member states and not subject to any other EU-level data protection provisions. The innovations introduced by the Lisbon Treaty may eventually affect the existence of this Framework Decision.

Over the years, specific data protection instruments have been building up different structures for monitoring the implementation of data protection law in this area. For instance, for Europol, which is the EU criminal intelligence agency, data protection supervision is in the hands of the Europol Joint Supervisory Body.⁷² In the context of Eurojust, whose objective is to improve EU-wide investigations and prosecutions, data protection monitoring is the responsibility of the Eurojust Joint Supervisory Body.⁷³

DATA PROCESSING IN THE AREA OF FREEDOM, SECURITY AND JUSTICE (AFSJ)

In 2010, the European Commission issued an overview of the numerous EU measures in place, under implementation or under consideration regarding the collection, storage, or cross-border exchange of personal information for the purpose of law enforcement or migration management.⁷⁴ The measures have been taken by EU institutions over the past years in relation both to security purposes, such as counterterrorism, and objectives linked to the creation of an area without internal borders (the "Schengen area"), and sometimes in relation to a blurred aim, somehow encompassing security targets and other concerns, such as immigration. In its 2010 overview, the European Commission conceded that two recently designed large-scale information systems, the Visa Information System (VIS), which is to store biometric data of visa applicants, and the Schengen Information System (SIS), as well as its upcoming successor, Schengen Information System II (SIS II), do not respect one of the most fundamental principles of EU data protection, namely the purpose limitation principle.⁷⁵

Other existing EU large-scale information systems include Eurodac, established by Council Regulation 2725/2000,⁷⁶ which is a database storing the fingerprints of asylum seekers (the system is supervised by the EDPS together with the competent national Data

⁷² See Europol Joint Supervisory Body's homepage at <http://europoljsb.consilium.europa.eu/default.asp?lang=EN>.

⁷³ Compare Rules of Procedure on the Processing and Protection of Personal Data at Eurojust (2005), OJ C 68/1, available at http://www.eurojust.europa.eu/official_documents/eju_dp_rules.htm.

⁷⁴ European Commission, Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice, COM(2010) 385 final, 20 July 2010, Brussels.

⁷⁵ *Id.*, at 22.

⁷⁶ Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15 December 2000.

Protection Authorities (DPAs)).⁷⁷ Among the EU initiatives that may be coming up in relation to the processing of individuals on the move, can be mentioned the creation of a so-called "Entry/Exit System" (EES),⁷⁸ an information system that is expected to record the time and place of entry, as well as of length of authorised stay, of all third-country nationals entering the Schengen area for the purpose of immigration control, and an Electronic System of Travel Authorisation (ESTA) for the collection of data on third-country nationals not subject to visa requirements before their arrival at EU borders.⁷⁹

The Custom Information System (CIS) was established in 1995 by the former third pillar Convention on the use of information technology for customs purposes.⁸⁰ CIS's aim is to enable national customs services to exchange and disseminate information on smuggling activities and requests for action. Some of these information are personal data. A Joint Supervisory Authority consisting of member states' DPAs is responsible for supervising CIS.

In order to improve personal data sharing among EU and member states' law enforcement agencies, different efforts have been made in the recent years to create "interoperability" between databases.⁸¹ "Interoperability", i.e., the blurring of boundaries between databases established for different purposes, containing information on different categories of individuals, accessed by different types of authorities and operating with different methods, poses a serious threat to the well-established data protection principles of purpose limitation and proportionality.

EU institutions are also considering the creation of a new agency, possibly called Agency for the Operational Management of Large-Scale Information Technology (IT) Systems in

⁷⁷ Council Regulation (EC) No. 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62, 5 March 2002, at 1-5.

⁷⁸ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13 February 2008, Brussels, at 7.

⁷⁹ *Id.*, at 5.

⁸⁰ Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, OJ C 316, 27 November 1995, at 34-47. In 1997, Council Regulation (EC) No. 515/97 of 13 March 1997 also established the CIS for the purposes of mutual assistance in respect of customs and agricultural matters. See OJ, L 082, 22 March 1997, at 1-16.

⁸¹ According to the Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (COM/2005/0597 final), Brussels, 24 November 2005, "interoperability" is the "ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". Regrettably the commission considered "Interoperability" a "technical rather than a legal or political concept. This is disconnected from the question of whether the data exchange is legally or politically possible or required".

the Area of Freedom, Security and Justice,⁸² to take care of the operational management of SIS II, VIS, Eurodac, and any other future large-scale IT system established in the area of freedom, security and justice.

Data processing exchanges in the EU additionally occur through channels that do not require the establishment of any new databases. In 2005, seven member states⁸³ signed a treaty in Prüm to enhance cross-border police and judicial cooperation, especially with respect to the fight against terrorism, cross-border crime, and illegal migration. Under the Treaty, member states grant one another access rights to their automated DNA analysis files, automated fingerprint identification systems, and vehicle registration data. In 2006, Germany and Austria became the first countries in the world to match their DNA databases.⁸⁴ The provisions of the Prüm Treaty have since then been integrated into the EU legal framework.⁸⁵

Another EU legal instrument promoting the exchange of information between relevant law enforcement authorities is the Framework Decision 2006/960/JHA. The Framework Decision establishes a regulatory regime under which law enforcement authorities of the member states are allowed to exchange "effectively and quickly" between them (but also with Europol and Eurojust) "information and/or intelligence for the purposes of conducting criminal investigations or criminal intelligence operations."⁸⁶

Efforts to boost the exchange of personal data in the contest of mutual legal assistance in criminal matters in the EU have also focused on facilitating the exchange of criminal records between national authorities. The recently adopted Framework Decision 2009/315/JHA on the exchange between member states of information extracted from their criminal records⁸⁷ aims to define modalities in which a member state where a conviction is handed down against a national of another member state transmits the information on such a conviction to the member state of the convicted person's

⁸² European Commission, Amended Proposal for a Regulation (EU) No ... / ... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010) 93 final, 19 March 2010, Brussels.

⁸³ Austria, Belgium, France, Germany, Luxembourg, Spain, and the Netherlands.

⁸⁴ "The Treaty of Prüm Makes Europe Safer - EU Police Forces Share Data," German Ministry of the Interior, 15 March 2007, at http://www.eu2007.bmi.bund.de/nn_1059824/EU2007/EN/DomesticPolicyGoals/News/Content__News/Hanning__dbb.html.

⁸⁵ See Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6 August 2008, at 1-11; See also Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA, OJ L 210, 6 August 2008, at 12-72.

⁸⁶ Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the member states of the European Union, OJ L 386 29 December 2006, at 89-100.

⁸⁷ Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between member states, OJ L 93, 7 April 2009, at 23-32.

nationality. On the basis of the above-mentioned Framework decision, the Council adopted Decision 2009/316/JHA on the establishment of the European Criminal Records Information System (ECRIS).⁸⁸ In its design, ECRIS is a decentralised information technology system based on the national criminal records databases. All criminal records data shall be stored solely in databases operated by the member states. member states shall take the necessary measures to comply with the provisions of both the above-mentioned legal instruments by April 2012.

In recent years EU institutions have been strongly supporting increased surveillance of the EU's physical borders. They have established Eurosur, a border surveillance technical framework targeting the improvement of border security through data exchange and coordination of activities,⁸⁹ and of Frontex, the European Agency for the Management of Operational Cooperation at the External Borders, created⁹⁰ to coordinate border-control surveillance operations. The possibility for Frontex to process personal data, and in particular to transmit it to Europol, is increasingly being discussed.

In the EU the collection, analysis and sharing of personal information for law enforcement and security purposes also involves activities by the private sector. The so called "privatisation of law enforcement activities" consists of calling on private entities (companies or professions) to cooperate with State authorities in the prevention or fight of criminal activities like terrorism. This cooperation takes different forms: retention of communications data,⁹¹ sharing of passenger name records,⁹² and the collection of information by financial and other kind of private entities for anti money-laundering purposes. With regard to this form of cooperation, Directive 2005/60/EC aims to prevent the use of the financial system for the purpose of money laundering and terrorist financing.⁹³ It applies to financial and credit institutions, as well as to certain legal and natural persons working in the financial sector. These entities are required to identify the customer and verify his/her identity, obtain information on the purpose and intended

⁸⁸ Council decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ L93, 7 April 2009, at 33-47.

⁸⁹ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the creation of a European border surveillance system (EUROSUR), COM(2008) 68 final, 13 February 2008, Brussels.

⁹⁰ Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25 November 2004, at 1-11.

⁹¹ *Cfr.* Section "The data retention Directive," *supra*.

⁹² *Cfr.* *infra* this Section and Section "The PNR data exchange Agreements".

⁹³ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25 November 2005, at 15-36. See also Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the member states in respect of exchanging information, OJ L 271, 24 October 2000, at 4-6.

nature of the business relationship. Furthermore, they must file a suspicious transaction report when there is suspicion of money laundering or terrorist financing, regardless of any exemption or threshold.⁹⁴ These suspicious transaction reports are transmitted to and processed by Financial Intelligence Units usually placed either within law enforcement agencies or administrative bodies reporting to Ministries of Finance. These reports can then be transmitted to competent authorities, including law enforcement agencies and Foreign FIUs. On that basis criminal investigations might be launched if necessary.

These forms of surveillance that make use of information held in the private sector involves the gathering, storing, and sharing with national authorities of a vast category of personal data generated by the individual in his/her ordinary and everyday life, and mostly in carrying out legitimate activities.

The Stockholm Programme,⁹⁵ the policy document orientating the development of the AFSJ for the period 2010-2014, confirms the trend towards reinforced data processing practices, while addressing the interplay between privacy intrusive techniques and the need to protect the right to private life and data protection.⁹⁶ The Programme notably calls for the development of an Internal Security Strategy (with its own external dimension), which makes extensive use of information management and exchanges, based on an Information Management Strategy underpinned by the principle of availability⁹⁷ and that of interoperability,⁹⁸ i.e., the technical possibility to conflate databases.

Among others, the Stockholm Programme suggests to restore the project for an EU-wide Passenger Name Record (PNR) system for law enforcement purposes.⁹⁹ This system would allow for the collection of data registered during the purchase of airline tickets

⁹⁴ *Id.*

⁹⁵ The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C 115, 4 May 2010. The Programme was issued in November 2009.

⁹⁶ *Id.*, at 18.

⁹⁷ See The Hague Programme, OJ C 53, 3 March 2005, at 1. See also EDPS, Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005)490 final), 28 February 2006, OJ C 116, 17 May 2006, at 8. The principle of availability refers to the possibility for law enforcement officers in one member state to obtain information from law enforcement agencies of another member state in the same conditions as law enforcement officers of the latter member state.

⁹⁸ See *supra* in the text.

⁹⁹ The idea was initially advanced in conjunction with the beginning of the negotiations with the United States to conclude the first PNR data exchange Agreement (see below) (European Commission, Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, COM(2003) 826, 16 December 2003). Nonetheless, a concrete proposal was only presented four years later (European Commission, Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes {SEC(2007) 1422} {SEC(2007) 1453} /* COM/2007/0654 final).

("PNR data")¹⁰⁰ of international flights passengers from the air carriers by national authorities designated by the member states, called Passenger Information Units (PIUs). The PIUs would use the PNR data, *inter alia*, for "carrying out a risk assessment of the passengers in order to identify the persons requiring further examination".¹⁰¹ The EU Fundamental Rights Agency (FRA),¹⁰² the EDPS,¹⁰³ and the WP29¹⁰⁴ have issued critical opinions on the possible establishment of this system.

EU-US DATA TRANSFERS

The Stockholm Programme also supports the proposal for an agreement of information sharing for law enforcement purposes with the United States (US). The agreement would be based on the work carried out by the informal High Level Contact Group (HLCG), which was established in 2006 in order to study how to bridge the differences between the EU and the US data protection regimes to foster data sharing for law enforcement purposes across the Atlantic. In fact, transatlantic information exchanges, and more precisely, unidirectional data transfers from the EU to the US, have been growing exponentially in the last decade. EU data protection laws, however, has been regularly portrayed as an obstacle to these data flows.

The activities of the HLCG finished in 2009 with the adoption of an Addendum to the Final Report of the HLCG.¹⁰⁵ Its work was devoted to identify principles shared between

¹⁰⁰ PNRs are different from Advanced Passengers Information (API) data, which is the information contained in the machine-readable zone (MRZ) of the passports. PNR data can contain up to 60 fields, partially overlapping with but exceeding Advanced Passengers' Information data, and are not official, verified data.

¹⁰¹ European Commission, Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes, *supra* at Art. 3.3.

¹⁰² Opinion of the European Union Agency for Fundamental Rights on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 28 October 2008.

¹⁰³ EDPS, Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 20 December 2007, OJ C 110, 01 May 2008, at 1.

¹⁰⁴ The Article 29 Data Protection Working Party and the Working Party on Police and Justice, Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, WP 145, 05 December 2007, Brussels.

¹⁰⁵ Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection, 23 November 2009, Brussels, available at <http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf>. The EDPS issued an Opinion on the Final Report: EDPS, Opinion on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 11 November 2008, OJ C 128, 06. June 2009, at 1. The Addendum addressed a series of issues previously described as pending. In particular: 1) Consistency in private entities' obligations during data transfers; 2) Equivalent and reciprocal application of privacy and personal data protection law; 3) Preventing undue impact on relations with third countries; and 4) Specific agreements regulating information exchanges and privacy and personal data protection.

the EU and the US¹⁰⁶ and, when possible, to reach common definitions for the principles.¹⁰⁷ As for the choice of the most adequate form for the discussed instrument, the HLCG strongly supported the adoption of a binding international agreement.

Both the EU and the US have subsequently endorsed the idea of working towards an international binding agreement on data protection and data sharing.¹⁰⁸ In January 2010, the European Commission launched a public consultation to collect opinions with a view to the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes,¹⁰⁹ setting in motion the institutional debate on the issue at EU level.

One of the main challenges emerging from these developments is the level of equivalency between the institutional frameworks of the EU and US. Another key challenge is how this agreement will govern other and future EU-US data exchange mechanisms, such as those related to the processing for security purposes in the US of data originally collected in the EU by private entities, in the context of unrelated activities – for instance in the context of the PNR or the so-called SWIFT data transfers.¹¹⁰

THE PNR DATA EXCHANGE AGREEMENTS¹¹¹

In 2001 the US Government began demanding access to the reservation systems of foreign carriers in order to gain access to Passenger Name Records, i.e., detailed

¹⁰⁶ The principles identified were: 1) Purpose Specification/Purpose Limitation; 2) Integrity/Data Quality; 3) Relevant and Necessary/Proportionality; 4) Information Security; 5) Special Categories of Personal Information (sensitive data); 6) Accountability; 7) Independent and Effective Oversight; 8) Individual Access and Rectification; 9) Transparency and Notice; 10) Redress; 11) Automated Individual Decisions; and 12) Restrictions on Onward Transfers to Third Countries.

¹⁰⁷ Common definitions were identified for nine out of twelve principles. A common definition of "redress" could not be reached; it was only possible to agree that any redress process should result in effective remedy; the definition of "independent and effective oversight" incorporated the structural differences of the two regimes, and, finally, the definition of "transparency and notice" only clarified the type of information to be made available to data subjects.

¹⁰⁸ EU-US Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom, and Security", adopted in Washington D.C. on 28 October 2009, at 6, available at <http://register.consilium.europa.eu/pdf/en/09/st15/st15184.en09.pdf>.

¹⁰⁹ The result of the consultation is available at http://ec.europa.eu/homeaffairs/news/consulting_public/consulting_0005_en.htm.

¹¹⁰ Another related issue is the relation between the agreement and agreements negotiated between the US and EU member states.

¹¹¹ All relevant documents are available on the Commission's website, under the paragraph "US - United States - Transfer of Air Passenger Name Record (PNR) Data," at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm#countries.

biographical and intelligence information on travellers.¹¹² Compliance with the request would require that airlines would be in breach of EU data protection law, whereas non-compliance could have led to economic sanctions from the US Government. Following the intervention of the European Commission, negotiations between the EU and the US were launched on how to resolve the two legal systems.¹¹³

A first agreement¹¹⁴ was finalised and signed in May 2004, accompanied by a Council Decision concerning the conclusion of an agreement on the processing and transfer of personal data¹¹⁵ and, based on CBP's Undertakings,¹¹⁶ an European Commission Decision on the adequate protection of those data.¹¹⁷ Hence the US was allowed to access directly the airline companies' reservation systems to "pull" the data needed. The agreement was reached amidst the doubts and criticism of the privacy community,

¹¹² More concretely, by Section 115 of the US Aviation and Transportation Security Act (ATSA) (The United States of America, Congress, Transportation and Aviation Security Act, 19 November 2001). In 2001, the Customs and Border Protection Bureau started demanding international air carriers operating flights to or from, or across the US territory, grant access to their automated reservation and departure control systems' data to obtain PNR data.

¹¹³ European Commission, Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, COM(2003) 826, 16 June 2003, Brussels.

¹¹⁴ Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20 May 2004, at 84–85.

¹¹⁵ Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20 May 2004, at. 83–85.

¹¹⁶ Letter from Commissioner Bolkestein to US Secretary Tom Ridge, Department of Homeland Security, 18 December 2003.

¹¹⁷ Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (notified under document number C(2004) 1914), OJ L 235, 6 July 2004, at 11–22.

especially the Article 29 Working Party of European privacy regulators,¹¹⁸ and, for different reasons, the airline companies.

The European Parliament voiced its criticism by adopting a resolution, and by filing two actions for annulment before the ECJ¹¹⁹ against the Council and Commission's Decisions allowing the adoption of the Agreement.¹²⁰ The ECJ did not consider all of the European Parliament's pleas, but annulled the two Decisions on the grounds that they had been adopted on the wrong legal basis. Since they pursued an aim falling within the scope of "public security and the activities of the State in areas of criminal law", the choice of a "first pillar" legal basis was incorrect.¹²¹ The ECJ therefore set a deadline (September 2006) for the adoption of a new agreement.

¹¹⁸ The Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, 24 October 2002, WP 66; Opinion 4/2003 of the Art. 29 Working Party, 13 June 2003, WP 78; Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), WP 87; Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 22 June 2004, WP 95 2 February 2004; Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, WP 97, 30 September 2004. The criticism of WP29 regarding the first agreement revolved around the proportionality of the measure as opposed to its purposes, the challenges to the principles of data protection, the technical features of the exchanges (in particular, it considered that the information sharing should happen by means of a "push" instead of a "pull", i.e. by asking the airline companies to send the US the requested data, instead of allowing the US to extract the needed data (which reduces consistently the possibility of oversight)) and the choice of the legal framework for the exchange.

¹¹⁹ ECJ GCh (Grand Chamber), Joined cases C-317/04 and C-318/04, *European Parliament v Council of the European Union* (C-317/04) and *Commission of the European Communities* (C-318/04), Judgment of 30 May 2006.

¹²⁰ In particular, in Case C-317/04, the European Parliament entered six pleas for annulment: the incorrect choice of Article 95 EC as legal basis for Decision 2004/496/EC and breach of, respectively, the second subparagraph of Article 300(3) EC, Article 8 of the ECHR, the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith. In Case 318/04, the European Parliament introduced four pleas for annulment, namely *ultra vires* action, breach of the fundamental principles of the Directive 95/46/EC, breach of fundamental rights, and breach of the principle of proportionality.

¹²¹ The Article 29 Data Protection Working Party, Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, 14 June 2006, WP 122; Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, 27 September 2006, WP 124.

Given the tight deadline set by the Court, the parties entered into negotiations for an Interim Agreement,¹²² signed in October 2006.¹²³ The new text¹²⁴ did not differ substantially from the first one and was met with renewed criticism and increased awareness.

A third Agreement was finalised within the time limits established by the sunset clause of the Interim Agreement.¹²⁵ It consisted of an international agreement¹²⁶ signed by both parties, and two letters, whose legal relation with the agreement was not clarified.¹²⁷ Although the new text addressed some of the substantial concerns raised by EU's different bodies since the beginning of the data exchanges,¹²⁸ it was not immune from criticism.¹²⁹ Since the entry into force of the Lisbon Treaty there have been strong demands to adopt a new agreement.

¹²² Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298, 27 October 2006, at 27–28.

¹²³ Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298, 27 October 2006, at 29–31.

¹²⁴ Which contained a sunset clause and was accompanied by two letters (Letter from the "US Department of Homeland Security" (PNR interpretations); Reply by the Council Presidency and the Commission to the letter from the USA's Department of Homeland Security).

¹²⁵ Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L 204, 4 August 2007, at 16–17.

¹²⁶ Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) OJ L 204, 4 August 2007, at 18–25.

¹²⁷ The first one explained how the United States Department of Homeland Security (DHS) handles the collection, use, and storage of PNR data, and the second one acknowledged its receipt.

¹²⁸ The Article 29 Data Protection Working Party, A common EU approach to the use of Passenger Name Record (PNR) data for law enforcement purposes, 31 January 2007; Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities, 15 February 2007, WP 132 and its Annex: Short notice for travel between the European Union and the United States; Workshop on EU approach towards a new passenger data agreement. This Workshop brought together national data protection authorities and other interested parties and was not a meeting of the Article 29 Working Party, 26 March 2007, Report.

¹²⁹ The Article 29 Data Protection Working Party, Opinion No. 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, 17 August 2007, WP 138; Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008, 24 June 2008, WP 151.

It should be noted that the EU has also signed PNR data exchange agreements with other countries, such as Australia.¹³⁰

TERRORIST FINANCING TRACKING PROGRAMME (TFTP)

In 2006, the New York Times unveiled¹³¹ the access of the US Treasury Department authorities to financial records held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), based in Belgium. Under the Terrorist Financing Tracking Programme (TFTP), US authorities accessed, through the US branch of the company and by subpoenas, financial records of both US and foreign citizens, including EU citizens, for the purposes of identifying, tracking, and pursuing terrorists. The issue caused strong criticism among the privacy community,¹³² already sensitised by the PNR *affaire*. EU authorities entered into transatlantic negotiations to regulate the access to and processing of EU citizens' banking data. As a result, EU member states too could access the result of the processing activities by US authorities.

Pending an international agreement, SWIFT adhered to the Safe Harbour Agreement and adopted a new "distributed architecture", allowing intra-European messages to be processed and stored in the European data centres. In addition, the US Treasury clarified issues concerning its access and processing of data obtained by SWIFT and offered assurances. As a result, an *interim* agreement was signed in November 2009¹³³ with the explicit intention of negotiating a proper agreement after the entry into force of the Lisbon Treaty.¹³⁴

The European Parliament, which has been granted by the Lisbon Treaty new powers in relation with international agreements, voted down the agreement in February 2010¹³⁵ on

¹³⁰ Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service, OJ L 213, 8 August 2008, at 49–57.

¹³¹ Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror," *The New York Times*, 23 June 2006, available at <http://www.nytimes.com/2006/06/23/washington/23intel.html>

¹³² EDPS, Opinion on the role of the European Central Bank in the SWIFT case, 1 February 2007, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2007/07-02-01_Opinion_ECB_role_SWIFT_EN.pdf; the Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, 22 November 2006.

¹³³ Simon Taylor, "EU Agrees New Bank Data Deal with US," *European Voice*, 30 November 2009 available at <http://www.europeanvoice.com/article/2009/11/eu-agrees-new-bank-data-deal-with-us/66563.aspx>.

¹³⁴ Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L 8, 13 January 2010, at 9–10.

¹³⁵ European Parliament Press Release, SWIFT: European Parliament votes down agreement with the US, Justice and home affairs, 11 February 2010, available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//EN>.

grounds of insufficient data protection, a concern also expressed by the EDPS.¹³⁶ Consequently, new negotiations started, and a Draft Council Decision was submitted in June 2010.¹³⁷ Although recognising the improvements made, the Council had failed to convince its critics, including the EDPS,¹³⁸ the WP29 together with the Working Party on Police and Justice¹³⁹ and some MEPs.¹⁴⁰ In spite of this, the EP found that the final agreement in combination with the legally binding commitments in the Council Decision met most of its demands, and therefore gave consent to the conclusion of the agreement on 5 July 2010.¹⁴¹

KEY REGULATORY ACTORS

THE ARTICLE 29 WORKING PARTY

The European Data Protection Supervisor (EDPS) is one of the key actors in the area of EU privacy and data protection.¹⁴² It is responsible for monitoring the EU administration's processing of personal data, advising on policies and legislation that concern or have an impact upon the right to privacy and the right to personal data

¹³⁶ EDPS, Comments on different international agreements, notably the EU-US and EU-AUS PNR agreements, the EU-US TFTP agreement, and the need of a comprehensive approach to international data exchange agreements, 25 January 2010.

¹³⁷ Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme (TFTP II), 28 June 2010, available at http://register.consilium.europa.eu/servlet/driver?page=Result&lang=EN&ssf=DATE_DOCUMENT+DESC&fc=REGAISEN&srm=25&md=400&typ=Simple&cmsid=638&ff_TITRE=TFTP&ff_FT_TEXT=&ff_SOUS_COTE_MATIERE=&dd_DATE_REUNION=.

¹³⁸ EDPS, Opinion of 22 June 2010 on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme (TFTP II).

¹³⁹ Article 29 Data Protection Working Party and the Working Party on Police and Justice, Letter from Mr. Jacob Kohnstamm, Chairman of the Art. 29 Working Party and Mr. Francesco Pizzetti, Chairman of the Working Party on Police and Justice addressed to Mr. Juan Fernando Lopez Aguilar, Chairman of the LIBE Committee regarding EU-US Terrorist Finance Tracking Programme Agreement (TFTP II Agreement), 25 June 2010.

¹⁴⁰ See the Recommendation on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Programme (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE)) Committee on Civil Liberties, Justice and Home Affairs, Minority Resolution, at 10-11.

¹⁴¹ *Id.*, Draft European Parliament Legislative Resolution on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Programme (11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178 (NLE)), at 5-9.

¹⁴² See EDPS's homepage at <http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en>.

protection, and co-operating with similar authorities (member states Data protection Authorities mainly through the participation to the WP29).

THE ARTICLE 29 WORKING PARTY

The WP29 serves as a platform for exchange and coordination between the supervisory authorities of the EU member states, and serves also an important role as consultative body.¹⁴³ The tasks of the WP29 are laid down in Article 30 of the Data Protection Directive and Article 15 of the e-Privacy Directive: examine any question covering the application of the national measures adopted under EU data protection law in order to contribute to their uniform application; provide the European Commission opinions on the level of protection in the Community and in third countries; advise the European Commission on any measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; provide opinions on codes of conduct drawn up at EU level.

The WP29 can make, on its own initiative, recommendations on all matters relating to privacy and data protection in the EU. It has conducted consultations on data protection issues related to different subjects,¹⁴⁴ and has published opinions on many different subjects, including the introduction of biometrics into passports and visas, the protection of children's personal data, standard contractual clauses for the transfer of personal data to processors established in third countries, or an industry proposal for a privacy and data protection impact assessment for RFID applications.¹⁴⁵ The opinions of the WP29 are a common point of reference for interpretation of EU data protection law.

OTHER NETWORKS OF DATA PROTECTION AUTHORITIES

There exist in Europe various networks of data protection authorities, formed by their own initiative. They include:

- the European Conference of Data Protection Authorities: representatives of data protection authorities of the member states of the EU and of the Council of Europe meet annually, together with sub-national authorities and EU joint supervisory bodies in the field of police, justice, and security. Their 2010 conference, held in Prague, was devoted to a series of issues such as EU/US data protection standards in the area of police and judicial co-operation in criminal matters, the use of body scanners for airport security and the future of privacy and data protection in Europe.

¹⁴³ See http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

¹⁴⁴ Such as intellectual property rights, RFID, video surveillance, binding corporate rules, electronic health records and most recently on the protection of children's personal data. WP29 online consultations, available at http://ec.europa.eu/justice/policies/privacy/workinggroup/consultations/index_en.htm.

¹⁴⁵ Documents adopted by WP29 are available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm.

- the Central and Eastern Data Protection Authorities (CEEDPA). In 2001, the Data Protection Commissioners from the Czech Republic, Hungary, Lithuania, Slovakia, Estonia, Latvia, and Poland signed a joint declaration agreeing to closer cooperation and assistance.¹⁴⁶ These countries have since been joined by Bulgaria, Romania, Croatia and Macedonia. The 12th Meeting of the Central and Eastern Europe Data Protection Commissioners took place on May 2010 in Sopot (Poland), and was attended by delegations from Albania and Moldova.

European Network and Information Security Agency

The European Network and Information Security Agency (ENISA) is an EU agency, which formally came into being in 2004.¹⁴⁷ The agency assists the European Commission, the member states, and the private sector in meeting the requirements of network and information security. ENISA also follows the development of standards, promotes risk assessment activities and interoperable risk management routines, and produces studies on those issues that impact public and private sector organisations.

The European Union Agency for Fundamental Rights (FRA)

The European Union Agency for Fundamental Rights¹⁴⁸ (FRA), based in Vienna, was established by Council Regulation 168/2007.¹⁴⁹ It replaced the European Monitoring Centre on Racism and Xenophobia (EUMC).

The FRA assists EU institutions, and member states in implementing EU law when they take measures or decide courses of action, in order to ensure full compliance with fundamental rights.¹⁵⁰ These include the fundamental rights as recognised by the ECHR and the Charter. The Agency is entitled, among other things, to inform the public, develop compatibility standards, conduct surveys, and formulate and publish conclusions or opinions, either on its own initiative or at the request of the European Commission, Council or European Parliament, on issues relating to data protection and privacy.¹⁵¹ To carry out its tasks, it cooperates with an array of EU and international bodies and institutions; especially the Council of Europe, to avoid duplication of work, but also member states and the civil society.¹⁵²

¹⁴⁶ Central and Eastern Europe Data Protection Authorities Webpage: <http://www.ceecprivacy.org/>.

¹⁴⁷ ENISA's homepage <http://www.enisa.europa.eu/index.htm>.

¹⁴⁸ FRA's homepage http://fra.europa.eu/fraWebsite/home/home_en.htm.

¹⁴⁹ Council Regulation No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L 53, 22 February 2007, at. 1-14.

¹⁵⁰ *Id.*, Art. 2.

¹⁵¹ *Id.*, Art. 4.

¹⁵² *Id.*, Art. 7.

THE COUNCIL OF EUROPE

The Council of Europe is distinct from the EU. In 1950 the Council of Europe adopted the European Convention on Human Rights, which is currently applicable in all EU member states.¹⁵³ Article 8 paragraph 1 of the ECHR declares that everyone has the right to respect for his private and family life, his home and his correspondence.¹⁵⁴ Paragraph 2 states that the above mentioned right is not absolute in that it may be acceptable for public authorities to limit it when the "interference" is "in accordance with law" and "necessary in a democratic society" in pursuit of one or more of the following legitimate aims: "in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The European Court of Human Rights (ECtHR), based in Strasbourg, is the highest court for the interpretation of the ECHR. It has been clarifying over the years the protective scope of Article 8 of the ECHR, notably in relation with the processing of personal data. The Court has in particular established that the right to respect for private life of Article 8 of the ECHR includes a series of positive obligations for states, which may involve the adoption of measures designed to secure the protection of personal data in the sphere of relations between individuals.¹⁵⁵ In many judgments, the Court explicitly or implicitly refers to data protection principles.¹⁵⁶

Following the advancements of information technologies, the Council of Europe issued a separate Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981 (known as "Convention No. 108").¹⁵⁷ Parties to this Convention, which include all EU member states, are required to implement it into their national laws. Convention No. 108 is open to any countries that have enacted legislation "in accordance with" the standards it establishes; and it was amended in 1999 making it

¹⁵³ See <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=15/11/2010&CL=ENG>.

¹⁵⁴ *Id.*

¹⁵⁵ ECtHR, Appl. No. 20511/03, 17 July 2008, *I. v. Finland*, Judgment, §§ 36-38.

¹⁵⁶ See, for example, ECtHR, Appl. No. 9248/81, 26 March 1987, *Leander v Sweden*, Judgment, § 48; ECtHR GCh, Appl. No. 14310/8828, 28 October 1994, *Murray v The United Kingdom*, Judgment, § 84; GCh, Appl. No. 28341/95, 4 May 2000, *Rotaru v Romania*, Judgment, §§ 43 and 44; GCh, Appl. No. 27798/95 16 December 2000, *Amann v Switzerland*, Judgment, §§ 15-29, 65; Appl. No. 44787/98, 25 September 2001, *P.G. and J.H. v The United Kingdom*, Judgment, §. 59; Appl. No. 44647/98, 28 January 2003, *Peck v The United Kingdom*, Judgment, § 59; GCh, Applications Nos. 30562/04 and 30566/04, 4 December 2008, *S. and Marper v The United Kingdom*, Judgment, § 68.

¹⁵⁷ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted by the Council of Europe in Strasbourg, 28 January 1981, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

possible for the EU to accede to it.¹⁵⁸ In 2001 was adopted an additional Protocol regarding supervisory authorities and transborder data flows, that entered into force in 2004.¹⁵⁹ Furthermore, Convention No. 108 is complemented by a series of Recommendations,¹⁶⁰ such as the Recommendation Regulating the use of Personal Data in the Police Sector.¹⁶¹

Recently, the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data has been actively working on the issue of profiling. It adopted in June 2010 a Draft Recommendation on the subject.¹⁶² Additionally, it has launched a process of analysis of Convention No. 108 and is expected to start discussing its possible revision in the near future.

* Updates to the EU Report published in the 2010 edition of EPHR have been provided by: Gloria González Fuster, Law, Science, Technology & Society (LSTS) at Vrije Universiteit Brussel, Belgium; Maria Grazia Porcedda, European University Institute, Italy; Matteo E. Bonfanti, Centre for Media and Communication Studies, Central European University, Hungary.

¹⁵⁸ Amendments to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to Accede, adopted by the Committee of Ministers, in Strasbourg, 15 June 1999, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108-1.htm>.

¹⁵⁹ Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (CETS No. 181), adopted by the Committee of Ministers of the Council of Europe in Strasbourg, 8 November 2001, available at <http://conventions.coe.int/treaty/en/Treaties/Html/181.htm>.

¹⁶⁰ All Recommendations are available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Legal_instruments_en.asp.

¹⁶¹ Council of Europe Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector.

¹⁶² Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Draft Recommendation on the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, adopted at its 26th plenary meeting, June 2010, Strasbourg.



This project was funded with the support of the Fundamental Rights and Citizenship Program of the European Commission.