New Zealand

Article 21 of the New Zealand Bill of Rights Act 1990 states "Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence or otherwise."[1] The New Zealand Court of Appeal has interpreted this provision in several cases as protecting the important values and interests that make up the right to privacy.[2]

New Zealand's Privacy Act of 1993 came into force on July 1, 1993, and has been amended several times.[3] It regulates the collection, use and dissemination of personal information in both the public and private sectors. It also grants to individuals the right to have access to personal information held about them by any agency. The Privacy Act applies to "personal information," which is any information about an identifiable individual, whether automatically or manually processed.[4] Recent case law has held that the definition also applies to mentally processed information.[5] The news media are exempt from the Privacy Act in relation to their news activities.

The Act creates twelve Information Privacy Principles generally based on the 1980 Organization for Economic and Cooperation Development (OECD) Guidelines and the information privacy principles in Australia's Privacy Act 1988. In addition, the legislation includes a new principle that deals with the assignment and use of unique identifiers. The Information Privacy Principles can be individually or collectively replaced by enforceable codes of practice for particular sectors or classes of information. At present, there are only two complete sectoral codes of practice in force, the Health Information Privacy Code 1994 and the Telecommunications Information Privacy Code 2003.[6] There are several codes of practice that alter the application of single information privacy principles: the Superannuation Schemes Unique Identifier Code 1995, the Justice Sector Unique Identifier Code 1998, and the Post-Compulsory Education Unique Identifier Code 2001.[7] The Commissioner released for public consultation a proposed Credit Information Privacy Code in July 2003. In addition to the information privacy principles, the legislation contains principles relating to information held on public registers; it sets out guidelines and procedures in respect to information matching programs run by government agencies, and it makes special provision for the sharing of law enforcement information among specialized agencies.

The Office of the Privacy Commissioner is an independent oversight authority that was created prior to the Privacy Act by the 1991 Privacy Commissioner Act, which focused on the supervision of information matching among government departments.[8] The Privacy Commissioner oversees compliance with the Privacy Act 1993, but does not function as a central data registration or notification authority. The

---

1 Bill of Rights Act, 1990, Chapter 4, Section 21, available at <http://www.oefre.unibe.ch/law/icl/nz01000_.html>.

2 Tim McBride, "Recent New Zealand Case Law on Privacy: Part I: Privacy Act and the Bill of Rights Act," Privacy Law & Reporter, January 2000, at 107.

3 The Privacy Act 1993, available at <http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html>; the Privacy Amendment Act 1993, available at <http://www.privacy.org.nz/slegisf.html>; The Privacy Amendment Act 1994, available at <http://www.privacy.org.nz/slegisf.html>; Privacy Amendment Act 1996, available at <http://rangi.knowledge-basket.co.nz/gpacts/public/text/1996/an/142.html>; Privacy Amendment Act 1997, available at <http://rangi.knowledge-basket.co.nz/gpacts/public/text/1997/an/142.html>; Privacy Amendment Act 1998, available at <http://rangi.knowledge-basket.co.nz/gpacts/public/text/1998/an/057.html>; Privacy Amendment Act 2000, available at <http://rangi.knowledge-basket.co.nz/gpacts/public/text/2000/an/076.html>; and Privacy Amendment Act 2002, available at <http://rangi.knowledge-basket.co.nz/gpacts/public/text/2002/an/073.html>.

4 *See* Paul Roth, "What is 'Personal Information'?," 20(1) New Zealand Universities Law Review 40 (2002).

5 *See* Re Application by L – Information stored in person's memory (1997) 3 HRNZ 716 (Complaints Review Tribunal).

6 <http://www.privacy.org.nz/comply/codes.html>. The Privacy Commissioner may issue codes of practice that modify the Information Privacy Principles set out in the Privacy Act to take into account the special characteristics of specific industries, agencies or types of personal information. This site has compiled the provisions, which may be more stringent or less stringent than the principles.

7 "How to Comply with the Privacy Act," available at <http://www.privacy.org.nz/comply/comptop.html>.

8 Homepage <http://www.privacy.org.nz/>.

Privacy Commissioner's principal powers and functions include promoting the objects of the Act, monitoring proposed legislation and government policies, dealing with complaints at first instance, approving and issuing codes of practice and authorizing special exemptions from the information privacy principles, and reviewing public sector information matching programs. In June 2002, the Commissioner had 18 full time and 6 part-time staff.

Complaints by individuals are initially filed with the Privacy Commissioner who attempts to conciliate the matter. In the 2003/04 year there were 934 new complains received. By contrast, in the year ending June 2002 the office received 1,044 new complaints and 6,772 enquiries. 1,049 complaints (new and from the year before) were closed during the year. 85 percent were resolved without issuing a final opinion.[9] The Commissioner regards the power to investigate and to require answers during investigations as "a vital element" in securing such a high conciliation rate. When conciliation fails, the Director of Human Rights Proceedings[10] or the complainant (if the Director of Human Rights Proceedings is unwilling) can bring the matter before the Human Rights Review Tribunal, which can issue decisions and award declaratory relief, issue restraining or remedial orders, and award special and general damages up to NZD 200,000 (~USD 115,000).[11]

Privacy Commissioner Marie Shroff has argued that privacy laws and press freedom are similar in that they are both about offering some protections and empowerment to citizens.[12]

Current issues of concern include the growing aggregation of New Zealander's DNA in public data banks.[13] The permanent collection of the genetic profiles is worrying privacy and civil liberties groups. These groups are concerned that a population-wide databank of DNA is being built up, without public awareness or debate, and without proper controls.

Commentators also note that in New Zealand it is widely accepted that employers are able to monitor all e-mails sent on work computers.[14] A new health law is raising privacy complaints because the once-private relationship more than a million New Zealand women and their gynecologists has been undermined by new legislation on the National Cervical Screening Programme (NCSP), according to women's health advocate Barbara Robson.[15] The Health (National Cervical Screening Programme) Amendment Act allows evaluators to investigate the case histories of any woman enrolled on the programme without seeking their consent.[16]

InternetNZ[17], a non-profit Internet interest group, created the Anti-Spam Task Force, of which the New Zealand Direct Marketing Association is a member. The group has met with the New Zealand government, held a conference in November 2003, funded a member to attend the OECD Conference on Spam, and worked with the press. The group encourages all ISPs to refer their customers to their website, which includes advice to individuals and businesses, and a discussion of legislative activity in the country. The group will hold a conference in Wellington on June 24.[18]

---

[9] New Zealand Privacy Commission, Annual Report for the year ended 30 June 2003, available at <http://www.privacy.org.nz/>.

[10] The Director of Human Rights Proceedings is an official appointed under the Human Rights Act of 1993.

[11] This limit can be raised by application to the High Court.

[12] She is also quoted as saying, "Privacy is not about keeping secrets, but about retaining a level of control over your own information. . . . Although privacy concerns are sometimes positioned as being in opposition to press freedom, I don't see that as being the case." Gamble Warren, "Freedom to Publish," The Press (Christchurch), May 1, 2004, at 8D.

[13] Courtney Dave, "Who's in Charge of DNA Bank?," The Press (Christchurch), April 28, 2004, at 15A.

[14] Andrew Kelly, "NZ Bosses Free to Read Staff E-mails," The Dominion Post (Wellington), April 10, 2004 at 5.

[15] Rankin Janine, "Privacy 'Undermined' by New Law," The Evening Standard (Palmerston North), March 4, 2004, at 3.

[16] *Id.*

[17] Stop Spam homepage <http://stopspam.net.nz>.

[18] David Harris, "A Presentation to APCAUCE on the 'State of the Nation,'" presented February 26, 2004 at the Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE) Conference, Kuala Lumpur, Malaysia.

Anti-spam legislation is likely on the horizon for New Zealanders.[19] The Government is inviting public submissions on how best to outlaw spam.[20] Associate Information Technology Minister David Cunliffe is trying to get an anti-spam law in front of Parliament by the end of 2004.[21]

A landmark Employment Court ruling in April 2004 gave Air New Zealand the right to conduct random drug tests on its workers in "safety-sensitive areas."[22] This was the first comprehensive decision on the issue in New Zealand.[23] While the court ruled that the national airline may not impose random tests for drugs or alcohol across its workforce, it may undertake random testing of workers in certain circumstances: in safety sensitive areas; to carry out pre-employment testing of workers before they join the company; testing of workers whose behavior suggests they have taken drugs; and workers involved in an accident or near-miss.[24]

In March 2004, the New Zealand Court of Appeal rejected broadcaster Mike Hosking's complaint of breach of privacy, over the intended publication of photographs taken of his twin baby daughters on a public street.[25] This was one of the very few privacy tort cases that went before the Court of Appeal in 2004.

In March 2002, the Commission hosted a meeting of the International Working Group on Data Protection in Telecommunications, a group created by the International Conference of Data Protection and Privacy Commissioners. In conjunction with that meeting the Commissioner also organized a one-day symposium on freedom of information and privacy.[26]

The Law Commission is reviewing the legal protection of privacy rights and the working of the 1993 Privacy Act. In February 2002, the Commission issued a discussion paper "Protecting Personal Information from Disclosure" for public comment.[27] In the summer of 2001, the Mental Health Commission began a study of privacy procedures in mental health services. The Privacy Commissioner participated in the work of the review board. In February 2002, the board issued its report: "A Review of the Implementation of the Privacy Act and Health Information Privacy Code by Mental Health Units of District Health Boards."[28]

New Zealand is one of several countries involved in negotiations with the European Commission concerning the "adequacy" of its privacy regime in relation to the European Union Data Protection Directive (1995/46/EC). Since 1998 the Commission has been urging the Government to introduce two minor amendments to the Privacy Act in order to secure a finding of adequacy. The first amendment would remove the existing requirement that in order to make an access or correction request, an individual must be a New Zealand citizen, permanent resident or present in New Zealand at the time the request is made. The second would introduce a limited data export control to regulate the transfer of personal information outside New Zealand. In December 12, 2000 these changes were finally included in

---

[19] Tom Pullar-Strecker, "Telcos Aim to Outlaw Spam Texts," New Zealand Infotech Weekly, March 15, 2004, at 2.

[20] Tom Pullar-Strecker, "Public Can Have Say on Spam," The Dominion Post (Wellington), May 17, 2004, at 9C.

[21] *Id*.

[22] Batchelor Kim, "Air NZ Case Opens Door for More Drug Testing," The Daily News (New Plymouth) May 3, 2004, at 6.

[23] *Id*.

[24] "Drug Testing a Safety Issue," Waikato Times (Hamilton) April 20, 2004, at 6.

[25] Hosking v. Runting, [2003] 3 NZLR 385, available at http://www.brookers.co.nz/legal/judgments/Default.asp?doc=2003\ca101.htm#Number1

[26] International Symposium on Freedom of Information and Privacy, Auckland, March 28, 2002 <http://www.privacy.org.nz/media/isfoip.html>.

[27] Available at <http://www.lawcom.govt.nz/>.

[28] Available at <http://www.mhc.govt.nz/publications/Publications/Privacy%20Review.pdf>.

the Statutes Amendment Bill[29] and submitted to Parliament. Accordingly, it was expected that these amendments would be approved and enacted without delay.[30] In the fall of 2001, however, one party withdrew its support of one of the amendments. In his annual report for the year ended June 30, 2001, the Privacy Commissioner encouraged "those responsible for the business of the House of Representatives [to] ensure that whatever vehicle these amendments proceed in is given priority." There has been no apparent progress to date on this issue. The Statutes Amendment Bill has not yet been introduced again. It is hoped that a Privacy Amendment Bill, including the earlier introduced changes (and others), might be introduced before the end of the 2004 calendar year.[31]

The High Court ruled in July 2000 that the implementation of a nationwide drivers license system with a digitized photograph that was required by the 1998 Land Transport Act was legal. The law creates a national database of digitized photographs. The individual challenging the law appealed the ruling. The Court of Appeals rejected her appeal in April 2001 saying much of the case was based on misconceptions of the law.[32]

The New Zealand Crimes Act and Misuse of Drugs Act govern the use of police interception powers.[33] Interception warrants authorize not just the interception of communications but also the placing of listening devices. A judge authorizes warrants where there are reasonable grounds to believe that certain offences have been committed or are being contemplated. Emergency permits may be granted for the bugging of premises and, following the 1997 repeal of a prohibition, for telephonic interceptions. Those who illegally disclose the contents of private communications illegally intercepted face two years in prison. However, those who illegally disclose the contents of private communications lawfully intercepted are merely liable for a NZD 500 (~USD 290) fine.

In 2002/2003 the New Zealand Police sought and were granted 31 interception warrants under the Misuse of Drugs Act. Six renewed interception warrants were sought and granted under the Act.[34] Under the Crimes Act, nine interception warrants were granted and no renewals were sought. By contrast, in 2001/2002 the Police sought and obtained 19 (new and renewed) interception warrants under the Misuse of Drugs Act and eight (new and renewed) interception warrants under the Crimes Act. One emergency permit was granted under the Crimes Act.[35] In 2003 a total of 85 warrants (new and renewed) were obtained under the Telecommunications Amendment Act 1997, whereas 52 warrants were obtained in 2002 for obtaining call data analyzers (pen registers and trap and trace devices that obtain call information but not the contents of communications).

The New Zealand Security Intelligence Service (NZSIS), established under the New Zealand Security Intelligence Service Act of 1969,[36] is also permitted to carry out electronic interceptions. The NZSIS has a staff of 115 and an annual budget of NZD 11 million (~USD 6.3 million). The majority of its work is devoted to threats to national security.[37] The Act was amended in 1999 to allow for the service to enter premises to install taps following a Court of Appeal case that prohibited entering of premises without a

---

[29] A statutes amendment bill is a procedure designed for the introduction of non-controversial legislation.

[30] Office of the Privacy Commissioner, Press Release, "Proposed Amendments to the Privacy Act Addressing the Questions of Adequacy under the EU Data Protection Directive, December 15, 2000 <http://www.privacy.org.nz/media/prppaam.html>.

[31] E-mail from Mr. Blair Stewart, Assistant Privacy Commissioner, New Zealand, to Amanda Reid, Law Clerk, Electronic Privacy Information Center (EPIC), July 15, 2004 (on file with EPIC).

[32] "Photo Licence Appeal Rejected," The Dominion (Wellington), April 12, 2001.

[33] Part XIA, Crimes Act 196; Misuse of Drugs Act 1978.

[34] New Zealand Police Annual Report 2003, available at <http://www.police.govt.nz/resources/2003/annual-report/annual-report.pdf>.

[35] New Zealand Police Annual Report 2002, available at <http://www.police.govt.nz/resources/2002/annualreport/>.

[36] New Zealand Security Intelligence Service Act of 1969, available at <http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes>.

[37] John Armstrong, "SIS Gives MPs New Details of NZ Terrorist Links," New Zealand Herald, December 9, 2000, available at <http://www.nzherald.co.nz/storydisplay.cfm?thesection=news&thesubsection=&storyID=163879>.

warrant. The amendment also created a "foreign interception warrant."[38] Another amendment created a Commissioner of Security Warrants to jointly issue warrants with the Prime Minister.[39] The Minister in Charge of the NZSIS is required to submit an annual report to the House of Representatives. During the year ending June 2002, the Minister reported that 21 domestic interception warrants were in force. Of these, 13 were new interception warrants and eight were carried over from the previous year. The average length of time for which these warrants were in force was 131 days.[40] According to the Minister's report "the methods for interception and seizure used were listening devices and the copying of documents." The report also stated that foreign interception warrants were in force during the year but does not give any statistics for these warrants.

One agency not governed by the restrictions imposed on law enforcement and the NZSIS is the Government Communications Security Bureau (GCSB), the Signals Intelligence (SIGINT) agency for New Zealand. The GSCB was established by Executive Authority in 1977 and focuses on foreign intelligence. Operating as a virtual branch of the US National Security Agency, this agency maintains two intercept stations at Waihopai and Tangimoana. The Waihopai station routinely intercepts trans-Pacific and intra-Pacific communications and passes the collected intelligence to NSA headquarters. David Lange, a former Prime Minister of New Zealand, said that he and other ministers were told very little about the operations of GCSB while they were in power. Of particular interest to GCSB and NSA are the communications of the governments of neighboring Pacific island states.[41] GCSB was specifically exempted from the provisions of the Crimes Act in 1997.[42]

The Government Communications Security Bureau Act was enacted in 2003. This enactment places the GCSB on a statutory footing. In August 2001, the Government announced that it set up a new unit within the Government Communications Security Bureau dedicated to the protection of the nation's critical infrastructure from cyber threats by Internet hackers or computer viruses. The Centre for Critical Infrastructure Protection (CCIP) was scheduled to begin operations in April 2002.[43]

The Government has created major new surveillance powers for these state agencies. New Zealand's Parliament passed the Crimes Amendment Bill,[44] effective October 1, 2003, which grants broader powers to police and security agencies to intercept electronic communications.[45] The Crimes Amendment Act overwhelmingly passed by Parliament in July 2003, gives intelligence agencies additional powers to intercept communications, with High Court approval; while also criminalizing similar unauthorized activities, and the distribution or possession of computer hacking programs.[46] The controversial anti-hacking legislation gives police explicit authority to intercept electronic communications. The new law makes it illegal to intercept, access, use or damage data stored on computers without proper authorization. It also makes the sale, distribution or possession of hacking programs illegal.[47] The Act prohibits the unauthorized interception of electronic communications and makes hacking and denial of service attacks illegal, but would grant exemptions to the police, the NZSIS and the GCSB, allowing them to secretly hack into individuals' computers and intercept e-mail, text

---

[38] New Zealand Security Intelligence Service Amendment Act 1999.

[39] New Zealand Security Intelligence Service Amendment (No 2) Act 1999.

[40] Report of the New Zealand Security Intelligence Service to the House of Representatives for the year ended 30 June 2002, available at <http://www.nzsis.govt.nz/ar02/part2.html>.

[41] Nicky Hager, Secret Power: New Zealand's Role in the International Spy Network (Nelson, NZ: Craig Potton 1996).

[42] Crimes (Exemption of Listening Device) Order 1997 (SR 1997/145).

[43] Adam Creed, "New Zealand Center to Combat Cyber Threats," Newsbytes, August 8, 2001.

[44] Crimes Act of 1961, as amended, available at <http://www.netlaw.co.nz/crime.cfm?PageID=28>.

[45] Francis Till, "Police Win Intercept Rights," The National Business Review, July 11, 2003, at 31.

[46] Associated Press, "NZ Police Get Tech Crime Powers," AustralianIT, July 4, 2003.

[47] Crimes Act of 1961 (as amended), available at <http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes>.

messages, and faxes. Police are required to specify a person, place, and specific electronic address, phone number, or similar facility when applying for an interception warrant.

Even more controversial was the Telecommunications (Interception Capabilities) Bill, introduced into Parliament on November 12, 2002. Similar to the United States Communications Assistance for Law Enforcement Act (CALEA) of 1994, this legislation would require all Internet Service Providers (ISPs) and telephone companies to upgrade their systems so that they are able to assist the police and intelligence agencies, including the Government Communications Security Bureau (GCSB) and Security Intelligence Service (SIS), intercept communications. The Bill would oblige telecommunications companies and ISPs to intercept phone calls and e-mails at the behest of the police and security services.[48] The legislation would also require a telecommunications operator to decrypt the communications of a customer if that operator had provided the encryption facility.[49] It would not require individuals to hand over encryption keys.

Prior to introducing the proposals the Government sought the advice of the New Zealand Law Commission on whether such a requirement would violate Section 21 of the New Zealand Bill of Rights on unreasonable searches and seizures. In its report, issued in February 2002, the Law Commission concluded, "the existence of comparable obligations in other democracies establishes reasonably conclusively either that the search is not thereby rendered unreasonable or that if there is a limitation of the rights described in Section 21 it can be demonstrably justified in a free and democratic society." The Commission recommended that the law be amended to impose an obligation on third parties to provide all reasonable and necessary information and assistance (including passwords and decryption keys) to enable law enforcement officers to access, copy or convert the data into intelligible form.[50]

The government introduced the Counter-Terrorism Bill on December 17, 2002. This measure, passed into law in October 2003,[51] was intended to implement obligations arising from international conventions relating to the suppression of terrorism, proposes to introduce new and sweeping criminal offences.[52] The Bill introduces powers to search and seize computer databases; seize and detain goods at border checks if there is cause to suspect that the recipient is "eligible" for designation as a terrorist; and it establishes a regime for the use of tracking devices (defined as devices which "when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person"). The Bill could force individuals to disclose their passwords, even in non-terrorism related investigations, or else face three months in jail or a fine of NZD 2,000 (~USD 1,150).

Since the terrorist attacks on September 11, 2001, the New Zealand government has been working to strengthen counter-terrorism laws.[53] Before September 11, 2001, New Zealand was a party to only eight of the 12 conventions that the international community had negotiated over the last 30 years. However, according to Foreign Minister Phil Goff, as of December 2003 New Zealand is a party to all 12 United Nations terrorism conventions.[54]

---

[48] Tom Pullar-Strecker, "Bugging Bill Fears Unfounded," New Zealand Infotech Weekly, November 17, 2003, at 2.

[49] "Interception Capability – Government Decisions," New Zealand Government Executive Press Release, March 21, 2002, available at <http://www.executive.govt.nz/speech.cfm?speechralph=37658&SR=0>.

[50] New Zealand Law Reform Commission, Study Paper 12, "Electronic Technology and Police Investigations: Some Issues," February 2002, available at <http://www.lawcom.govt.nz/Documents/Publications/SP%2012%2028-2-02.pdf>.

[51] "Terror Powers Could Be Misused," The Press (Christchurch, New Zealand) October 23, 2003, at 1.

[52] Phil Goff, "Counter Terrorism Act Boosts Government Fight against Terrorism," October 22, 2003, available at <http://www.beehive.govt.nz/ViewDocument.cfm?DocumentID=18168>. According to Prime Minister Helen Clark, New Zealand has not taken any special measures after the March 2004 bombings in Madrid, Spain, because it already had extra counter-terrorism capabilities in place following the September 11, 2001 attacks. Kevin Taylor, "NZ Anti-terrorism Measures in Place, Says Helen Clark," The New Zealand Herald, March 16, 2004.

[53] Phil Goff, "NZ Now Party to All 12 UN Terrorism Conventions," December 23, 2003, available at <http://www.beehive.govt.nz/ViewDocument.cfm?DocumentID=18735>.

[54] *Id.*

Other recent bills before Parliament implicate privacy and data protection interests. These bills include the Border Security Bill and the Maritime Security Bill.[55] The Border Security Bill,[56] according to Customs Minister Rick Barker, would seek to strengthen border control measures against terrorism and trans-national crime including drug smuggling, across both travel and trade sectors.[57] The Maritime Security Bill, on the other hand, adds to the framework of laws seeking to reduce the risk of terrorism to international shipping.[58] New Zealand is a party to the 1974 International Convention for the Safety of Life at Sea (SOLAS). The Maritime Security Bill was intended to give effect to these requirements under the SOLAS Convention.[59]

The Broadcasting Act of 1989 requires broadcasters to maintain standards that are consistent with "the observance of good taste and decency . . . the maintenance of law and order and the privacy of the individual."[60] It establishes a Broadcasting Standards Authority (BSA) to oversee enforcement and to rule on complaints. The BSA has ruled on several privacy cases.[61] Recently, particular controversy surrounded several television broadcasts unreasonably intruding on the privacy of children. In March 1999, one program, widely publicized in advance, revealed the results of a DNA paternity test live on TV with mother, father and young child present.[62] The Broadcasting Amendment Act of 2000, which came into effect on July 1, 2000, empowers the BSA to encourage the development and observance by broadcasters of codes of broadcasting practice in relation to the privacy of the individual.

The Criminal Investigations (Blood Samples) Act of 1995 authorized the establishment of a national DNA databank. Police have to get an order from a High Court judge before a compulsory test can be conducted and they can only take samples from suspects of violent crimes and convicted burglars. Voluntary samples from anybody can be included in the databank. In October 2000, police were ordered to reduce the number of voluntary DNA samples due to budgetary concerns. By 2002, however, it was reported that police were being advised to increase this number again and to try and obtain voluntary samples from anyone arrested with a prior criminal record.[63] In February 2001, the Justice Minister announced that he planned to introduce legislation to allow DNA samples to be taken from burglary suspects.[64] As of 2003, the total number of DNA profiles stored on a DNA databank in New Zealand was 33,892. Of these, 28,614 were obtained by consent and 5,116 were obtained by compulsion orders.[65] By contrast in June 2002, the total number of DNA profiles stored in the national database was 24,001. Of these, 19,453 were obtained by consent and 4,426 were obtained by compulsory order.[66] In May 2002, a new NZD three million (~USD 1.7 million) purpose-built laboratory was opened in Auckland for forensic DNA testing.[67] Testing was carried out by the Institute of Environmental Science and Research (ESR).

---

[55] E-mail from Mr. Blair Stewart, Assistant Privacy Commissioner, New Zealand, to Amanda Reid, Law Clerk, Electronic Privacy Information Center (EPIC), July 1, 2004 (on file with EPIC).

[56] Available at <http://www.knowledge-basket.co.nz/gpprint/docs/bills/20040532.txt>.

[57] Rick Barker, "Putting New Zealand Security on the Front Foot," May 20, 2004, available at <http://www.beehive.govt.nz/ViewDocument.cfm?DocumentID=19768>.

[58] Ministry of Transportation, Maritime Security, available at <http://www.transport.govt.nz/business/maritime/maritime-security.php>.

[59] *Id*.

[60] Available at <http://www.spectrum.net.nz/archive/acts.shtml>.

[61] *See, e.g.*, Tim McBride, "Recent New Zealand Case Law on Privacy: Part II: the Broadcasting Standards Authority, the Media and Employment," Privacy Law & Reporter, February 2000, at 133.

[62] "DNA Test Matches Father and Son on TV," The Dominion (Wellington), March 30, 1999.

[63] "Police DNA Drive," The Evening Post (Wellington), March 21, 2002.

[64] "Police Say They Can Afford Bigger DNA Database," The Dominion (Wellington), February 13, 2001.

[65] New Zealand Police Annual Report 2003, *supra.*

[66] New Zealand Police Annual Report 2002, *supra*.

[67] "DNA Laboratory to Be Ready in May," The Dominion (Wellington), February 23, 2002.

The Official Information Act of 1982[68] and the Local Government Official Information and Meetings Act of 1987[69] are freedom of information laws governing the public sector. The Official Information Act is seen as an important weapon in the armory of keeping the executive and the ministers honest.[70] There are significant interconnections between this freedom of information legislation and the Privacy Act in subject matter, administration, and jurisprudence, so much so that the three enactments may be viewed, in relation to access to information, as complementary components of one overall statutory scheme. The Office of the Ombudsman supervises enforcement.[71] The Ombudsman hears around 1,100 complaints each year under the Official Information Act and 170 each year under the Local Government Official Information and Meetings Act. The Privacy Commissioner and the Ombudsmen work closely together where Official Information Act requests involve privacy issues.

New Zealand 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.

Self-governing Territories

The Privacy Act does not apply to self-governing territories associated with New Zealand, the Cook Islands and Niue, nor does it apply to the soon-to-be self-governing territory of Tokelau.

Federal Republic of Nigeria

Chapter IV, § 37 of the 1999 Constitution declares that "the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected."[72] The Constitution also allows courts to exclude certain parties from judicial proceedings for "the protection of the private lives of parties."[73] However, the Constitution's ban on secret societies[74] raises concerns regarding the privacy of association.

The principal body for Nigerian Internet policy is the National Information Technology Development Agency (NITDA, a sub-agency of the Nigerian Communications Commission. NITDA has developed a draft Nigerian Information Technology Policy which was approved by the Nigerian Federal Executive Council in 2001.[75] NITDA's IT Policy identifies some of its objectives as, "promot(ing) legislation (Bills and Acts) for the protection of on-line business transactions, privacy and security,"[76] and "enhanc(ing) freedom and access to digital information at all levels while protecting personal privacy."[77]

The menace of fraudsters soliciting victims via email prompted the Nigerian government in 2002 to create a National Committee to address the problem.[78] NITDA was involved in this process and one of the committee's recommendations was a draft Cybercrime Act which includes a Data Retention Provision that declares, "[a]ll service providers under this Act shall have the responsibility of keeping all

---

[68] Official Information Act 1982 <http://www.ombudsmen.govt.nz/official.htm>.

[69] Local Government Official Information and Meetings Act 1987 <http://www.ombudsmen.govt.nz/local.htm>.

[70] Richard Worth, "Bill Boosts Secrecy Powers," The National Business Review (New Zealand), May 21, 2004, at 32.

[71] Homepage <http://www.ombudsmen.govt.nz/>.

[72] <http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm>.

[73] 1999 Constitution of the Federal Republic of Nigeria, Chapter IV, §36 (4-a).

[74] *Id.* at Chapter IV, §38 (4).

[75] "The Nigerian National Information Technology Policy," Jidaw Systems Website <http://www.jidaw.com/policy.html>.

[76] "Nigerian National Policy for Information Technology: USE IT" 4, available at <http://www.nitda.gov.ng/docs/policy/ngitpolicy.pdf>.

[77] *Id.* at 32.

[78] Sam Olukoya, "Nigeria Grapples with E-Mail Scams," BBC News Online, April 23, 2002 <http://news.bbc.co.uk/1/hi/world/africa/1944801.stm>.

transactional records of operations generated in their systems and networks for a minimum period of five years."[79] This data retention provision raises privacy concerns as the draft Act defines service providers as "Internet service providers, cybercafés, communications service providers, application service providers, any individual or body corporate that deploys information and communication technology resources in Nigeria."[80] This broad definition of service providers possibly extends the five-year data retention requirement to virtually all Internet communications in Nigeria.

In February 2003 the Nigerian government launched an extensive National ID Card Drive in which everybody over 18 years of age was eligible to participate.[81] While registration for the identity card was not compulsory, those who chose to participate were required to provide information which included their name, age, sex, address, occupation, state of origin, local government area, height measurement, thumbprint, and passport photograph.[82] Despite allegations that the ID contract was corruptly awarded, in 2004, the Minister in charge of the project reaffirmed the government's commitment to the project and announced that the first batch of cards were ready for collection.[83]

The operation of *Sharia* Law[84] in 12 northern Nigerian states[85] also raises issues of privacy. Of particular concern is the provision in several of the states for the punishment of adultery by stoning to death.[86] While no one has been stoned for adultery under the *Sharia* laws, several accused Nigerian women have had to undergo judicial proceedings in which, by necessity, the consideration of the details of their sexual lives have been the basis for both their prosecution and defense.[87]

The Nigerian Evidence Act protects the confidentiality of communication during marriage by providing that no husband or wife shall be compelled to disclose any communication made to him or her during marriage by any person to whom he or she is or has been married; nor shall he or she be permitted to disclose any such communication, unless the person who made it, or that person's representative consents, except in suits between married persons, or proceedings in which one married person is prosecuted for certain specified offenses.[88]

In 1999, a Nigerian Right to Information Bill was introduced in the House of Representatives. The bill went through several readings but has not yet been enacted.[89] The draft bill allows even non-citizens to make information requests, mandates the annual publication of certain operational records by every government institution, and provides several exemptions to the disclosure requirement (*e.g.*, certain international affairs and defense matters, certain law enforcement and investigation information, and information of a personal nature).[90]

---

79 Femi Oyesanya, "The Nigerian Patriot (Act) Is Coming: Compliments of NITDA," Gamji.com News, July 6, 2004, <http://www.gamji.com/NEWS3569.htm>.

80 *Id.*

81 Nigerian Information Service Center, "National Identity Card for Nigerians," February 20, 2003, available at <http://www.nigeriaembassyusa.org/022103_2.shtml>.

82 "Nigerians Register for National Identity Card from Today," NigeriaBusinessInfo.com, February, 18, 2003 <http://www.nigeriabusinessinfo.com/id-card180203.htm>.

83 Iyefu Adoba, "FG Restates Commitment to ID Card Project," This Day, June 9, 2004 <http://allafrica.com/stories/200406090330.html>.

84 The *Sharia* is a body of Islamic law that governs not only aspects of religious faith, but also offers dictates for the conduct of everyday secular activities.

85 Dan Isaacs, "Nigerian in Crisis over Sharia Law," BBC News Online, March 26, 2002, available at <http://news.bbc.co.uk/1/hi/world/africa/1893589.stm>.

86 *Id.*

87 *Id.*

88 Evidence Act, Laws of the Federation of Nigeria, 1990, Cap 112.

89 "The Campaign for a Freedom of Information Act," Nigerian Media Rights Agenda Website <http://www.internews.org/mra/campaigns/campaigns.htm>.

90 Freedom of Information Bill 1999, available at <http://www.internews.org/mra/freeinfo/freeinfo.htm>.

Kingdom of Norway

The Norwegian Constitution of 1814 does not have a specific provision dealing with the protection of privacy.[91] The closest provision is Article 102, which prohibits searches of private homes except in "criminal cases." More generally, Article 110c of the Constitution places state authorities under an express duty to "respect and secure human rights."[92] In 1952, the Norwegian Supreme Court held that there exists in Norwegian law a general legal protection of "personality" which embraces 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.[93] 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."[94]

The Norwegian Constitution also protects freedom of speech (Article 100). Persons may not be liable in law 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).[95] Postal communications may be censored only by institutions and by leave of a court of law.[96]

The Electronic Communications Act of 2003 and its accompanying regulations implement the requirements of the European Union (EU) Directive on Privacy and Electronic Communications (2002/58/EC). Under Section 2-9 of the Act, telecommunications providers must safeguard the secrecy of the content of telecommunications.[97] The duty of confidentiality, however, does not prevent such information from being given to the prosecuting authority or the police, or to another authority pursuant to the law.[98] The Act has reduced some safeguards on electronic communications provided for in the Telecommunications Act of 1995, which the Electronic Communications Act replaced. Previously, customers could provide a minimum of personal information when purchasing a mobile phone. By using unregistered cell phones and anonymous cash cards, individuals could communicate almost undetected. Article 6-2 of the accompanying regulation states that all electronic communication providers must keep records of all their end users. The consequence of this provision is that mobile phone cash cards can no longer be sold anonymously.[99]

The regulation 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).[100] The PDA 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, including the need to protect personal integrity and private life and to ensure adequate quality of personal data (section 1). Enforcement of the

---

91 The Constitution of the Kingdom of Norway <http://odin.dep.no/odin/engelsk/norway/system/032005-990424/>.

92 Lee A. Bygrave & Ann Helen Aaro, Norway, International Privacy, Publicity and Personality Laws 333 (M. Henry ed., 2001).

93 *Id.* at 340.

94 *Id.* at 334.

95 Per-Kaare Svendsen, The Association for Progressive Communications (APC) European Internet Rights Project, Country Report: Norway (2000) <http://www.apc.org/english/rights/europe/c_rpt/norway.html>.

96 *Id*.

97 The Electronic Communications Act (*ekomloven*), July 4, 2003, No. 83 <http://www.npt.no/iKnowBase/FileServer/ekom_eng.pdf?documentID=7922> (Unofficial English translation).

98 *Id.*

99 E-mail from Morten Foss, Legal Adviser, The Norwegian Post and Telecommunications Authority, to Kenneth Farrall, IPIOP Law Clerk, Electronic Privacy Information Center (EPIC), June 14, 2004 (on file with the EPIC).

100 The Data Inspectorate's homepage <http://www.datatilsynet.no/>.

PDA is overseen by The Data Inspectorate (*Datatilsynet*), a body originally set up in 1980.[101] The Inspectorate is placed under the administrative wings of the Ministry of Labor and Government Administration, but is otherwise expected to function completely independently of government or private sector bodies. The Inspectorate employed 30 staff members as of 2004, 12 of which are lawyers, five are engineers, three are information personnel, and the rest hold administrative positions.[102]

The responsibilities of the Inspectorate include verifying that statutes and regulations which apply to the processing of personal data are complied with, and that errors or deficiencies are rectified; identifying risks to protection of privacy; and providing guidance on measures to avoid or limit such risks.[103] The Data Inspectorate has answered 3,500 incoming letters from June 1, 2003 to June 1, 2004. This figure includes the whole range from small to extensive complaints and 141 written submissions. In the period from November 2003 to June 2004, the Data Inspectorate's answering service responded to 6,000 telephone calls. The most frequent complaints concerned direct marketing. The second most frequent topic was related to privacy in the workplace (13 percent), closely followed by video surveillance (10 percent). About one half of the calls came from private individuals with rights according to the PDA, and the other half from different organisations and enterprises with duties according to the PDA.[104] Decisions of the Inspectorate may be appealed to a quasi-judicial body, the Data Protection Tribunal (*Personvernnemnda*). Decisions of the Tribunal may be appealed to civil courts on questions of law.[105]

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.[106] The PDA covers all data that may be linked directly or indirectly to individuals.[107] The PDA applies to both the public and private sectors, and it covers both manual and computerized 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 license 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 to the Act). The Inspectorate also has the power to make on-site visits to data register licensees to determine compliance with the Act (Section 44). 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 which 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 is being collected and the name of the controller collecting the personal data (Sections 19-20). New in relation to the 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, *i.a.*, fines or imprisonment (Sections 46 *et seq.*).[108]

---

[101] *Id.*

[102] E-mail from Gunnel Helmers, Data Inspectorate, Norway, to Kenneth Farrall, IPIOP Law Clerk, EPIC, June 30, 2004 (on file with EPIC).

[103] *Id.*

[104] E-mail from Gunnel Helmers, *supra*.

[105] Bygrave & Aarø, at 337.

[106] *Id.* at 336.

[107] Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits 48 (The Hague: Kluwer Law International, 2002).

[108] *See also* Bygrave & Aarø, *supra*, at 339-340.

A decision of principle by the Data Protection Tribunal in late 2002 defines the scope of the Act, specifically as it applies to human biological material such as blood samples. The tribunal'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.[109] 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 Data Protection Tribunal, applying a view of "data" and "information" typical in 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.[110]

The new law also provides specific rules for video surveillance. Video surveillance that does not create actual files falls under weaker protection than regular personal data registers. However, if the surveillance results in the actual 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 the surveillance if it does not conform with the Act. If the 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 the surveillance is of "essential significance" for investigating suspected criminal conduct that can result in more than six months imprisonment (Section 202a).

General exemptions to the Personal Data Act are made for processing of data for purely private or purely artistic, literary or journalistic purposes (Sections 3 and 7). Processing of data for historical, statistical, or scientific purposes is also treated leniently (*see, e.g.*, Section 11(2)). Some data registers kept for purposes of policing and/or national security are also taken outside the control competence of the Data Inspectorate (Chapter 1 of the regulations to the Act).

The Personal Data Act is expected to undergo a comprehensive review followed by changes to some of its provisions.[111] For example, the recent Court of Justice of the European Communities decision in the criminal proceedings against Bodil Lindqvist has led to a change in policy of the Norwegian Data Inspectorate.[112] The Inspectorate had exempted the posting of personal data on homepages for ostensibly private or domestic purposes from the Act. The *Lindqvist* decision, however, states that the exemption for "private" processing does not apply when the data can be accessed by an indefinite number of persons. Unless personal data posted on a web site 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 European Data Protection Directive and the PDA.[113]

Wiretapping normally requires the permission of a tribunal and is initially limited to four weeks.[114] The total number of telephones monitored was 360 in 1990, 467 in 1991, 426 in 1992, 402 in 1993, 541 in

---

[109] *See* appeal decision in case 8/2002, available at <http://web.archive.org/web/20030618200212/http://www.personvernnemnda.no/klagesaker/nrVIII2002.html>.

[110] Lee A. Bygrave, "The Body as Data? Reflection on the Relationship of Data Privacy Law with the Human Body," edited text of speech given at an international conference organized by the Office of the Victorian Privacy Commissioner on the theme "The Body as Data", Federation Square, Melbourne, September 8, 2003, available at <http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/CF51D885BA101AACCA256E050012CBA5/$FILE/Bygrave%20paper.pdf>.

[111] Email from Lee A. Bygrave, Associate Professor, Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo., to Kenneth Farrall, IPIOP Law Clerk, EPIC, June 11, 2004 (on file EPIC).

[112] *See* EU Data Protection Directive (1995/46/EC), OJEC of November 23, 1995 No L. 281 p. 31, Article 3(2), second indent, available at <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett>.

[113] *Id.*

[114] *See generally* Criminal Procedure Act, chapter 16 a.

1994 and 534 in 1995.[115] A Supervisory Board reviews the warrants to ensure the adequacy of the protections. 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.[116] This included keeping files on children as young as eleven years old.

A recent report from an official Norwegian commission has tackled the controversial issue of balance between crime prevention and privacy in the light of global terrorism and organized crime.[117] One proposal in the report involves reducing current restrictions on police bugging of non-telephonic conversations between criminals, a practice known as "*romavlytting*" in Norwegian. Although similar proposals have been made in the past, there are indications that some conservative politicians who have previously opposed such a measure now support it.[118]

Another official commission has recently issued a major report concerning the regulation of personal data registers established by the police, of which there are many types.[119] The report, which has not raised much controversy, recommends the enactment of a new statute to regulate specifically the establishment and use of such registers.[120] A proposition based on an ILO convention proposes that the national governments shall issue biometric ID cards to seafarers. The ID cards are proposed as a safeguard against terrorism. An amendment was also proposed to the regulations regarding object security based on the need to secure objects against terrorism and crime. The proposed amendment prepares for a somewhat increased use of security clearance, access control and camera surveillance.[121]

Provisions of the Criminal Procedure Act allow for wiretapping without the permission of the tribunal in two circumstances. First, Section 216a allows wiretapping for narcotics investigations and in connection with cases involving national security, albeit with the permission of a magistrate court. Second, Section 216b allows wiretapping in connection with some less serious offenses but requires the permission of a magistrate court.

New legislation to monitor the secret services was approved in 1995 following the Lund Commission's recommendations.[122] The legislation created a new Control Committee to monitor the activities of the Police Security Services, the Defense Security Services, and the Defense Intelligence Services. The former Minister of Justice and the head of the Norwegian security police (POT) were forced to resign from the government in 1996 after it was revealed that the POT had placed a member of the Lund Commission under surveillance and requested a copy of her *Stasi* file from the German authorities four times.[123] Later it was discovered that the POT had also investigated several key members of the Parliament who have oversight over the agency.[124] In 1997, the Parliament agreed to allow people who were under surveillance by the POT to review their records and to obtain compensation if the

---

[115] Government of Norway report to the UN Human Rights Commission, CCPR/C/115/Add.2, 26 May 1997.

[116] "Judicial Inquiry into Norwegian Secret Surveillance," Fortress Europe Circular Letter (FECL) 43 (April/May 1996), available at <http://www.fecl.org/circular/4305.htm>.

[117] *See* "*Mellom Effektivitet og Personvern,*" NOU 2004:6.

[118] Email from Lee Bygrave, *supra.*

[119] *See* "*Kriminalitetsbekjempelse og Personvern*," NOU 2003:21.

[120] *Id.*

[121] E-mail from Gunnel Helmers, *supra*.

[122] Act No. 7 of 3 February 1995 on the Control of the Secret Services.

[123] "Minister Resigns," Statewatch bulletin, November-December 1996, vol. 6 no 1.

[124] "Minister Steps back after New Snooping Scandal," FECL 49 (December 1996/January 1997), available at <http://www.fecl.org/circular/4906.htm>.

surveillance was unlawful. The POT has records on over 50,000 people.[125] The period for allowing access to these records has now terminated.

Many other laws contain provisions relevant to privacy and data protection. These include the Administrative Procedures Act of 1967 and the Criminal Code of 1902.[126] The Criminal Code first prohibited the publication of information relating to "personal or domestic affairs" in 1889.[127] The Criminal code also prohibits the unauthorized opening of sealed correspondence, including cracking security mechanisms.[128] The Criminal Code also prohibits covert monitoring or recording of telephone conversations or other conversations in closed settings.[129] In December of 2000, a Norwegian news service reported that Norwegian military and police intelligence units entered into an agreement with the country's 15 largest companies to perform Internet surveillance.[130] The system was reported to be similar to the US FBI's Carnivore system, which intercepts and monitors any information sent across the Internet. The Norwegian Justice Department confirmed the existence of the system, but sources claimed that it has not been implemented on a large scale. The Norwegian Parliament has demanded a review of the project, which was created to defend the national information technology infrastructure.

The 1970 Act on Public Access to Documents in the (Public) Administration provides for public access to government records. Under the Act, there is a broad right of access to records. The Act has been in effect since 1971. The Act does not apply to records held by the Parliament, the Office of the Auditor General, the Ombudsman for Public Administration, or other parliamentary institutions. There are exemptions for internal documents; information that "could be detrimental to the security of the realm, national defense or relations with foreign states or international organizations;" subject to a duty of secrecy; "in the interests of proper execution of the financial, pay or personnel management;" 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; and documents prepared by a ministry in connection with annual fiscal budgets. The King can make a determination that historical documents in the archive that are otherwise exempted can be publicly released. If access is denied, individuals can appeal to a higher authority under the act and then to a court.

A news report early in the year 2000 indicated that Norway's Data Protection Registrar intended to investigate the merged banking giant Postbanken/DnB, which had been criticized for using postal employees to collect information and make lists of potential clients. The investigations were to determine whether the postmen and women were breaching regulations governing the privacy of postal service clients.[131] An article published in February 2002 indicates the state welfare agency, *Trygdeetaten*, would like to order banks to advise of any "unusual" transactions involving accounts held by welfare recipients. The proposal, which would require the relaxation of existing privacy laws, has prompted opposition from the banking industry and some politicians. The banking industry has warned against law changes which would threaten client confidentiality. The agency, however, feels that it is the only way they will be able to "crack down" on welfare cheating.[132] In June, 2003, a new money laundering law was passed which

---

125 "Parliament Says People Can See Files," Statewatch bulletin, May-June 1997, vol 7 no 3.

126 *See generally* Bygrave & Aarø, *supra*, at 334-335.

127 *See* Prof. Dr. Juris Jon Bing, Data Protection in Norway, 1996, available at <http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html>.

128 Bygrave & Aaro, *supra*, at 334.

129 *Id*.

130 Digi.no, available at <http://www.digi.no/d2.nsf/frames/b9569727*1913023575>.

131 "Norway's Big Bank Tactics under Fire," Aftenposten, Jan. 27, 2000, available at <http://tux1.aftenposten.no/english/business/d121739.htm>.

132 "State Wants a License to Snoop," Aftenposten, Feb. 12, 2002, available at <http://www.aftenposten.no/english/local/article.jhtml?articleID=274418>.

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.[133]

In addition to data protection regulations that contain privacy provisions, Norway has also addressed privacy issues stemming from threats of terrorism and human rights violations. The European Convention on Human Rights and Fundamental Freedoms of 1950 (ECHR) and the International Covenant on Civil and Political Rights of 1966, both of which contain a catalogue of basic human rights, including express rights to privacy, have recently been incorporated into Norwegian law.[134] In April 2002, the Norwegian Parliament adopted amendments to the Norwegian Penal Code, which include prohibitions against "terrorist acts."[135] Many privacy advocates and non-governmental organizations 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.[136]

Norway has also agreed to support United Nations (UN) Security Council Resolution 1368, which reconfirms the right to individual or collective self defense, and Resolution 1373, which outlines the measures member states of the UN must implement in order to prevent and suppress terrorist activities.[137] Other steps Norway has taken to counteract terrorism are to call for the establishment of the International Criminal Court in The Hague, to ratify all UN Conventions against international terrorism in force, and to sign the UN Convention for the Suppression of the Financing of Terrorism.[138] To safeguard human rights and fundamental freedoms in light of the threat of terrorism, the Norwegian government granted the Norwegian Institute for Human Rights the status of a national human rights institution in 2002. The Institute monitors Norway's adherence to international human rights standards. One area of particular concern that the Institute is monitoring is Norway's treatment of persons in pre-trial detention.[139]

Norway is a member of the Council of Europe (CoE) and has signed and ratified the CoE's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) and has signed ETS No. 181.[140] It has signed and ratified the ECHR.[141] Norway has signed, but not ratified, the CoE's Convention on Cybercrime.[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.

Republic of Peru

Different articles of the 1993 Constitution protect the right to intimacy, the secrecy of communications and private documents, the inviolability of the home, the freedom of press, freedom of expression and access to the public information. Article 2 states, "Every person has the right: 6. To assurance that

---

133 "New Money Laundering Law Passed," Aftenposten, May 29, 2003, available at <http://www.aftenposten.no/english/business/article.jhtml?articleID=554420>.

134 Bygrave & Aaro, *supra.*

135 International Helsinki Foundation (IHF) Report, "Human Rights in the OSCE Region: Europe, Central Asia and North America 2003 (Events 2002)"<http://www.ihf-hr.org/viewbinary/viewdocument.php?doc_id=2261>.

136 *Id.*

137 UN GAOR 56th Sess. Plen. Item 166: Measures to Eliminate International Terrorism (Statement by H.E. Mr. Ole Peter Kolby Ambassador Permanent Representative) (2001), available at <http://www.un.org/terrorism/statements/norwayE.html>.

138 *Id.*

139 *Id.*

140 Signed March 13, 1981; ratified February 20, 1984; entered into force October 1st, 1985, available at <http://www.coe.fr/dataprotection/edocs.htm>.

141 Signed November 11, 1950; ratified January 15, 1952; entered into force September 3, 1953.

142 Signed November 23, 2001.

information services, whether or not they are computerized, public or private, will not release information affecting one's personal and family intimacy. 7. To his honor and good reputation, personal and family intimacy, and his own voice and image. Every person affected by inaccurate or injurious statements contained in any medium of social communication has the right to free, immediate and proportional rectification, other legal responsibilities notwithstanding. 10. To the inviolability and secrecy of private documents and communications. Communications, telecommunications, or documents stemming there from may only be opened, seized, intercepted, or tapped with a bench warrant and all the guarantees set forth by law. Confidentiality must be maintained regarding all matters not related to the cause of the search. Private documents obtained in violation of this precept are legally inadmissible. Books, receipts, as well as accounting and administrative documents are subject to inspection or auditing by the proper authorities in accordance with the law. Any action taken involving them may not include their removal or seizure without a court order. 9. To the inviolability of his home. No one may enter the home or conduct any investigation or search without authorization from the inhabitant or a court warrant except in the case of flagrante delicto or very grave danger of the same. Law governs exceptions for reasons of health or serious risk. 3. To freedom of conscience and religion, individually or as a member of a group. No one may be persecuted for his ideas or beliefs. There is no such thing as a crime of opinion. (. . .) 4. To freedom of information, opinion, expression, and the dissemination of thought through the spoken or written word or in images, by any means of social communication, and without previous authorization, censorship, or impediment whatsoever, in accordance with the law. Crimes committed by means of books, the press, or other media of social communication are outlined in the Penal Code and will be tried in a court of law. Any action that suspends or closes any organ of expression or prevents its free circulation also constitutes a crime. The right to inform and express opinions includes the right to found means of communication. 5. To request information that one needs without disclosing the reason, and to receive that information from any public entity, within the period specified by law, at a reasonable cost. Information that affects personal intimacy and that is expressly excluded by law or for reasons of national security is not subject to disclosure. Banking secrecy and confidentiality concerning taxes may only be lifted at the request of a judge, the National Prosecutor, or a congressional investigative commission in accordance with the law and provided that such information relates to the case."[143]

All this constitutional rights are included, in one way or another, inside the article 1, that settles down that "the protection of the person and respect for his dignity plows the supreme goal of society and the State".

The Civil Code of 1984 recognizes the intimacy of the private life, in all its aspects, like an object of legal protection with the only limits of the consent of the own person, the existence of a social interest or a reason of public order. Article 14 of the Civil Code states that "personal and family intimacy may not be made public without the consent of the person or, if this one is dead, without the consent of its spouse, descendants, ascendants or brothers, excluding and in that order."

This norm tries to prevent the unfolding of diverse attitudes that suppose to snoop and to interfere in the intimacy of the private life or that represents an invasion or illegal search of goods or properties of the person, without mediation a public interest. A second aspect does not only refer to intimacy but also to divulging, by any means, some privacy manifestations.[144]

According to article 16 of the Civil Code, "the mail, the communications of any sort or the recordings of the voice, when they are confidential or talk about personal and familiar private life, cannot be

[143] Constitution of Peru, available at <http://www.asesor.com.pe/teleley/biblioteca/constitucional/5000f.htm> <www.idlo.int/texts/leg6577.pdf>.
[144] Carlos Fernández Sessarego, *Derecho de las Personas* 59 (Studium 1987).

wiretapped or disclosed without the assent of the author and, in their case, of the recipient. The publication of the personal or familiar memories, in equal circumstances, requires the authorization of the author. When the author or the recipient has died (…) corresponds to its heirs the right to grant the respective assent. If there is no agreement between the heirs, the judge will decide. The prohibition of the posthumous publication made by the author or the recipient cannot extend beyond fifty years from its death."

Peru does not have a comprehensive Data Protection Act. However, numerous specific legal regulations protect the privacy and the Ombudsman is doing the work of an agency of data protection.[145] In August 2004, the Ministry of Justice published a project of bill of data protection. It contains provisions related to general data protection principles in accordance with the Peruvian Constitution, based on the European Union Data Protection Directive and the Spanish Data protection Act of 1992, the rights of data subjects, the obligations of data controllers and data users, the supervisory authority and sanctions. The rules of procedures would be developed by the regulation of the law. If the project of bill is passed, the specific regulations should have to be adapted to it.[146]

In the Public Registries any person has the right to request, without disclosing the reason, through a payment of a fee, copy of the documentation that exists in the Registries. However, the General Regulation of Public Registries, article 128, relative to publicity of the registries states: "when the information requested affects the right to intimacy, this information can only be granted to those who demonstrate legitimate interest, according to the regulations established by the National Superintendent of the Public Registries."[147]

The Public Registries handles information that might be sensitive. This might include, for example, information from the Personal Registry such as judicial rulings regarding the mental status of someone, separation agreements between spouses, or child custody rulings. The office of Lima (and several of the main registry offices of Peru) has an online service for subscribers. Soon, the interconnection between all offices of the Public Registries in Peru will be completed, making possible to access them from any computer connected to Internet, after paying the standard rate.

Article 69 of the Penal Code establishes that "anyone who has completed a penalty or security measure imposed on them by the court must be reinstated in the society without further proceedings. The reinstatement produces the following effects: (. . .) 2. The cancellation of their criminal, judicial and police official records. The corresponding certificates do not have to express the penalty nor the reinstatement." In crimes against the honor (insult, calumny, defamation), article 135 states that "the evidence is never admitted by the court in any case if: (. . .) 2. The imputation treats on personal and familiar intimacy, or a crime against the sexual freedom" (. . .).

The Organic Law of the National Identification Registry and Civil Status (1995) created an autonomous agency which may "collaborate with the exercise of the functions of pertinent political and judicial authorities in order to identify persons" but is "vigilant regarding restrictions with respect to the privacy and identity of the person" and "guarantees the privacy of data relative to the persons who are

[145] Constitution of Peru, article 162: "It is the duty of the Ombudsman to defend constitutional rights and fundamental personal rights and those of the community; and to supervise the fulfillment of the duties of State administration and public services to the citizenry. (. . .) It has the right to initiate proposals for laws, and may propose measures to facilitate the fulfillment of the functions of the office. (. . .)

[146] Project of bill of data protection available at <http://www.minjus.gob.pe/minjus/PROYECTODELEY.PDF>.

[147] *Superintendencia Nacional de los Registros Públicos* <http://www.orlc.gob.pe>.

registered." The Law also requires all persons to carry a National Identity Document featuring a corresponding number, photograph and fingerprint.[148]

In January 2002, a law creating a National Registry of Persons with Disabilities was adopted.[149] The registry is administered by the National Council of Integration of Persons with Disabilities (CONADIS).

The Law of Telecommunications[150] article 4, states "all person has right of the inviolability and secrecy of the telecommunications. The Ministry of Transports, Communications, Housing and Construction is in charge to protect this right." Every concession contract of public services of telecommunications has to indicate the guarantees that the providers of the services must offer to ensure the secrecy of the communications. Constitute very serious infractions to the concession contract "the interception or unauthorized interference of the services of telecommunications not destined to the free use of the general public", and the "spreading of the existence or the content, or the publication or any other use of all class of data obtained by means of the interception or interference of the services of telecommunications not destined for general public use."[151]

The General Regulation of the Law of Telecommunications says that "it is attempted against the inviolability and secrecy of the telecommunications, when deliberately a person who is not the one who originates nor is the addressee of the communication, removes, intercepts, interferes, changes or alters its text, turns aside the course, publishes, discloses, uses, tries to know or to facilitate that himself or another person, knows the existence or the content of any communication. (…) The concessionaires of public services of telecommunications are forced to safeguard the secrecy of the telecommunications and the protection of personal data, to adopt the reasonable measures and procedures to guarantee the inviolability and secrecy of the communications attended through such services, as well as to maintain the confidentiality of the personal information relative to their users who obtain in the course of their businesses, except for previous, express consent and in writing of its users and other involved parts or by judicial mandate. The holders of private services of telecommunications will have to adopt their own security measures on inviolability and secrecy of the telecommunications." (. . .)[152]

In April 2002, Peru passed a new law to govern the interception of communications and private documents.[153] Under this law, a judicial warrant is needed to seize documents or intercept communications. The law requires telecommunications operators to provide all necessary technical assistance and facilities to carry out interceptions. The powers may be used in the investigation of crimes including kidnapping, child traffic, drug traffic, customs violations, terrorism, crimes against the humanity, and treason.

In the recent past there were numerous reports of abuse of surveillance of the National Intelligence Service (*Servicio de Inteligencia Nacional* - SIN). The SIN conducted widespread surveillance and illegal phone tapping of government ministers and judges assigned to constitutional cases, beginning in the early 90s. Army agents used sophisticated Israeli phone-tapping equipment to monitor telephone conversations, and copies of the conversations were delivered to Vladimiro Montesinos.[154] The SIN maintained close ties with the US Central Intelligence Agency, including a covert assistance program to

---

[148] *Ley Orgánica del Registro Nacional de Identificación y Estado Civil*, Law 26497, July 11, 1995, available at <http://www.leyes.congreso.gob.pe/Imagenes/Leyes/26497.pdf>.
[149] *Ley General de la Persona con Discapacidad*, Law 27050, available at <http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27050.pdf>.
[150] *Texto Unico Ordenado de la Ley de Telecomunicaciones*, D.S. 013-93-TCC, available at <http://www.mtc.gob.pe/secom/mlegal/leyes/ley.htm>.
[151] Law of Telecommunications article 52-f), article 87, numerals 4 and 5.
[152] *Texto Unico Ordenado del Reglamento General de la Ley de Telecomunicaciones*, D.S. 027-2004-MTC, published on July 15, 2004, article 13.
[153] Law 27697, *Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional*, *Diario Oficial El Peruano*, April 12, 2002, available at <http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27697.pdf>
[154] "Former Agent Accuses Peru Spy Chief," AP, March 17, 1998.

combat drug trafficking.[155] The SIN has allegedly conducted a nationwide surveillance campaign with the sole purpose of intimidating political opposition figures, including the former UN General Secretary Javier Pérez de Cuéllar while he ran for President against Alberto Fujimori.[156]

In 2003, the parliamentary investigation that looked into telephone wiretapping carried out during the government of Alberto Fujimori, discovered that Vladimiro Montesinos had used the Office of Electronic Information (DIE) of the SIN for exclusive dedication to telephone monitoring. For that purpose, they activated 29 interception points in Lima and Callao, of which only 20 have been deactivated.[157]

According to the parliamentary commission, some of this surveillance equipment is still in operation. This presumption is also based upon reports of telephone wiretapping made after the deactivation of the SIN operation. Last September, journalists of a television program denounced a continuation of this operation by the current intelligence service. The accusation caused the dismissal of the head of intelligence, who admitted spying on journalists, but who alleged that the investigation only studied how "reserved information" was filtered from the government to the press.[158]

Telephonic monitoring is being carried out by ex-personnel of the intelligence service (technicians in telecommunications) working freely in the job market. Between 2001 and 2003, the National Intelligence Council has made several operations to break-up the clandestine wiretapping network that uses wiretap equipment that belonged to the prior SIN established by Fujimori´s government. This network would have 80 wiretapping equipment and electronic espionage (equipment from Israel such as Octopus and Cellular Telephone Monitoring Systems - CTMS, models 6000 and 6001) operating in seven cities including Lima, and its members would have international contacts in Panama, Colombia, Venezuela, Brazil and Chile.[159]

CPSR-Perú and *Privaterra*, an on going project of *Computer Professionals for Social Responsibility*, organized trainings in privacy and secure communications for human rights and research journalism NGOs in Peru and Colombia.[160]

In August 2001, Peru enacted a data protection law covering private credit reporting agencies called *Centrales Privadas de Información de Riesgos* – CEPIRS.[161] These private companies are in charge of collecting and processing the credit risk information of individuals and companies whose information is recorded in databases. The law regulates the incorporation of credit bureaus, qualifications for shareholders and the sources of information they can use. Similar to Article 11 of the EU Data Protection Directive, it sets out the information that must be provided to the data subject when the data has not been obtained from him or her. In addition, the law prohibits credit bureaus from collecting sensitive information; data violating the confidentiality of bank or tax records, inaccurate or outdated information, bankruptcy records older than five years, other debtor records five years after the debt was paid. It provides that credit agencies must adopt security measures and grants individuals have the following rights: (1) the right to access to information; (2) the right to modify or cancel their personal data; (3)

---

[155] 1998 Human Rights Watch Report, available at <http://www.hrw.org/hrw/worldreport/Americas.htm>.
[156] "Former U.N. Chief Charges Peru Tapped His Phone," Reuters, August 4, 1997.
[157] The equipment used by the DIE for the interception of fixed and cellular telephones was manufactured in Israel, Germany and the United States and it is calculated that more than 100 units were involved.
In downtown Lima six interception points were implemented where practically all public, newspaper, private and even ecclesiastical organizations were controlled. *Diario El Comercio, Lima*.
[158] "Now journalists are spied upon. We must remember what happened with Montesinos, we let him, we played the fools (…) I see that history is repeating itself", said Cecilia Valenzuela, program director for *La Ventana Indiscreta* ("The Indiscreet Window") of Channel 2 Television, also director of the *Instituto Prensa y Sociedad* (Press and Society Institute) – IPYS, who denounced the harassment of their journalists by intelligence agents.
[159] La República, March 14, 2004, at 15.
[160] CPSR-Perú <http://www.peru.cpsr.org>, Privaterra <http://www.privaterra.org>.
[161] *Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información*, Law 27489, available at <http://www.leyes.congreso.gob.pe/Imagenes/Leyes/27489.pdf>.

judicial relief for non-consumers or consumer protection law. The law also creates strict liability for damages. The C*omisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual* – INDECOPI (Government Agency for Consumer Protection) is in charge of applying fines for violation of the law and issuing injunctions to correct errors.

In May 2004, a journalist research of *El Comercio*, the most important newspaper in Lima, published an extensive report in which they revealed the sale of data bases from approximately 60.000 Peruvian citizens, in CDs, at the cost of US$ 20 each one, carried out by data dealers based in popular stores where hardware and software are also commercialized. The data bases contain name, address, fixed and cellular telephone, e-mail, work place, consumer habits, economic activities. In the file called "segmented", there is a list of lawyers, architects, doctors, notaries, executive women, university professors, "top companies", NGOs, information that is upgraded every six months, according to the data dealers[162].

The right of informational self-determination is partially protected under the action of habeas data. However, habeas data does not have a preventive character, it is a reparative mechanism used only after the damage has been done.[163] In several sentences the Constitutional Tribunal has mentioned the right of informational self-determination, which is not specifically noted in the Peruvian Constitution, "one of whose manifestations consist on the ability of all person of requesting the rectification of inexact information on itself, contained in databases or registries".[164]

Article 154 of the Penal Code[165] states that "a person who violates personal or family privacy, whether by watching, listening to or recording an act, a word, a piece of writing or an image using technical instruments or processes and other means, shall be punished with imprisonment for not any longer than two years." Article 157 criminalizes the disclosure of sensitive data including "political and religious convictions" and other aspects of intimate life.

Article 161 of the Penal Code establishes "that a person who unlawfully opens a letter, document, telegram, radio telegram, telephone message or other document of a similar nature that is not addressed to him, or unlawfully takes possession of any such document even if it is open, shall be liable to imprisonment of not more than two years and to sixty to ninety days' fine." A sentence of not less than one year nor more than three years is to be given to any "person who unlawfully interferes with or listens to a telephone or similar conversation." Public servants guilty of the same crime must serve not less than three or more than five years and must be dismissed from their post. A person who unlawfully tampers with, deletes, or misdirects "the address on a letter or telegram," but does not open it, "is liable to twenty to fifty-two days' community service."

In July 2000 a Computer Crimes Act was adopted and codified in Article 207(A)(B)(C) of the Penal Code.[166] The Act prohibits unlawful access, use, interference or damage to a system, database, or network of computers. Sanctions include up to five years imprisonment.

In October 2003, Congressman Flórez-Araoz presented the bill project 8749, called *Law that regulates the advertising or commercial communications by Internet*. This proposal intends to eliminate spam and

[162] El Comercio, May 10, 2004, at A2.
[163] Tribunal Constitucional, Expediente 0666-96-HD/TC. Published on July 8, 1998, available at <http://www.tc.gob.pe/jurisprudencia/1998/0666-1996-HD.html>.
[164] Tribunal Constitucional <http://www.tc.gob.pe/jurisprudencia/2003/0700-2003-HC Resolucion.html>.
[165] *Código Penal* (Penal Code), available at <http://www.leyes.congreso.gob.pe/CodigoP.htm>.
[166] Law 27309, *Diario Oficial El Peruano*, July 17, 2000, incorporating article 207 A, B y C of the Penal Code.

forbids the sale of personal data bases of e-mails for being used for commercial or advertising communications.[167]

In November 2003, the Parliament passed a law that obligate to the administrators of Internet cafes to install a navigator filter or another mechanism that makes impossible the visualization of pornographic content to prevent that a minor surfing the Internet, could see it, under the administrator´s responsibility.[168] In addition, local authorities of several districts of Lima passed similar regulations that also include penalties such as fines and the definitive closing of the local.

In Miraflores district, in Lima, 25 video cameras have been settled in the main streets and parks. These cameras have visualization fields of 360 degrees, a scope up to 300 meters and are connected to two centrals of surveillance: the communications station of the Municipality, called *Alerta-Miraflores*, and the National Police emergencies station.[169]

Local authorities of Santiago de Surco, another district in Lima, announced the obligatory use of radio frequency identification (RFID) devices for the identification of dogs of dangerous races. If they do not use it under its loin, the owner of the dog should pay a fine and, if relapse again, the animal will be captured.[170]

The Constitution provides for freedom of speech and of the press, and the Government generally respected this right in practice; however, some problems remained. On August 18, César Hildebrandt, the director of TV program *En la Boca del Lobo* ("In the Wolf's Mouth"), disseminated a clandestine, recorded audio of a private telephone conversation of President Toledo with one of his advisors.[171]

Freedom of information is constitutionally protected under the habeas data. In May 1994, Law 26301 was passed in order to set temporary legal standards for the legal application of habeas data.[172] The Law requires that all habeas data actions be notarized, although reasons for the requested action must not necessarily be given, and filed with the legal authority from which information or an action is desired. The Law sets out the time periods and procedures for taking actions under clauses 5 and 6 of Article 2 of the Constitution.

A Law of Transparency and Access to Public Information was adopted in August 2002 and amended in January 2003.[173] Under the law, every person has the right to request information in any form from any government body or private entity that offers public services or executes administrative functions without having to explain why. Documentation funded by the public budget is considered public information. Public bodies must respond within seven working days, which can be extended in extraordinary cases for another five days.

There are three classes of exceptions: for national security information, the disclosure of which would cause a threat to the territorial integrity and/or survival of the democratic systems and the intelligence or counterintelligence activities; reserved information about crimes and external relations; and confidential information relating to pre-decisional advice, commercial secrets, ongoing investigations and personal

---

[167] *Ley que regula las comunicaciones comerciales publicitarias o promocionales por vía electrónica*, available at <http://www.elcomercioperu.com.pe/ecenre/Html/2003-11-06/EcEnReArticu0450.html>.
[168] *Ley que Prohíbe el Acceso de Menores de Edad a Páginas Web de Contenido Pornográfico*. Law 28119.
[169] *Miraflores Boletín Informativo*, Year 2, July 2004, at 5.
[170] *Dominical de La República*, May 9, 2004, at 19.
[171] U.S. Department of State <http://www.state.gov/g/drl/rls/hrrpt/2003/27916.htm>.
[172] Law 26301, A*prueban la Ley referida a la aplicación de la Acción Constitucional de Habeas Data*, May 2, 1994, available at <http://www.leyes.congreso.gob.pe/Imagenes/Leyes/26301.pdf>.
[173] *Ley de transparencia y acceso a la información pública,* Law 27808, modified by Law 27927, both consolidated in an unified text approved by Supreme Decree 043-2003-PCM. A history of the development of the bill is available at <http://www.freedominfo.org/news/peru2/>.

privacy. Information relating to human rights violations and the Geneva Convention of 1949 cannot be classified. The exempted information can be obtained by the courts, Congress, the General Comptroller, and the Ombudsman in some cases. Once administrative procedures are completed and refused, the requestor can claim access to courts under Law 27584[174] or under Law 26301 for the constitutional habeas data.[175] In practice, habeas data is faster and more effective.

The law also requires government departments to create web sites and publish information on its organization, activities, regulations, budget, salaries, costs of the acquisition of goods and services, and official activities of high-ranking officials. Detailed information on public finances has to be published every four months on the Ministry of Economy and Finance's web site.

The campaign for the law was lead by the *Consejo de la Prensa Peruana*[176] and other organizations such as the *Instituto Prensa y Sociedad.*[177] The amendment to the law incorporated a revised exemption for national security that was negotiated by the Peruvian Press Council and the armed forces.[178] Also included almost all of the proposals concerning national security restrictions put forward by the Peruvian Press Council and the Ombudsman.[179]

The Constitutional Tribunal has settled down clearly that the right of access to public information imposes to the organisms of the public administration the duty of informing, and that the information that is provided is not false, incomplete, fragmentary or confusing.[180]

In 1992, during Alberto Fujimori´s government, were passed several anti-terrorism laws that allowed penal suits for civilians in military courts, tribunals without face, secret hearings, life sentences, criminalization of behaviors that ware not properly terrorism, among other, forcing the article 139 of the Constitution of Peru, the articles 8, 9, 10 and 11 of the Universal Declaration of Human Rights, the articles 9 and 14 of the International Pact of Civil and Political Rights, and the article 8 of the Inter-American Convention of Human Rights. The Constitutional Tribunal concluded on January 3, 2003, that it was unconstitutional and an excessive punishment.[181]

On February 12, 2003, was promulgated the Legislative Decree 922 by President Alejandro Toledo. It was published, along with seven other security laws. Article 12 states that "oral hearings for the crime of terrorism will be public. The public and media outlets will have access to the courtroom. However, the use of video cameras, tape recorders, cameras and similar technology is prohibited.[182]

Peru signed the American Convention on Human Rights on July 28, 1978, and accepted the jurisdiction of the Inter-American Court of Human Rights on January 21, 1981, withdrew from the jurisdiction of the Inter-American Court of Human Rights in July 1999, which was reestablished on January 12, 2001.

---

[174] Law 27584, *Ley que regula el Proceso Contencioso Administrativo*, December 7, 2001.
[175] Law 26301, *aprueban Ley referida a la aplicación de la acción Constitucional de Habeas Data*, May 2, 1994, available at <http://www.asesor.com.pe/teleley/bull505.htm>.
[176] Peruvian Press Council, a NGO of media owners that works on freedom of press and freedom of information.
[177] Press and Society Institute, a NGO of national and Latin American journalists, affiliated with Reporters without Borders and the International Freedom of Expression Exchange (IFEX) of Canada that protect freedom of press, freedom of information and fight against corruption.
[178] See <http://www.freedominfo.org/news/peru1/>.
[179] See <http://www.freemedia.at/wpfr/Americas/peru.htm>.
[180] *Tribunal Constitucional* <http://www.tc.gob.pe/jurisprudencia/2003/1797-2002-HD.html>.
[181] *Sentencia del Tribunal Constitucional, Expediente N° 010-2002-AI/TC*, published on January 4, 2003, <http://www.tc.gob.pe/jurisprudencia/2003/0010-2002-AI.html>.
[182] See <http://www.ifex.org/es/content/view/full/33608/>.

According to Article 205º of the Constitution, "after exhausting internal remedies, those who consider themselves denied the rights recognized in the Constitution may resort to international tribunals or organs constituted by treaty or agreement to which Peru is a party."

Republic of the Philippines

Article III of the Constitution of the Philippines contains the Bill of Rights. Section 1 of the Bill of Rights states that the "Congress shall give highest priority to the enactment of measures that protect and enhance the right of all the people to human dignity."[183] Section 2 states that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized."[184] Section 3(1) states that the "privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law."[185] It further states that "any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding." Section 7 states that "the right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law."[186]

Although there is currently no general data protection law, the Information Technology and E-Commerce Council (ITECC) has proposed in 2003 a data privacy law.[187] This law is expected to adhere to EU standards of data privacy, despite the difficulty of negotiating the differences between the policies of the EU and the US, one of Philippines' largest trading partners.[188] The proposed privacy law may also address some of the privacy concerns inherent in a national ID system.[189]

Despite the lack of a current data protection law, there is a recognized right of privacy in civil law.[190] The Civil Code of the Philippines states that "[e]very person shall respect the dignity, personality, privacy, and peace of mind of his neighbors and other persons," and punishes acts that violate privacy by private citizens, public officers, or employees of private companies.[191]

Article 26 of the Civil Code states that "every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief: (1) Prying into the privacy of another's residence; (2) Meddling with or disturbing the private life or family relations of another; (3) Intriguing to cause another to be alienated from his friends; (4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical

---

183 Constitution of the Philippines, Art. VIII, § 1.
184 *Id.* § 2.
185 *Id.* § 3(1).
186 *Id.* § 7.
187 Eleanore C. Sanchez, "Technology Body Drafts Data Privacy Measure," Business World, April 16, 2003, at 3.
188 *Id.; see also* Eleanore C. Sanchez, "ITECC Mulls Data Privacy Law Proposal," ITMatters.com, March 14-15, 2003, available at <http://itmatters.com.ph/news/news_03142003a.html>.
189 *Id.*
190 Cordero v. Buigasco, 34130-R, April 17, 1972, 17 CAR (2s) 539; Jaworski v. Jadwani, CV-66405, December 15, 1983.
191 Civil Code, Article 26; "Philippine Supreme Court Decision of the National ID System," July 23, 1998, G.R. 127685.

defect, or other personal condition."[192] Article 32(11) of the Civil Code states that "any public officer or employee, or any private individual, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs the privacy of communication and correspondence shall be liable to the latter for damages."[193]

The Philippines has only one law on data transfer, Presidential Decree (P.D.) No. 1718 entitled Providing for Incentives in The Pursuit of Economic Development Programs by Restricting The Use of Documents and Information Vital to The National Interest in Certain Proceedings and Processes. While the law was passed in 1980, it lacks force because rules and regulations have not been issued to allow enforcement. Broadly, P.D. 1718 prohibits the export of all documents and information from the Philippines to other countries that may adversely affect the interests of Philippine corporations, individuals, or government agencies. P.D. 1718 contains exceptions for exportation of information that are a matter of form, in connection with business transactions or negotiations that require them, in compliance with international agreements, or made pursuant to authority granted by the designated representative of the President.[194]

Bank records are protected by the Bank Secrecy Act[195] and the Secrecy of Bank Deposits Act.[196] The Act provides that deposits with banks or banking institutions are confidential and may not be examined, inquired, or looked into absent "exceptional circumstances." Those circumstances include: the written permission of the depositor, cases of impeachment, court orders in cases of bribery or dereliction of duty of public officials, cases where the money deposited or invested is the subject matter of litigation, and cases covered by the Anti-Graft and Corrupt Practices Act.[197] The Anti-Money Laundering Act of 2001 allows exceptions to the Bank Secrecy Act and the Secrecy of Bank Deposits Act.[198] Section 9(c) of the Act requires banks, insurance companies, financial institutions, and "other entities administering or otherwise dealing in currency, commodities, or financial derivatives"[199] to report to the Anti-Money Laundering Council of the *Bangko Sentral ng Pilipinas* all transactions (including series or combinations of transactions) in excess of PP four million (~USD 75,000).[200] The institution does not have to report the transaction if it involves a "properly identified client and the amount is commensurate with the business or financial capacity of the client; or those with an underlying legal or trade obligation, purpose, origin, or economic justification."[201] The Act does provide neither explicit definitions of a "properly identified client," nor a method for determining values commensurate with a particular financial capacity. Those who are compelled to report covered transactions to the AMLC are also prohibited from communicating that they have made such a report to anyone.[202] Those who do communicate or publish the existence of a report or any information connected with one are criminally liable.[203]

The Supreme Court ruled in July 1998 that Administrative Order No. 308, the Adoption of a National Computerized Identification Reference System, introduced by former President Ramos in 1996, was unconstitutional. The Court found the order would "put our people's right to privacy in clear and present danger… No one will refuse to get this identity card for no one can avoid dealing with government. It is

---

192 Civil Code, Article 26.

193 *Id.* Article 32(11).

194 Christopher Lim, E-com Legal Guide, The Philippines, Baker & McKenzie, Manila, January 2001, available at <http://www.bakerinfo.com/apec/philapec_main.htm> (June 2, 2003).

195 Bank Secrecy Act, Republic Act No. 7653.

196 Secrecy of Bank Deposits Act, Republic Act No. 1405.

197 Natividad Kwan and Cornelio B. Abuda, Internet Banking – Key Legal Considerations, Baker & McKenzie, Manila, November 2000.

198 Republic Act No. 9160, § 7(c).

199 *Id.* §3(a).

200 *Id.* § 3(b).

201 *Id.*

202 *Id.* §9(c).

203 *Id.*

thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges." While stating that all laws invasive of privacy would be subject to "strict scrutiny," the Court also was careful to note that, "the right to privacy does not bar all incursions to privacy."[204] Then-president Joseph Estrada reiterated his support for the use of a national identification system in August 1998, stating that only criminals are against a national ID.[205] Justice Secretary Serafin Cuevas authorized the National Statistics Office (NSO) to proceed to use the population reference number (PRN) for the Civil Registry System-Information Technology Project (CRS-ITP) on August 14, claiming that it is not covered by the decision.[206]

However, President, Gloria Arroyo, who was newly re-elected in May 2004, has stepped up efforts to revive the National ID Scheme. Presidential spokesman, Ignacio Bunye, was quoted by the Manila Times of December 1, 2003 as asserting the necessity of the ID system for "peace and order," to facilitate transactions, and to reduce the number of IDs currently required.[207] Bunye has sought to allay privacy concerns by explaining that, "the data that we would give once we apply for this ID are the information that we usually provide when applying for an ATM card or an SSS (Social Security System) ID."[208] Proponents of the ID Scheme argue that it will reduce crime and be constitutional because it would be backed not by an Executive Order like the former ID Scheme the Supreme Court had ruled invalid, but rather by a Congressionally passed law.[209] There, however, continues to be opposition to the bill.[210]

In May 2000, the ILOVEYOU e-mail virus was traced to a hacker in the Philippines, focusing international attention on the country's cyberlaw regime.[211] Lacking specific laws on hacking and cybercrime, prosecutors were only able to gain a warrant under the Access Devices Regulation Act of 1998,[212] a law intended to punish credit card fraud that outlaws the use of unauthorized access devices to obtain goods or services broadly.[213]

On the heels of the virus attack, in May, The Electronic Commerce Act of 2000 was signed into law.[214] Section 33 of the Act mandates a minimum fine of PHP 100,000 (~USD 1,900) and a prison term of six months to three years for unlawful and unauthorized access to computer systems. Section 31 provides that only individuals with legal right of possession shall be granted access to electronic files or electronic keys. Section 32 imposes an obligation of confidentiality on persons receiving electronic data, keys, messages, or other information not to convey it to any other person.[215]

In June of 2001 the Philippine National Bureau of Investigation brought their first formal hacking and piracy charges under the Electronic Commerce Act. The charges involved two former employees of a

---

204 "Philippine Supreme Court Decision of the National ID System," *supra*.

205 Leotes Marie T. Lugo, "Erap Wants National ID System (Only Criminals Disagree with It, Says the President)," Business World, August 12, 1998, at 12.

206 Opinion Number 91; *see* "Foundation Laid for Proposed Nat'l ID," Business World, August 14, 1998, at 11.

207 Ma. Theresa Torres, "Congress Told: Pass Law for National ID," Manila Times, December 1, 2003. <http://www.manilatimes.net/national/2003/dec/01/yehey/top_stories/20031201top7.html>.

208 *Id.*

209, "Gov't to Push for nNtional I.D. System-Palace," press release December 12, 2003, available at <http://www.freewebs.com/no2id/newid.html>.

210 Manila Times Editorial, "Scary ID System," Manila Times, December 3, 2003 <http://www.manilatimes.net/national/2003/dec/03/yehey/opinion/20031203opi1.html>.

211 Lim, *supra*.

212 Access Devices Regulation Act of 1998, Republic Act No. 8484.

213 *Id.*

214 Electronic Commerce Act of 2000, Republic Act No. 8792.

215 Kwan and Abuda, *supra.*

business school who allegedly broke into the school's computer system and stole an undisclosed amount of proprietary digital material.[216]

While restrictions on search and seizure within private homes are generally respected, searches without warrants do occur.[217] More recently, Communist organizations have complained of a "pattern of surveillance" of their activities.[218] Members of the *Bayan Muna* political party have reported that offices and a clinic catering to their members were ransacked.[219] The United Church of Christ of the Philippines has also reported the ransacking of their human rights, peace, and interfaith offices in what many consider to be acts of political intimidation.[220]

The Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication and for Other Purposes[221] contains a notwithstanding clause that supersedes all inconsistent statutes.[222] Section 1 states that all parties to a communication must give permission for a recorded wiretap or intercept and makes it illegal to knowingly possess any recording made in prohibition of this law, unless it is evidence for a trial, civil or criminal.[223] Section 2 assesses liability for any person who contributes to the actions described in § 1.[224] Section 3 provides certain exceptions to the conditions found in §§ 1-2 but adopts stringent criteria for wiretap warrants, including the identity of the wiretap target; who may execute the warrant; reasonable grounds that a crime has been, is or will be committed; and, a reasonable belief that the evidence obtained via the wiretap will aid in a conviction or prevention of a crime.[225] Further, predicate offences – or offences for which a court may authorize a wiretap – are limited to several particularly onerous severity.[226] Section 4 states that any communication obtained in violation of this Act shall not be admissible as evidence in any court.

Despite the legal prohibitions on wiretapping, illegal wiretaps appear to be a continuing problem. In August 1997, the Philippine Congress investigated the admissions of telephone company officials who said that they had conducted illegal wiretaps. The Philippine National Police also conducted an internal investigation of electioneering and illegal wiretaps in May 1998.[227] Reports of illegal wiretaps continued into April of 1999, when the National Bureau of Investigation and the Ombudsman investigated reports that police had tapped up to 3,000 telephone lines including those of top government officials, politicians, religious leaders, businessmen and journalists.[228] 2001 saw the investigation of former members of the defunct Presidential Anti-Organized Crime Task Force, again for illegal wiretaps.[229]

---

216 "Philippines' NBI Clamps Down on 'Cyberthieves'," Metropolitan Computer Times, (June 13, 2001).

218 US Department of State Country Report on Human Rights Practices 2002, Philippines, March 2003.
U.S. Department of State, Bureau of Democracy, Human Rights, and Labor, Philippines: Country Report on Human Rights Practices for 2003, available at <http://www.state.gov/g/drl/rls/hrrpt/2002/18261.htm>.

219 *Id.*

220 *Id.*; *see also* Jowel F. Canuday, "UCCP's Human Rights, Peace, Interfaith Offices Ransacked," MindaNews, January 6, 2003, available at <http://www.mindanews.com/2003/01/2nd/arn07uccp.html>.

221 Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication and for Other Purposes, Republic Act No. 4200, June 19, 1965.

222 *Id.* § 5.

223 *Id.* § 1.

224 Penalties include imprisonment, disqualification from public office or deportation, in the case of a foreigners.

225 Republic Act No. 4200, § 3.

226 Offences falling into this category include: crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security.

227 Lim, *supra*.

228 *Id.*

229 Cecille S Visto, "Ombudsman Starts Probe of Surveillance Activities," Business World, August 24, 2001, at 12.

Section 5 of the Rape Victim Assistance and Protection Act of 1998, stipulates that "any stage of the investigation, prosecution and trial of a complaint for rape, the police officer, the prosecutor, the court and its officers, as well as the parties to the complaint shall recognize the right to privacy of the offended party and the accused." It further states that a police officer, prosecutor or court may order a closed-door investigation, prosecution or trial and that the name and personal circumstances of the offended party and/or the accused, or any other information tending to establish their identities, and such circumstances or information on the complaint shall not be disclosed to the public.[230] Section 3 provides for the establishment of a rape crisis center in every province and city "for the purpose of: ensuring the privacy and safety of rape victims."[231]

However, recently, there have been several instances in which the Filipino popular media has identified victims of sexual assaults. For instance, in relation to the conviction of a Congressman, the Manila Times reports that the 11-yr old victim was identified even though the victim was supposedly under witness protection.[232] It was also reported that a victim of a highly publicized incestuous rape case, was identified in the media,[233] and that in 2003 the identity of an adult rape victim was disclosed on government-backed television.[234]

Section 8 of the Proposed Rule on Juveniles in Conflict (the Rule) with the Law stipulates that "the right of the juvenile to privacy shall be protected at all times. All measures necessary to promote this right shall be taken, including the exclusion of the media."[235] Section 9 of the Rule, dealing with the fingerprinting and photographing of a juvenile, states "while under investigation, no juvenile in conflict with law shall be fingerprinted or photographed in a humiliating and degrading manner," and stipulates procedural guidelines such as separate storage of fingerprint files from adult files; restricted access by prior authority of the Family Court; and automatic destruction if no charges are laid or when the juvenile reaches the age of majority (21).[236] Section 26(k) of the Rule confers a duty on the Family Court to respect the privacy of minors during all stages of the proceedings.[237]

The Local Government Code of the Philippines[238] provides that all *barangay*[239] "proceedings for settlement shall be public and informal provided that the . . . chairman . . . may upon request of a party, exclude the public from the proceedings in the interest of privacy, decency, or public morals."[240]

The drive to fight corruption has also resulted in several measures that have privacy implications. Media reports indicate that in 2003 there was a government-sponsored raid of nightclubs under the pretext of a "morality checks" to root out corrupt officials,[241] and there has been a political party sponsored "Report-

---

230 Rape Victim Assistance and Protection Act of 1998, No. 8505, § 5.

231 *Id.* § 3(d).

232 Eric F. Mallonga, "Child Friendly Media," Manila Times. September 15, 2003 <http://www.manilatimes.net/national/2003/sept/15/opinion/20030915opi3.html>.

233 *Id.*

234 Laarni Ilagan, "Ifuago OFW in OWWA's Custody." Manila Times. December 4, 2003 <http://www.manilatimes.net/national/2003/dec/04/yehey/prov/20031204pro8.html>.

235 Proposed Rule on Juveniles in Conflict With the Law A. M. NO. 02-1-18-SC (April 15, 2002), available at <http://www.chanrobles.com/amno02118sc.htm>, § 8.

236 *Id.* § 9.

237 *Id.* § 26.

238 Local Government Code of the Philippines.

239 As the basic political unit, the *barangay* serves as the primary planning and implementing unit of government policies, plans, programs, projects, and activities in the community, and as a forum wherein the collective views of the people may be expressed, crystallized and considered, and where disputes may be amicably settled.

240 Local Government Code of the Philippines, § 414.

241 Ricardo V. Puno Jr., "Viewpoint: Onion Skins," Manila Times, September 22, 2003 <http://www.manilatimes.net/national/2003/sept/22/opinion/20030922opi2.html>.

a-Mistress" program also aimed at corrupt officials.[242] Under the Report-a-Mistress Program, sponsored by the party-list group, Citizen's Battle Against Corruption (CIBAC), members of the public are encouraged to call in and report government officials who have mistresses, as this is seen as an indication of corruption.[243]

Section 14 of Alien Social Integration Act of 1995[244] provides that "information submitted by an alien applicant pursuant to this Act, shall be used only for the purpose of determining the veracity of the factual statements by the applicant or for enforcing the penalties prescribed by this Act."[245]

The use of biometric technologies has been rising in the Philippines. Since March of 1996, dozens of companies and government agencies have adopted fingerscan technologies in applications ranging from time management and payroll systems to security access control. Many companies use the technology primarily to reduce fraudulent time card punching.[246] Banks use the technology to reduce fraudulent transactions and to promote security. Additionally, GTE and IriScan, Inc. introduced iris-scan technology in 1998 to ensure the security of online transactions. Other uses of biometric technology in the Philippines include the dispensation of health care and social services; privacy systems for database and records protection; travel security systems with passport, ticket, and baggage verification; business, residence, and vehicle security with access and operator authentication; processing and circulation control in the corrections or prison environment; and portable systems for on-scene recognition of individuals for use in law enforcement.[247] National ID proposals also typically include fingerprints as part of the information available on the ID card.[248]

In July of 2001 the Philippines' Civil Service Commission released a resolution requiring all government officials and employees to refrain from sending indecent messages. The resolution took effect on August 5, 2001 and bans public officials from sending sexist jokes, pornographic pictures and lewd letters or mails through electronic means including mobile phones, fax machines and e-mails. Individuals who feel sexually harassed may report cases directly to the Civil Service Commission. The resolution is a follow-up to a proposal by the Commission on Elections and the National Telecommunications Commission to monitor, track and prosecute senders of "politically motivated text messages."[249]

The Code of Conduct and Ethical Standards for Public Officials and Employees[250] mandates the disclosure of public transactions and guarantees access to official information, records or documents. Agencies must act on a request within 15 working days from receipt of the request. Complaints against public officials and employees who fail to act on request can be filed with the Civil Service Commission or the Office of the Ombudsman.

Terrorism has continued to be a menace in the Philippines in 2003 and 2004. There were bomb attacks by Islamist terrorists in March and April 2003.[251] Part of the government's anti-terrorism measures has been the 2003 installation of an Airport Identification Computer System at the Ninoy Aquino

---

[242] Niel Villegas Mugas, "Report-a-Mistress Program Swamped." Manila Times. October 1, 2003 <http://www.manilatimes.net/national/2003/oct/01/top_stories/20031001top6.html>.

[243] *Id.*

[244] Alien Social Integration Act of 1995, No. 7919.

[245] *Id.* § 14.

[246] The Government Service Insurance System, National Computer Center, Philippine Tourism Authority, Department of Social Welfare and Development, and the Light Railway Transit Authority use the fingerscan as a means to ensure that employees are actually at the worksite.

[247] "Biometrics System Usage Rises," Business World, February 17, 1998, at 14.

[248] *See, e.g.*, "Pactech: Philippines Prepares National ID Card," Pacific Business News, May 29, 2002, available at <http://pacific.bizjournals.com/pacific/stories/2002/05/27/daily19.html>.

[249] "Philippine Agency Acts on 'E-Harrassment' In Government Workplaces," Metropolitan Computer Times, July 23, 2001.

[250] Republic Act No. 6713.

[251] BBC News Online, "Lethal Blast Hits Philippines." April 2, 2003 <http://news.bbc.co.uk/1/hi/world/asia-pacific/2910073.stm>.

International Airport.[252] The system called PISCES (Personal Identification Security Comparison System) is designed to screen for potential terrorists attempting to travel to the United States while they are still in their country of origin's airport. PISCES collates and processes facial images, fingerprints, and biographical information and is purportedly linked to US Government Databases, allowing for exchange of passenger information.[253]

Republic of Poland

The Polish Constitution recognizes 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 honor 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."[254]

The Law on the Protection of Personal Data Protection (LPPDP) was approved in October 1997 and took effect in April 1998.[255] 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 fulfillment of at least one of the conditions required by the LPPDP 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 or sexual preferences, convictions, and other decisions issued in court or administrative proceedings. Everyone has the right to control the processing of his *or* her personal data contained in the filing systems, and has the right to be informed whether such databases exist and who administers them; queries should be answered within thirty 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.[256] Personal information cannot generally be transferred outside of the European Economic Area unless the third country has "comparable" protections. The law sets out administrative and criminal sanctions for violations. A 1998 regulation from the Minister of Internal Affairs and Administration sets out standards for the security of information systems that contain personal information,[257] which was updated by the regulation of 2004.[258] In August 2001, the Act was

---

[252] Jonathan M. Hicap, "NAIA Survillance System Linked to FBI Computers." Manila Times. September 25, 2003 <http://www.manilatimes.net/national/2003/sept/25/top_stories/20030925top11.html>.

[253] Wayne Madsen, "The Business of the Watchers: Privacy Protections Recede as the Purveyors of Digital Security Technologies Capitalize on September 11," Multinational Monitor, Vol 23, No. 3, March 2002, available at <http://multinationalmonitor.org/mm2002/02march/march02corp3.html>.

[254] The Constitutional Act of 1997.

[255] Law on the Protection of Personal Data, Dz.U. nr 133, poz. 833, October 29, 1997.

[256] "The Info Boom's Murky Side," Warsaw Voice, November 9, 1997.

[257] The Regulation of June 3, 1998 by the Minister of Internal Affairs and Administration as regards Establishing Basic, Technical and Organizational Conditions which Should Be Fulfilled by Devices and Information Systems Used for the Personal Data Processing, Journal of Laws, June 30, 1998, No. 80, item 521.

[258] Regulation of April 29, 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.

amended in order to bring it into full compliance with the EU Data Protection Directive.[259] 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. On May 1, 2004, the day of Poland's accession to the European Union, the Amendments to the Act on the Protection of Personal Data entered into force. [260] These amendments brought into effect the regulation regarding the prior checking of sensitive data, the transfer of personal data to a third country, and specified some of the controller's duties.

The Inspector General enforces the LPPDP.[261] Ewa Kulesza was appointed as the first Inspector General for the Protection of Personal Data by the Polish Parliament in April 1998. The Inspector General has six central duties: to supervise compliance of data processing 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; and 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 organizations and institutions involved in personal data protection. The Inspector General for Personal Data Protection is an independent authority and performs her duties assisted by the Bureau of the Inspector General (Bureau). The functioning of the Bureau is determined by regulation of the President of the Republic of Poland.[262] The Bureau secures performing the tasks being due to the Inspector General's power conferred upon by the Act and other provisions in force.

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 the security measures. The specimen of a notification of the data filing system to registration by the Inspector General are constituted in the Appendix to the Regulation of April 29, 2004. An Inspector has the right to access data, check data transfer and security systems, and determine whether the information gathered is appropriate for the purpose that it is supposed to serve.[263] The office monitors the activities of all central government, local government and private institutions, individuals and corporations. As of June 2004, the Bureau had 117 staff members.[264] The Bureau is structured into several departments.[265]

In 2003, the Bureau answered 1,482 enquiries concerning the binding provisions on data protection and the interpretation of the Act, considered 753 complaints, gave 374 legal opinions on bills, conducted 184 inspections at data controllers' facilities in order to assess the compliance of the data processing with the provisions on the personal data protection, registered 3,461 data filing systems, issued 522 decisions and

---

259 Act of August 25, 2001 amending the Act on Personal Data Protection, Journal of Laws, No. 100, item 1087.

260 *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 <http://www.giodo.gov.pl/272/j/en/>.

261 Homepage <http://www.giodo.gov.pl>.

262 The Regulation of May 29, 1998 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 1998, No. 73, item 464 with later amendments, available at <http://www.giodo.gov.pl/272/j/en/>.

263 "A One-Woman Orchestra," Warsaw Voice, June 21, 1998.

264 As of June 2003, the Bureau had 112 staff members, up from 102 in June 2002.

265 The Legal Department prepares answers to the legal questions being lodged; analyzes legal acts with regard to their compliance with the LPPDP; prepares legal opinions for the Inspector General, the Director of the Bureau and the other departments. The Inspection Department performs inspection activities in order to assess the compliance of processors with the appropriate provisions of the LPPDP; works on projects to the decisions issued as a result of inspections; demands institution of disciplinary proceedings against persons found to be guilty of the negligence during inspections, and prepares notifications of committed offences addressed to law enforcement. The Registration Department keeps the register of personal data filing systems, accepts applications for data filing system registration, drafts decisions on refusal of data filing system registration and other letters connected with registry procedure, and issues certificates on personal data filing systems. The Computer Department carries out inspection activities together with the employees from the Inspection Department, assesses the requests for registration of data filing system with regards to compliance with technical and organizational requirements for processing systems, and secures the access to the Bureau's computer system. The Complaints Department considers complaints and motions concerning the compliance with the provisions on personal data protection, drafts decisions issued in cases examined by the Complaints Department, drafts notifications on committed offences addressed to law enforcement bodies, and requests inspections on the basis of complaints received. Letter from Mr. Jaroslaw Trelka, *supra*.

addressed 74 notifications of committed offences provided for by the provisions on personal data protection.[266] From the beginning of the Bureau's operation in 1998 through the end of May 2004, 80,117 notifications for registration of data filing systems have been received and 62,830 data filing systems have been registered.[267]

In general, the issues which are most often raised in the complaints include the collection of excessive personal data (in particular by banks, insurance companies, employers, telecommunications operators, social assistance centers, administration of justice and law enforcement bodies); disclosure of data from medical documents, records of criminal proceedings, or various records collected by public bodies (*e.g.*, motor vehicle or census records); public disclosure of debtors' data and their transfer to professional debt collectors; the legal basis of data processing for the purpose of direct marketing or political campaigns; appropriate means of ensuring the security of personal data (*e.g.*, data contained in employees' files in case of bankruptcy); and the legal basis and scope of processing on the Internet.[268] The Bureau has, from its inception, conducted an educational campaign in an attempt to educate citizens, government officials and the private sector on the provisions of the Act. Some of the more significant decisions issued by the Inspector General in 2001 were to prohibit: telecom and insurance companies from making photocopies of identity cards at the time of entering into a contract to provide their services; banks from using their former clients' personal data for marketing purposes; and employers from processing data on employees' sexual life during recruitment. The Inspector has also opened an investigation into a brokerage house that accidentally disclosed clients' personal data on the Internet.[269] In 2003, the Inspector General ordered Polish telecommunication operators to limit the scope of data collected by them to the extent allowed by the telecommunication law.[270]

In November 2001, the Inspector General, in conjunction with the Council of Europe, hosted a major conference on data protection[271] and in September 2004, the Inspector General will host the 26th International Conference on Privacy and Personal Data Protection in Wroclaw under the theme "The Right to Privacy – the Right to Dignity." The annual meetings involve national authorities of personal data protection, the Council of Europe, the European Commission, scientists, economic entities, public institutions and human rights organizations.[272]

The Bureau also maintains close relations 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 closer cooperation and assistance.[273] The Commissioners have been meeting twice a year. The fourth meeting took place at the end of April 2003 in Budapest.[274] The sixth Meeting of the Central and Eastern European Data Protection Commissioners was held in Riga, Latvia in May 2004.

---

266 Letter from Ms. Alina Szymczak, Director of the Bureau of the Inspector General for Personal Data Protection, Poland, to Samantha Liskow, Law Clerk, EPIC, June 11, 2004 (on file with EPIC).

267 In 2002, the Bureau received 1324 inquiries about the Act, 830 complaints and 351 legislative proposals for comment. The Bureau conducted 233 inspections, and issued 507 decisions and 61 notifications of breaches. Statistics Concerning the Activity of the Bureau of the Inspector General for the Protection of Personal Data, available at <http://www.giodo.gov.pl/241/j/en/>.

268 Letter from Mr. Trelka, *supra*.

269 E-mail from Igor Kowalewski, International Relations Officer, Bureau of the Inspector General for Personal Data Protection, to Sarah Andrews, Research Director, EPIC, June 20, 2002 (on file with EPIC).

270 Letter from Ms. Alina Szymczak, Director of the Bureau of the Inspector General for Personal Data Protection, Poland, to Samantha Liskow, Clerk, EPIC, June 11, 2004 (on file with EPIC).

271 European Conference on Data Protection, "Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future," November 19-20, 2001, Warsaw (Poland).

272 <http://www.giodo.gov.pl/259/id_art/175/j/en/>.

273 <http://www.giodo.gov.pl/234/j/en/>.

274 Agenda and meeting notes available at Central and Eastern Europe Data Protection Authorities Web Site <http://www.ceecprivacy.org/main.php?s=1>.

There are sectoral laws in place to deal with the processing of medical and financial data. The 1996 Act on the Profession of a Doctor imposes a duty of confidentiality in relation to patient information on medical professionals, subject to certain exceptions. The Constitutional Tribunal ruled in March 1998 that requiring doctors to identify, on sick leave certificates, the disease of the patient violated the patients' right to privacy. The Banking Act 1997 imposes a requirement of secrecy on banks in relation to an individual's banking activities and identity, and limits the exchange and disclosure of personal data among banks and third parties except for the purpose of assessing credit risks or investigation fraud. However, broad exemptions are granted to state entities. 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.[275]

Chapter 33 of the 1997 Penal Code, "Offences against the Protection of Information," deals, among other things, with computer related offences. Unauthorized access to computer systems, computer eavesdropping, interference with data, and computer sabotage are crimes punishable by up to eight years imprisonment. The code also prohibits telecommunications fraud, the handling of stolen software, computer espionage, and causing harm from interference with automatic data processing.[276]

The Government of Poland carries out a large number of wiretaps with limited oversight. Under the Criminal Code, the use of wiretaps shall be authorized by the court, after appropriate motion by the 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, specified, in the way of the regulationm the manner of the control and technical requirements of wiretaps and how to carry out the tap.[277] The law specifies for which cases the interception of communications may be authorized. In exceptional cases, the police may initiate a wiretap at the same times as they apply for authorization. Furthermore, under the Police Code electronic surveillance may be used for the prevention of crime as well as for investigative purposes. The government does not openly release statistics on the number of wiretaps applied for and authorized, tending to view this as a state secret. In 1997, the reports of numbers of wiretaps varied from 2000 to 4000.[278] There are unsubstantiated reports that these numbers increased further in 1999 and 2000.[279] The United States Department of State, in its annual Country Reports on Human Rights Practices, has been consistently critical of high number of wiretaps authorized in Poland. In its most recent report, despite the fact that no credible estimate existed of the number of police wiretaps, the US government agency wrote that "[t]here was no independent judicial review of surveillance activities, nor was there any control over how the information derived from investigations is used. A number of agencies have access to wiretap information, and the Police Code allows electronic surveillance to be used for the prevention of crime as well as for investigations."[280] In its 1999 report, the United Nations Human Rights Committee said it was "concerned that the Prosecutor (without judicial consent) may permit telephone tapping and that there is no independent monitoring of the use of the entire system of tapping telephones." The Committee recommended that Poland "review these matters so as to ensure compatibility with article 17 [of the International Covenant on Civil and Political Rights],

---

[275] "Constitutional Tribunal Allows Treasury to Screen Bank Accounts," Polish News Bulletin, April 12, 2000.

[276] Andrzej Adamski, "Computer Crime in Poland: Three Year's Experience in Enforcing the Law," presented to the Council of Europe Conference on Cybercrime, Budapest, November 2001, available at <http://www.coe.int/T/E/Legal%5FAffairs/Legal%5Fco%2Doperation/Combating%5Feconomic%5Fcrime/Cybercrime/International_conference/3National_reports.asp#TopOfPage>.

[277] The Regulation of June 24, 2003 by the Ministry of Justice.

[278] 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, available at <http://www.hfhrpol.waw.pl/en/index.html>.

[279] United States Department of State, Country Reports on Human Rights Practices 2001, March 4, 2002, available at <http://www.state.gov/g/drl/rls/hrrpt/2001/eur/8321.htm>.

[280] United States Department of State, Country Reports on Human Rights Practices 2003, February 25, 2004, available at <http://www.state.gov/g/drl/rls/hrrpt/2003/27858.htm>.

introduce a system of independent monitoring, and include in its next report a full description of the system by then in operation."[281]

Various proposals to expand law enforcement surveillance capabilities over the last few years have been put forward. In July 2001, amendments to the Police Act gave the 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 the amendments "were dubious in terms of the right to privacy."[282] The Ministry of Internal Affairs and Administration announced in January 2000 that it was setting up a new unit of 1,500 officers based on the United States Federal Bureau of Investigation to combat organized crime. The new unit will have the power to conduct electronic surveillance and create extensive databases.[283] Efforts to require all service operators (including mobile phone and Internet access providers) to install equipment, to facilitate this increased monitoring, are also going forward. There are serious concerns within the Bureau about the Polish Executive Regulation of February 22, 2003 adopted pursuant to the Telecommunications Law. The provisions of this regulation impose upon telecommunications networks operators the obligation to ensure the public security bodies the access to information sent through telecommunications networks for the purpose of national defense, state security and public order.[284]

In February 2003, legislation was enacted exempting officials from the law of "lustration" if they cooperated with intelligence and counterintelligence agencies. The law of lustration is designed to expose collaborators with the Communist-era secret police by requiring sworn affidavits that may be reviewed by a court. The Constitutional Tribunal in June 2003 found the legislation to be procedurally unconstitutional, but a new, similar law was enacted in October.[285]

The Constitutional Tribunal also found unconstitutional, in April 2004, an act regarding the Internal Security and Intelligence Agencies that allowed 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.[286]

Controversy still surrounds the expanded national identification (ID) system. The Electronic Census System (PESEL) number, which has been issued 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 computerized. The Government began issuing the new ID cards in January 2001.

In June 2004, the Polish Ministry of Infrastructure introduced a requirement, in implementing the EU e-communication directives,[287] that buyers of pre-paid "GSM" cards for cell phones be identified. The bill was being examined in June by parliament's infrastructure committee.[288]

The Parliament approved the Act on Access to Public Information in September 2001. It went into effect in January 2002. The Act creates a presumption of access to information held by all public bodies,

---

[281] United Nations, Report of the Human Rights Committee, A/54/40, October 21, 1999.

[282] 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://www.ihf-hr.org/reports/AR2002/country%20links/Poland.htm>.

[283] "New Police Unit to Combat Organised Crime," Polish News Bulletin, January 4, 2000.

[284] The Regulation of January 24, 2003 by the Minister of Infrastructure – Journal of Laws of 2003, No. 19, item 166. (The concern is mentioned in the Mr. Trelka's letter, *supra*.)

[285] United States Department of State, Country Reports on Human Rights Practices 2003, *supra*.

[286] "Court Says Parts of Secret Services Law Unconstitutional," BBC Worldwide Monitoring, April 20, 2004 (source Polish Radio 1, Warsaw, in Polish, April 20, 2004).

[287] Directive on Privacy and Electronic Communications (2002/58/EC).

[288] *See* "Edri-Gram," Number 2.11, June 2, 2004. <http://www.edri.org/cgi-bin/index?id=000100000151>.

private bodies that exercise public tasks, trade unions and political parties. The bodies 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 to a court. In July 2003, the Polish Access to Public Data Bill came into force, requiring thousands of public institutions, such as local government, political parties and schools, to put public information on web sites.[289] The Public Data Bulletin, a system of Internet sites, serves to collect these informational sites in one place.[290]

Poland enacted the Classified Information Protection Act in January 1999 as a condition to entering North Atlantic Treaty Organization (NATO).[291] The act covers classified information or information collected by government agencies that disclosure "might damage interests of the state, public interests, or lawfully protected interests of citizens or of an organization." 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 (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.[292] 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. Under the Data Protection Act, individuals have the right to access and correct records that contain personal information about them from both public and private bodies. However, in November 2003 the government asked Parliament to amend the law on the protection of secret information, [] which amendment introduces 64 forms of information to be declared top secret and classified. The amendment also allows officers to mark any information as classified that might be "inconvenient" for them.[293]

Poland 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. In May 2002 it ratified the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).[294] In November 2001, it signed, but has not ratified, the CoE Cybercrime Convention (ETS No. 185).[295] Poland 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.

Republic of Portugal

The Portuguese Constitution has extensive provisions on protecting privacy, secrecy of communications and data protection.[296] Article 26 states, "(1) Everyone's right to his or her personal identity, civil capacity, citizenship, good name and reputation, image, the right to speak out, and the right to the protection of the intimacy of his or her private and family life is recognized. (2) The law establishes effective safeguards against the abusive use, or any use that is contrary to human dignity, of information concerning persons and families. (3) A person may be deprived of citizenship or subjected to restrictions on his or her civil capacity only in cases and under conditions laid down by law, and never on political grounds." Article 34 states "(1) The individual's home and the privacy of his correspondence and other means of private communication are inviolable. (2) A citizen's home may not be entered against his will,

---

289 Journal of Laws No 112, item 1198, available at <http://home.online.no/~wkeim/files/poland-foia.htm>.

290 *See* <http://www.bip.gov.pl/> (in Polish).

291 The Classified Information Protection Act of 22 January 1999.

292 *See* "Freedom of Information and Access to Government Records Around the World," *supra*.

293 International Helsinki Federation for Human Rights, Human Rights in the OSCE Region: The Balkans, the Caucasus, Europe, Central Asia and North America, Report 2004 (events 2003), available at <http://www.ihf-hr.org/documents/doc_summary.php?sec_id=3&d_id=3860>.

294 Signed April 21, 1999; ratified May 23, 2002; entry into force September 1, 2002.

295 Signed November 23, 2001.

296 Constitution of the Portuguese Republic, available at <http://www.parlamento.pt/leis/constituicao_ingles/IND_CRP_ING.htm>.

except by order of the competent judicial authority and in the cases and according to the forms laid down by law. (3) No one may enter the home of any person at night without his or her consent. (4) Any interference by public authority with correspondence or telecommunications, apart from the cases laid down by law in connection with criminal procedure, are prohibited."

In 1997, Article 35 of the Constitution was amended to give citizens a right to data protection. The new Article 35 states, "1. All citizens have the right of access to any computerized data relating to them and the right to be informed of the use for which the data is intended, under the law; they are entitled to require that the contents of the files and records be corrected and brought up to date. 2. The law shall determine what is personal data as well as the conditions applicable to automatic processing, connection, transmission and use thereof, and shall guarantee its protection by means of an independent administrative body. 3. Computerized storage shall not be used for information concerning a person's ideological or political convictions, party or trade union affiliations, religious beliefs, private life or ethnic origin. Such storage is only allowed when there is express consent from the data subject, authorization is provided for under the law with guarantees of non-discrimination, or as long as it is not possible to identify individuals in the case of data processing done for statistical purposes. 4. Access to personal data of third parties is prohibited, aside from exceptional cases as prescribed by law. 5. Citizens shall not be given an all-purpose national identity number. 6. Everyone shall be guaranteed free access to public information networks and the law shall define the regulations applicable to the transnational data flows and the adequate norms of protection for personal data and for data that should be safeguarded in the national interest. 7. Personal data kept on manual files shall benefit from protection identical to that provided for in the above articles, in accordance with the law."

The 1998 Act on the Protection of Personal Data adopts the European Union (EU) Data Protection Directive requirements into Portuguese law.[297] 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.[298]

The Act is enforced by the National Data Protection Commission (*Comissão Nacional de Protecção de Dados*, or CNPD).[299] The Commission is an independent agency that is directly responsible before the Parliament. Its functions are to register existing databases with private data, authorize and control such databases, issue directives, and oversee the Schengen Information System (SIS). The number of investigations conducted has risen steadily from 5 in 1994 to 42 in 1997, 78 in 1998, 151 in 2000, 223 in 2001 and 211 in 2002. 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 and two in 2002. The Commission applied 22 fines in 2001, totaling EUR 52,000 and 119 in 2002 in a total of EUR 435,000. The Commission authorized 483 databases in 2000, for a total of 3,161 approvals between 1994 and 2000. The Commission also handled 133 inspections in 2000, mostly relating to financial services.[300] 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, and approved transborder data flows to the United States when the transferee company promised to protect the personal data collected pursuant to European data protection legal standards. In June 1997, the Supreme Administrative Tribunal upheld the Commission's decision in a case against a shoe company

[297] Act No. 67/98 of October 26, 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/Leis/lei_6798en.htm>.
[298] Law No. 10/91 - *Lei da Protecção de Dados Pessoais face à Informática*, amended by Law No. 28/94 of August 29, 1994, *Aprova medidas de reforço da protecção de dados pessoais*.
[299] Homepage <http://www.cnpd.pt/>.
[300] *Comissão Nacional para a Protecção de Dados*, 2000 Report, available at <http://www.cnpd.pt/relat/relatorio.htm>.

that used smart cards to control employees' bathroom visits. In 2003, the CNPD published "Guidelines on Privacy in the Workplace."[301] These guidelines establish that information and contents of phone calls, e-mails and Internet access for private use of a worker is protected as private data and must be respected as such by the employer. In 2004 the CNPD published guidelines on the usage of RFID[302], biometrics[303] and surveillance systems.[304] 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 Penal Code has provisions against unlawful surveillance and interference with privacy.[305] Evidence obtained by any violation of privacy, the home, correspondence or telecommunications without the consent of the interested party is null and void.[306] 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.[307] The Portuguese government ordered cellular telephone companies to assist with surveillance in October 1996.[308] Law No. 69/98[309] implements the EU Telecommunications Privacy Directive (1997/66/EC).

There are also specific laws on the SIS,[310] computer crime,[311] and counseling centers.[312]

Law No. 65/93 of August 26, 1993 (*Regula o Acesso aos Documentos da Administrção*) (Law on the Regulation of, and Access to, Administrative Documents) provides for access to government records in any form by any person.[313] Documents can be withheld for "internal or external security," secrecy of justice, and personal privacy. 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 issued 177 opinions in 1998, 231 in 1999, 333 in 2000 and 260 in 2001.

Portugal 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 (ETS No. 108) (Convention No. 108).[314] In November 2001, it signed the CoE Convention on Cybercrime (ETS No. 185) but has not ratified it.[315] It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[316] 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.

---

[301] *Comissão Nacional para a Protecção de Dados*, "*Princípios sobre a Privacidade no Local de Trabalho,"* October 29, 2002 <http://www.cnpd.pt/bin/princitrabalho.htm>.
[302] *Comissão Nacional para a Protecção de Dados*, "*Identificação por radiofrequência*," January 13, 2004 <http://www.cnpd.pt/actos/del/2004/del%20009-04.htm>.
[303] *Comissão Nacional para a Protecção de Dados*, Principles for the use of biometric data in controlling access and monitoring hours worked, February 26, 2004 <http://www.cnpd.pt/actos/del/2004/Guidelinesbiometric.htm>.
[304] <*Comissão Nacional para a Protecção de Dados*, "*Princípios sobre o tratamento de videovigilância*," April 19, 2004 <http://www.cnpd.pt/actos/del/2004/del%20061-04.htm>.
[305] Chapter VI, Penal Code, Section 179-183.
[306] Article 126 of the Code of Penal Procedure, Paragraph 3. *see* United Nations, Committee Against Torture Consideration of Reports Submitted by States Parties Under Article 19 of the Convention, Addendum, Portugal, June 10, 1997.available at <http://www1.umn.edu/humanrts/cat/catPortugal94.htm>.
[307] "Bug Found in Portuguese State Prosecutor's Office," The Reuters European Business Report, April 27, 1994.
[308] "Portugal to Tap Mobile Phones in Drugs War," Reuters World Service, October 9, 1996.
[309] Law No. 69/98 available at <http://www.cnpd.pt/Leis/lei_6998.htm>.
[310] Law No. 2/94 (*Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen*), available at<http://www.cnpd.pt/Leis/lei_294.htm>.
[311] Law No. 109/91 (*Sobre a criminalidade informática*) (Law on Computer Crime)–available at <http://www.cnpd.pt/Leis/lei_10991.htm>.
[312] This law creates a duty of confidentiality duty for counseling centers. Law No. 3/84 (*Educação sexual e planeamento familiar*), March 24, 1984, *Diário da República.*
[313] Law No. 65/93, including alterations made by Laws No. 8/95 and 94/99, available at <http://www.cada.pt/paginas/lada.html>.
[314] Signed May 14, 1981; ratified September 2, 1993; entered into force January 1, 1994.
[315] Signed November 23, 2001.
[316] Signed September 22, 1976; ratified November 9, 1978; entered into force November 9, 1978.

Romania

The Romanian Constitution[317] adopted in 1991 recognizes under Title II (Fundamental Rights, Freedoms and Duties) the rights of privacy, inviolability of domicile, freedom of conscience and expression. Article 26 states, "(1) Public authorities shall respect and protect intimacy, 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 of the Constitution 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."

In November 2001, the Parliament enacted Law No. 676/2001 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector[318] and Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data.[319] These laws follow very closely the European Union Telecommunications Privacy (1997/66/EC) and Data Protection (1995/46/EC) Directives respectively.

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. The law applies to the operators of public telecommunications networks and the providers of publicly available telecommunications services who, in the context of their activities, carry out processing of personal data. The regulatory authority established by Law No. 676/2001 was originally the Ministry of Communication and Information Technology, but it was changed by the Government Emergency Ordinance No. 79/2002 for the National Regulatory Authority for Communication (NRAC).[320] No specific department was created to take care of the application of Law 676/2001.

Law No. 677/2001 applies to the processing of personal data, made, totally or partially, through automatic means, as well as to the processing through means other than automatic, which are part of, or destined to, an evidence system.

The supervisory authority for Law No. 677/2001 is the Ombudsman (also called "The People's Advocate").[321] The Organizational and Functional Regulations of the Ombudsman were changed in order to provide the creation of a special Private Information Protection Office (PIPO), concerned with the protection of individuals in relation to private data processing. The Ombudsman adopted several orders

317 <http://www.cdep.ro/pls/dic/act_show?ida=1&idl=2&tit=2#t2c2s0a26>.
318 <http://www.riti-internews.ro/lg676.htm>.
319 <http://www.avp.ro/leg677en.html>.
320 <http://www.anrc.ro/en/index.htm>.
321 <http://www.avp.ro>.

in 2002 in order to apply Law No. 677/2001.[322] In 2003 the Ombudsman proposed a normative act establishing a notification fee; to that effect, Law No. 476/2003 was adopted.[323]

The specialized structure established for the implementation of the data protection legislation is provided with 19 positions. The complaints are solved according to Article 25 Law No. 677/2001. Pursuant to these provisions, the complaint cannot be submitted to the supervisory authority earlier than 15 days from the time a complaint is submitted that deals with the same problem to the data controller. In order to solve the complaint, the supervisory authority may listen to both the respective person and the data controller or, if applicable, the person who represents the interests of the respective persons. If the complaint is justified, the supervisory authority is empowered to order the temporary interruption or ceasing of the data processing, the partial or total erasure of the processed data, and may also notify the criminal bodies or bring a lawsuit.[324]

In 2003, the Ombudsman issued Order No. 6 of January 29, 2003 that establishes standard contractual clauses for the transfer of personal data to third countries that do not provide an adequate level of protection.[325]

According to the most recent Ombudsman Report,[326] 266 operators registered with the operator's registry in 2003. They filed 308 notices, of which 29 concerned transfers of personal data abroad. The report states: "We find that there is a small number of operators registered; it's mainly private law operators that do not notify the fact that they process personal data, although the law has been in force since March 2002." The small number of operators registered is due to the fact that many data controllers have not yet declared that they process personal data, despite the publicity measures taken by the Ombudsman. Data protection legislation is very recent in Romania, and the Ombudsman lacks the resources necessary to make a proper promotion of the legal requirements, which explains why assessing the Ombudsman's competence as a data protection supervisory authority is still faced with several hurdles.[327] As of end June 2004, there were 1,182 registered data controllers, either as natural persons or legal persons, including central and local public authorities and institutions, as well as private enterprises.[328]

In 2003 the Ombudsman only ordered four prior controls and eight investigations, performed both at public and private operators.[329] In 2004, three investigations and three preliminary controls were carried out. In 2004, the supervisory authority received four claims, most of them involving the sending of unsolicited commercial messages (spam) by direct marketers.[330]

---

[322] Ombudsman Order No. 52 (April 18, 2002) for the approval of the minimum security measures for data processing laying at the basis of the operators adopting technical and organizational measures to guarantee a proper legal security level of data processing, Official Monitor, June 5, 2002; Ombudsman Order No. 53 (April 18, 2002) for the approval of standardized notification forms, Official Monitor, June 5, 2002; Ombudsman Order No. 54 (April 18, 2002) for the determination of situations requiring the notification of data processing that falls under Law No. 677/2001, Official Monitor, June 5, 2002; Ombudsman Order No. 75 (June 4, 2002) to establish specific measures and procedures to provide a satisfactory level of protection for data subjects, Official Monitor, June 26, 2002.

[323] Official Monitor, No. 814 of November 18, 2003.

[324] E-mail from Ioan Muraru, People's Advocate to Cédric Laurant, Policy Counsel, Electronic Privacy Information Center (EPIC) (July 4, 2004) (on file with EPIC).

[325] Official Monitor No. 151, March 10, 2003.

[326] Romanian Ombudsman Annual Report 2003, available at <http://avp/ro/rpeng.html>.

[327] In 2002, the Ombudsman received 211 notifications of processing of personal data, 145 of which were complete while 66 lacked some information. At the same time, 303 operators reported, out of which 11 declared transfers of personal data abroad. One of them only managed to receive an authorization, where the others did not meet the necessary conditions <http://www.avp.ro/raporten.html>.

[328] E-mail from Ioan Muraru, *supra*.

[329] In a public statement the President of the Ombudsman, Ioan Muraru, declared that the designation of this institution as the surveillance authority for personal data processing is against the purpose on this institutions and asked the Parliament to transfer these tasks to other public institutions. He believes that such an institution requires very specialized personnel and the Ombudsman does not and cannot have such structures. He asked for a specialized Control Authority on Personal Data Processing. "*Avocatul Poporului îsi declină competentele privind protectia datelor cu caracter personal*" (The Ombudsman Declines Responsibilities on Personal Data Protection) Azi, February 13, 2004, available at <http://www.azi.ro/arhive/2004/02/13/social.htm#stirea2>.

[330] E-mail from Ioan Muraru, *supra.*

In 2001, Law No. 682/2001 was enacted to ratify the Council of Europe (CoE)'s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108).

In 2002, Law No. 365/2002 on Electronic Commerce[331] adopted the opt-in principle for unsolicited commercial e-mails ("spam").[332] In 2002, the National Audiovisual Council[333] issued regulations regarding privacy and television and radio programs in Decision No. 80 of August 13, 2002 Regarding the Protection of Human Dignity and the Right to Protect One's Own Image 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 places 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."

The interception of telephone calls, the opening of correspondence and other similar actions are regulated by Law No. 51/1991 on National Security in Romania and Law No. 26/1994 on Police Organization.[334] Article 13 of Law No. 51/1991 allows the interception of calls in case of crimes against the state, only as a result of a mandate issued by the General Prosecutor of the Office related to the Supreme Court. The mandate has a duration of maximum six months with the possibility of being extended by up to three months by the General Prosecutor. According to Article 16 of the same law, the means to obtain information may not infringe citizens' fundamental rights and freedoms, *i.e.,* their private life, honor or reputation, or to subject those rights and freedoms to legal restrictions. The citizens who consider that their rights have been infringed, can appeal to the Commissions of Human Rights of the 2 Chambers of the Parliament. According to Article 17 of Law No. 26/1994 that aims at preventing organized crime and serious infringements in the interest of a criminal investigation, the police can require the Prosecutor's Office to intercept calls and open correspondence pursuant to Law No. 51/1991.

In 1996 the Criminal Code was modified by Law No. 41/1996 that introduced a new section on the use of audio and video recordings for interception purposes. The section establishes the conditions under which video and audio recordings may be carried out, including the interception of telephone calls. Therefore, according to Article 91 of the Criminal Code, the 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 use and efficiency in finding out the truth; the authority that carries out the wiretap has been properly authorized to do so. The authority competent to issue such an authorization is the prosecutor designated by the General Prosecutor of the Office related to the Court of Appeals. The authorization to wiretap is given for a period of up to 30 days. The authorization can only be extended for very substantiated reasons, and no longer than days.

The law also compels law enforcement authorities to report specific information about their wiretapping: the authorization given by the prosecutor, the number of the telephones between which the calls take place, the names of the people carrying out the conversations, and, 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.

---

331 Available at <http://www.legi-internet.ro\en\e-commerce.htm>.

332 Art. 6 (1) provide that "commercial communications through electronic mail are forbidden, except where the recipient has expressly consented to receive such communications."

333 Homepage <http://www.cna.ro>.

334 Nicolae Volonciu, Penal Procedure Treatise, 509-514 (Ed. Padeia 1999).

Similar provisions related to the recording of traffic data were introduced by the Law on Anti-Corruption No. 161/2003[335] in order to prevent and combat cyber-crime. Romanian law does not provide for the retention of traffic data by Internet service providers (ISPs). The law provides that, only in emergency 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 offense 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 ordinance and at the request of the investigative body or ex-officio, and during trial, by a court settlement. This ordinance is valid only for no longer than 90 days, and can be exceeded only once by a period not longer than 30 days.

Most of the cases involving invasion of privacy concerned the illegal interception of telephone calls. Several complaints were filed, especially by Opposition's members.[336] The president of the Senate Human Rights Commission recently declared[337] that a hearing of those people who complained on these issues should take place in the Commission. The Foundation Horia Rusu organized a public debate on those issues on 14 April 2003.[338] Two Opposition deputies presented a draft law[339] that would establish the conditions pursuant to which telephone calls could be intercepted so as to limit the intrusion into people's privacy. The draft provides that the warrant authorizing interception could be issued only by a judge and that, later on, the person wiretapped would have to be informed about the reasons of wiretapping. Other cases involved the invasion of privacy of several Romanian TV stars.[340]

Romania signed the Council of Europe Cybercrime Convention on November 23, 2001, and ratified it by adopting Law No. 64/2004.[341] 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.[342] Additional laws deal with privacy issues, such as the Patient's Rights Law[343] or the Law on Combating and Preventing the Traffic of Human Beings.[344]

The Law regarding Free Access to Information of Public Interest was approved in October 2001.[345] The law allows any person to ask for information from public authorities and state companies. The authorities must respond in maximum 30 days. There are exemptions for national security, public safety and public order, deliberations of authorities, personal data. Those whose requests have been denied can appeal to the agency concerned or to a court.

The 1999 Law on the Access to the Personal File and the Disclosure of the *Securitate* as a Political Police[346] allows Romanian citizens to access their *Securitate* (secret police) files. It also allows public access to the files of those aspiring for public office. The law sets up the National Council for the Search of Security Archives (CNSAS) [347] to administer the *Securitate* archives.

---

335 Official Monitor No. 279, April 21, 2003, available at <http://www.legi-internet.ro/en/cybercrime.htm>.

336 Such as Dan Carlan, vice-president of the Liberal Party; Iasi Count, Dorin Marian, ex-counsellor of the former President Emil Constantinescu.

337 Roxana Ristache, "Interception of Telephone Calls from Iasi in Attention of the Senate," Cotidianul, April 16, 2003.

338 Ovidiu Banches, "The Citizen Threatened by National Safety," Ziua, April 15, 2003.

339 Draft law No. 207/2002 amending Law No. 51/1991 on the National Security of Romania.

340 "Extensions of Free Speech against Privacy?" Cotidianul, April 19, 2002, available at <http://www.cotidianul.ro/anterioare/2002/reportaj/rep1521apr.htm>.

341 Official Monitor No. 343, April 20, 2004, available at <http://www.legi-internet.ro/ratifcybercrime.htm> (in Romanian).

342 Official Monitor No. 279, April 21, 2003, available at <http://www.legi-internet.ro/en/cybercrime.htm>.

343 Law No. 46/2003, Chapter IV.

344 Law No. 678/2001, Art. 26, Parag. 2.

345 <http://www.publicinfo.ro/INITIAT/Legea%20accesului%20engl.pdf>.

346 Law No. 187/1999 available at <http://www.cnsas.ro/legeeng.html>.

347 Homepage <http://www.cnsas.ro/indexeng.html>.

The Law on Protecting Classified Information was enacted in April 2002 at the behest of North Atlantic Treaty Organization.[348] Its drafters used an expansive view of classification that will limit access to records under the access to information law. The law was strongly criticized by the Opposition and the civil society.[349]

In the draft of the new Penal Code,[350] an article provides that the infringement of a person's right to privacy by using remote means of interception to get data, information, images or sounds from home or other similar private property without its owner's consent or by breaking the law, is punished with an imprisonment of two to five years. It is also prohibited to disseminate data, information, images or sounds obtained in one of the ways set out in Paragraph 1 of Article 204. Some Romanian NGOs[351] have requested the elimination of this article, because, in its current wording, it limits the freedom of expression and the debate of matters of public interest. The new version of the Penal Code[352] will enter into force on June 29, 2005. The former Article 204 is now replaced by Article 209 that provides that it is not a crime to make a photo or to film a building from public places."[353]

A Government Decision No. 952 of August 14, 2003[354] calls for the establishment of an Integrated Informational System (SII) The SII is a database that will centralize the information held by all public institutions on natural and legal persons. It may become the electronic arm of the Romanian Intelligence Service (SRI). Both the Association for the Defense of Human Rights in Romania – Helsinki Committee (APADOR-CH) and the media criticized this decision by arguing that the Government Decision was not legal, and because of the threats the decision raises for certain fundamental rights, especially the right to privacy.[355]

APADOR-CH filed an administrative complaint with the Government, based on Article 5 of Law 29/1990 on administrative courts, pointing out that the decision was illegal and violated the right to privacy, and requesting that the decision be annulled/ withdrawn.[356] The government rejected all objections. As a consequence, the APADOR-CH as a legal entity, and two of its members as individuals, filed a court complaint considering that the decision has seriously infringed upon the subjective right to privacy of APADOR-CH's members (as well as of all other people), a right guaranteed by Article 26 of the Constitution and Article 8 of the European Convention of Human Rights. The court has taken no decision yet.

---

348 Law No. 182/2002, Official Monitor, April 12, 2002, available at <http://www.crji.go.ro/legeainfclas.htm> (in Romanian).

349 *See* for more details: The Association for the Defense of Human Rights in Romania – The Helsinki Committee (APADOR-CH). The Limits to Information in Romanian, available at <http://www.apador.org/limits.htm>.

350 Available at <http://www.just.ro/bin/proiecte/cod_penal.htm> (in Romanian).

351 Such as APADOR-CH and the Association for Promoting and Protecting the Freedom of Expression (APPLE).

352 Official Monitor No. 575, June 29, 2004.

353 "Practically, it may be considered a crime even if a journalist takes pictures of an official's villa without permission because the villa is inside the yard and taking pictures of whatever is inside the yard violates the official's right to privacy. Of course, not listing these deeds as crimes does not mean that privacy remains unprotected, only that it has to be protected by civil, not criminal laws. If there is no political will to eliminate this incrimination, the draft should at least be modified by introducing a provision to stipulate that the deed is not a crime if it refers to aspects of private life impeaching over a person's capacity to exercise a public function." APADOR – CH Report on 2003 – available at <http://www.apador.org/rapoarte/anuale/report2003.htm>.

354 Official Monitor No. 631, September 3, 2003.

355 APADOR-CH considers that the government resolution refers to a decision of the Supreme Defence Council (CSAT), which could not be substituted to the Parliament's. APADOR-CH's representative Manuela Stefanescu said: "We do not know to whom this integrated information system is subordinated; we do not know to whom it is of use, and it is extremely dangerous to create a superpower, especially without the slightest guarantee that the personal data will be protected. . . . Furthermore, natural and legal persons lack any means of controlling the way in which the data centralized in this mammoth system will be used. . . .". Evenimentul zilei, September 29, 2003, available at <http://www.evz.ro/english/?news_id=132980>.

356 *See* the complaint in the APADOR 2003 report available at <http://www.apador.org/rapoarte/anuale/report2003.htm>.

Russian Federation

The Constitution of the Russian Federation recognizes rights of privacy, data protection and secrecy of communications. Article 23 states, "1. Everyone shall have the right to privacy, to personal and family secrets, and to protection of one's honor and good name. 2. Everyone shall have the right to privacy of correspondence, telephone communications, mail, cables and other communications. Any restriction of this right shall be allowed only under an order of a court of law." Article 24 states, "1. It shall be forbidden to gather, store, use and disseminate information on the private life of any person without his/her consent. 2. The bodies of state authority and the bodies of local self-government and the officials thereof shall provide to each citizen access to any documents and materials directly affecting his/her rights and liberties unless otherwise stipulated under the law." Article 25 states, "The home shall be inviolable. No one shall have the right to enter the home against the will of persons residing in it except in cases stipulated by the federal law or under an order of a court of law."[357]

According to the federal Law on Information, Informatization and the Protection of Information (LIIPI),[358] governmental data resources are open for general use except for documented information of limited access (data relevant to state secrets and confidential information). Personal data is considered confidential information. The Law states, in particular, that collection, storage, use and distribution (processing) of information pertaining to the private life of a natural person without his or her permission, shall be prohibited, except for processing implemented on the basis of judicial warrant.[359] The term "personal data" and some guarantees for personal data protection appear in new laws, in particular, the Tax Code,[360] the Labor Code[361] and the federal Law on Statements of Civil Status. Also, confidentiality of information has been mentioned in various laws relevant to professional secrets.[362] Russian federal laws establish over 30 types of classified data while other governmental regulations add about 10 types of data to the list. Approximately 45 laws of the Russian Federation have provisions concerning various classified data.[363]

According to Articles 11 and 21 of the federal Law on Information, Informatization and the Protection of Information, the list of personal data and the ways it is protected are to be stipulated by special federal law. The *Duma* (the lower chamber of the Russian Parliament) has not yet approved this law. Two bills names on Personal Data were proposed in 1998 and in 2000 but are still pending in the Parliament.

In Russia (especially in Moscow and St. Petersburg) illegal collection and distribution of data on private persons and organizations is quite commonplace. Quite popular are databases on purchase/sale of cars, car owners, passport data and foreign passport data of Russian citizens, data on real estate (purchase and sale of apartments, their parameters, location and proprietors), databases of taxpayers, information about people wanted for crimes and those who have been previously convicted. Cheap CDs with such databases are easily available on the streets and the Internet. In the beginning of 2003, Mobile Telesystems (MTS), a mobile phone company, suffered a massive security breach that led to the sale of

---

357 Constitution of the Russian Federation, available at <http://www.russianembassy.org/RUSSIA/CONSTIT>.The Constitution of the Russian Federation was adopted by national voting on December 12, 1993. The previous Constitution (which was adopted in 1977 by the Supreme Soviet of the USSR) ensured weaker privacy guarantees.

358 Russian Federation Federal Law No. 24-FZ, Law of the Russian Federation on Information, Informatization and Information Protection, January 25, 1995 <http://www.datenschutz-berlin.de/gesetze/internat/fen.htm> (extracts).

359 *Id.* Article11.

360 Tax Code, Article 84, Part 1.

361 Labor Code, Articles 85-90. *See also* "Improved Russian Labor Code Entered Into Force," Vol. 8, No. 2, International Law Update, February 2002.

362 Law "On banks and Banking Activity," Principles of legislation of the Russian Federation with regard to citizens' health protection, Family Code, Tax Code, etc.

363 Human Rights Network, Privacy in the Russian Internet (Human Rights Publishers, 2003), available at <http://www.russianlaw.net/english/ae05.htm>.

CDs with MTS's entire database of several million customers. By law, MTS was required to share information about their customers with the police and government agencies. MTS claimed that the database had been stolen and that the company had started its own internal investigation without seeking help from law enforcement agencies. The company refused to provide details as to the results of this investigation, and the results of this investigation have not been announced. Widespread speculation and comments from an MTS spokesperson indicate that the data was leaked by a low-paid employee from one of these government agencies.[364] In May 2003, Russian media wrote about a similar database theft case in Saint Petersburg.

Russian legislation does not establish a central regulatory body for data protection. Some efforts are being carried out by regional ombudsmen, *e.g.*, the Ombudsman of the region of Perm that initiated an investigation on the practices of a local communications company that used clients' phone numbers for commercial purposes. The Chamber of Appeals on Informational Conflicts, a quasi-judicial body which scope includes the protection of privacy, was also active.[365] This "structure" operated with the support of the mass media, and although its decisions were not binding, they were usually complied with The Chamber of Appeals was closed during President Putin;s presidency.[366]

The 1995 Communications Law protects secrecy of communications. A new version of this law came intro force on January 1, 2004. The tapping of telephone conversations, scrutiny of electronic communications, delay, inspection and seizure of postal mailings and documentary correspondence, receipt of information therein, and other restriction of communications secrets are allowed only with a court order.[367] The Law on Operational Investigation Activity that regulates surveillance methods used by secret services requires a court-issued warrant.[368] The law was amended in December 1998 by the State *Duma*. Guarantees for the protection of privacy were emphasized and additional controls imposed on prosecutors. Article 5 of the Law provides that an investigative structure must secure people's privacy. The Law also provides: "If one believes that some actions of bodies conducting operational investigation have infringed on an individual's rights or freedoms, the individual has the right to appeal to a court, a prosecutor, or to a higher body that carries out investigative activities." Article 6 of the federal Law on Federal Security Services of the Russian Federation has a similar provision:[369] "If a person has not been convicted during a legally established procedure, then all materials obtained during this operational investigation must be archived for a period of one year (in compliance with the Law on Operational Investigations) and subsequently deleted." However this provision is virtually revoked by the following addition: ". . . unless official interests or justice require otherwise."[370] In December 1999, the law was amended to allow surveillance by the tax police, Interior Ministry, Border Guards, the Kremlin Security Service, the Presidential Security Service, the parliamentary security services and the Foreign Intelligence Service.[371] In 2001 the following provision was added to the Law:[372] "Audio recordings and other materials resulting from interception and wiretapping of the conversation of persons being out of criminal proceedings must be deleted within six months after the wiretapping is over with an appropriate

---

[364] Sabrina Tavernise, "Personal Data Is Pirated from Russian Phone Files," New York Times, January 23, 2003, available at <http://www.nytimes.com/2003/01/23/business/worldbusiness/23DATA.html?ex=1054440000&en=fee2785ba6eafbb5&ei=5070>.

[365] The Chamber mostly tried to settle conflicts in the media community by establishing a mechanism of self-regulation. Its status was unclear because the Chamber was officially attached to the president's administration (executive branch) while playing the role of a court (judicial branch). The establishment of such an institution isarguably against the basic principle of the division of powers between the executive, the legislative, and the judicial branches). However, since the Chamber's decisions were not binding, no one opposed its establishment.

[366] The Chamber was closed by the presidential Decree No. 1031 of June 3, 2000.

[367] Russian Federation Federal Law "On communication" No. 15-FZ, Article 32. Adopted by the State Duma on January 20, 1995.

[368] The Federal Law No. 144-FZ of August 12, 1995.

[369] The Federal Law No. 40-FZ of April 3, 1995.

[370] Article 5 of the Federal Law "On operational investigations" of August 12, 1995 (the Federal Law No. 144-FZ of 1995).

[371] "Police Get Window of Access to E-mail," The Moscow Times, January 13, 2000.

[372] This amendment has been introduced by the Federal Law No.26-FZ of March 20, 2001.

protocol.[373] The judge must be notified three months before materials reflecting the results of operational investigations, implemented on the basis of a court warrant, are deleted." Disclosure of data that affects someone's privacy without his or her consent, is legally prohibited unless otherwise stipulated by federal laws. The Law on Federal Security Service of the Russian Federation contains no requirement for the deletion of data but stipulates that the information shall not be transferred to anyone else.

The Federal Security Service (FSB) has conducted phone tapping using the "SORM" system (or "System of Operative Investigative Activities"). In 1998 information about a new SORM-2 system that applies to the Internet was revealed. SORM-2 requires Internet Service Providers (ISPs) to install surveillance devices and high-speed links to local FSB departments which would allow the FSB to directly access Internet users' communications, although with a warrant requirement.[374] These rather expensive devices and links are to be paid for by the ISPs themselves. While most ISPs have not publicly resisted FSB's demands to install SORM-2,[375] one ISP in Volgograd, Bayard-Slaviya Communications, challenged the FSB's demands. The local FSB and the Ministry of Communications attempted to have their license revoked but backed off after the ISP challenged their decision in court.

The existence of SORM-2 was confirmed by the State Committee of the Russian Federation on Communication and Informization (*Goskomsvyaz*, now the Ministry of Communications) as Order No. 47 in March 27, 1999, and Order No. 130, in July 25, 2000, which was registered with the Ministry of Justice on August 9, 2000. Order No. 130 was immediately challenged in the Russian Supreme Court by Pavel Netupsky, a Saint-Petersburg journalist. Although the Court upheld SORM-2, it ruled part 2.6 illegal, and therefore made sure that ISPs would know whom the FSB is monitoring.[376] Netupsky lost on all other counts. SORM-2 has now been implemented, although FSB representatives have not provided any evaluation of how effective SORM-2 has been for the prevention and investigation of criminal activities, and there have been no announced arrests as of yet. Although the FSB insists that there have been no violations of privacy, its assertions cannot be verified as Russia lacks the appropriate supervisory and independent body to control FSB's activities. ISPs are used to avoid comments on any issues connected with SORM-2.

Governmental proposals concerning digital rights tend to be intrusive. In the beginning of April 2000, the Committee of the State *Duma* for Information Policy introduced a bill on Regulation of the Russian Segment of the Internet that raised many critiques. The Russian Internet community did its best to prevent this bill from becoming a law and suggested an alternative bill on the State Policy of the Russian Federation Pertaining to the Development and Use of the Internet.[377] On May 18, 2000, parliamentary hearings took place to discuss the bill and the legislation relevant to the Internet. Most of its participants agreed that there was "no need for a special law applicable to the Internet."[378] However, in June 2004, the Moscow major Yuri Luzkov published a contradictory article with the main idea of establishing control over the Internet. Soon afterwards Lyudmila Narusova, member of the higher chamber of the Russian Parliament, confirmed that appropriate law on the Internet is being prepared in the Parliament.[379]

---

[373] The "protocol" is an official paper, a form that must be completed and signed to certify that the data was deleted.

[374] "Russia Prepares to Police Internet," The Moscow Times, July 29, 1998. More information in English and Russian is available from the Moscow Libertarium Forum <http://www.libertarium.ru/libertarium/sorm/>.

[375] In Russia a license is necessary for providing Internet services. ISPs have to meet license terms and conditions including cooperation with secret services.

[376] "Supreme Court Rules Phone-Tapping Clause in Decree to be Illegal," BBC World Monitoring, September 28, 2000.

[377] Alexander Kostinsky and Sergei Smirnov, "Hello! The Parliament Is listening!," Internet.ru, May 19, 2000, available at <http://www.internet.ru/articles/n_r9z1.esp>.

[378] Human Rights Network, Privacy in the Russian Internet (Human Rights Publishers, 2003), available at <http://www.hro.org/docs/reps/privacy/2002/eng/>.

[379] "Russian Parliament Plans to Regulate Internet," MosNews, June 3, 2004 <http://www.mosnews.com/news/2004/06/03/internet.shtml>.

The Federal Law on Commercial Secret was enacted on July 29, 2004.[380] The law regulates the disclosure of commercial secrets and how its confidentiality can be protected. It also defines information that may not be considered "commercial secret," and establishes a list of information that may constitute commercial secret, including but lot limited to, the number of employees, the system of remuneration, labor conditions including safety arrangements, work-related injuries, occupational morbidity figures, and vacancies; as well as past infringements to the Russian Federation legislation and ensuing prosecutions. The law expressly stipulates that the owner of commercial secrets is the employer.

Anti-terrorist campaigns the United States government promoted worldwide after the terrorist acts of September 11, 2001 in New York and Washington have influenced Russian legislation. On December 20, 2000, the State *Duma* approved the amendments to federal laws on Terrorism and on Mass Media in first reading. Although these amendments did not specifically concern online privacy, they seriously limited distribution of "extremist materials" via the Internet (even though "extremism" and "extremist materials" were not defined in Russian law at the time). On April 30, 2002, the President announced a bill on Counteraction to Extremist Activities. The bill contained broad definitions of "extremist activities" and, some critics argued, enabled a wide range of public protest actions to be viewed as extremism. The first draft contained an article relevant to the Internet: ISPs were forced to censor materials on their servers and remove/block "extremist sites." This article was later replaced with the indistinct reference to other legislation and the controversial procedure of Internet monitoring and censorship was dropped[381]. After the terrorist attack in Moscow of October 2002[382] the State *Duma* quickly adopted several amendments to the laws on Mass Media and Terrorism, banning any distribution of information that could impede anti-terrorist actions.[383]

According to Article 53 of the new Federal Law on Communications, the data about telecommunications users are confidential and are protected by Russian legislation.

Russian legislation provides criminal liability for the invasion of privacy. The Criminal Code provides a penalty for violation of the immunity of private life,[384] violation of secrecy of communications,[385] infringement of home inviolability,[386] The Criminal Code also provides liability for unauthorized access to legally protected computer information,[387] The Criminal Code provides with sentences ranging from fines, forced labor, arrest, to a ban on the right to hold certain positions or to be engaged in a certain activity and, in some cases, imprisonment for a period of up to 5 years.[388] Maximum fine is as high as 800 "minimal legal monthly wage."[389] According to the Civil Code,[390] privacy is a legally protected non-property right. Attached to this right are personal dignity, personal immunity, honor and good name, business name, personal secret and family secret. If an individual suffers physical or moral damages by violation of his or her personal non-property rights or some other non-material welfare rights, as well as in other cases provided by the law, a court can force the person invading privacy to provide financial

---

380 Federal Act N98-FZ.

381 The Law "On Counteraction Extremist Activity" No. 114-FZ of July 25, 2002. *See also* Declan McCullagh, "Russia Poised to Restrict Net Activities," CNET, June 24, 2002, available at <http://news.com.com/2100-1023-938810.html>.

382 On October 23, 2002, a group of Chechen terrorists captured about 800 hostages in one of Moscow theaters. Their demand to the Russian government was to withdraw their troops from the territory of Chechnya. The terrorist attack ended up with the death of all terrorists and 129 of the hostages. Since 1999 a war in Chechnya opposed the Russian federal government and Chechen rebels.

383 The Russian government considers the war in Chechnya to be an "counter-terrorist" operation.

384 Criminal Code, Article 137.

385 *Id.* Article 138.

386 *Id.* Article 139.

387 *Id.* Article 272.

388 *Id.* Article 272, Part 2.

389 Due to inflation, this unit (called "MROT") is regularly reviewed and changed by the State *Duma*. For the period of summer/fall 2003, 800 MROT is about USD 10,000.

390 Civil Code, Article 150, Part 2.

compensation.[391] The Administrative Code (effective since July 1, 2002) states that "infringement of a legally established procedure of collection, storage, use or distribution of information about citizens (personal data)" shall lead to a warning or penalty.[392] The Administrative Code also establishes liability for disclosure of information if access to it is restricted by federal law.[393] The illegitimate refusal by a public official to submit information to a person is also an administrative breach of the law.[394]

The United Nations Human Rights Committee expressed concerns over the state of privacy in Russia in 1995 and recommended the enactment of additional privacy laws. It noted: "The Committee is concerned that actions may continue which violate the right to protection from unlawful or arbitrary interference with privacy, family, home or correspondence. It is concerned that the mechanisms to intrude into private telephone communication continue to exist, without a clear legislation setting out the conditions of legitimate interference with privacy and providing for safeguards against unlawful interference. The Committee urges that legislation be passed on the protection of privacy, as well as strict and positive action be taken, to prevent violations of the right to protection from unlawful or arbitrary interference with privacy, family, home or correspondence."[395]

The Fifth Periodical Report of the Russian Federation on the Implementation of the International Covenant on Civil and Political Rights provides that in the last four years 42 persons were convicted for violations of privacy, 61 for the violation of the secrecy of communications. According to the same source, the number of persons convicted for breaching the inviolability of the home for the same period is much higher (5,476 persons). This apparently shows the lack of legislation and enforcement required for the investigation of crimes related to the breach of privacy, as well as the lack of governmental oversight and independent institutions that could monitor how privacy laws are implemented. Law enforcement structures used to refer to the lack of legal grounds and, in particular, to the vagueness of the legal status of "data."[396] The constitutional right of personal privacy is usually considered insufficient to provide a legal basis for criminal proceedings. People usually choose not to turn to courts when their privacy is violated for several reasons: lack of laws and procedures that could be effectively used by plaintiffs; monetary damages in all cases are usually small; people do not consider privacy as a fundamental right and do not believe it can be effectively protected from government interference.[397]

In January 2002, the government adopted the federal program "Electronic Russia" for the period 2002-2010. The program has provisions about freedom of search, access, transfer, production and distribution of information, and privacy safeguards for any legally protected information available on information systems For these purposes the authors of the program have proposed to elaborate an effective ground for regulations. This basis should extend to the regulation of issues of information security and realization of citizens' constitutional rights. However, the confidentiality was not mentioned as a major governmental policy issue. One of the tasks in this program is described as a "legal solution of the problems concerning performance of operational investigations through computer networks." Other program items include the electronic circulation of documents, business information security, etc. The Russian Ministry for Communication and Information and the Ministry for Economic Development and Trade of the Russian Federation are the leading coordinator for this program.

---

391 *Id.* Article 151.

392 Administrative Code, Article 13.11.

393 *Id.* Article 13.14.

394 *Id.* Article 5.39.

395 United Nations Human Rights Committee, Comments on Russian Federation, U.N. Doc. CCPR/C/79/Add.54 (1995), available at <http://sim.law.uu.nl/SIM/CaseLaw/uncom.nsf/0/9172bc5146972b6dc125663c00343b49?OpenDocument>.

396 The law contains no clear definition of what "personal data" are and how they are to be processed; instead the law refers to federal law which should contain everything but has not been adopted in Russia by now.

397 Human Rights Network, Privacy in the Russian Internet (Human Rights Publishers, 2003), available at <http://www.russianlaw.net/english/ae05.htm>.

The notion of "privacy policy" has not yet become commonplace in Russia. Few web sites ensure the privacy of their customers. ISPs take appropriate measures to control spam after receiving consumer complaints. Freeware and shareware programs for the protection of personal privacy of Internet users are available on Russian servers.[398]

Russia has a national ID system. Each person above 14 years old must have a personal document (internal passport) that can be obtained at a local department of the Ministry of Internal Affairs. This Passport is used as the main ID document and is necessary for many activities, including the purchase of train and plane tickets. Each passport bears a residency permit stamp (the so-called *propiska*). Russian courts (including the Supreme Court in 1998) have asserted that this permission regime is unconstitutional. Moscow authorities insist that the *propiska* is only a notification procedure. However, for those attempting to move to Moscow, bureaucrats can make this registration a painful and complicated process. Without *propiska* it is difficult get a well-paid job, get full public medical aid, children cannot attend public schools, etc. Moscow police used to stop people at streets and fine them if they did not carry their *propiska*.[399]

In recent years, officials, both at federal and Moscow levels, announced several times that a new system of electronic IDs would be introduced in the near future. According to these statements, the new system would supplement, and later replace, internal passports.[400] In January 2004, the Russian Ministry of Economical Development announced its plans to build a national system that would connect existing major public databases through a new ID system. According to the Ministry, each newborn Russian will be assigned a unique ID. Other people will get their IDs too. No central database will be created but a new governmental body responsible for data processing may be created later on. Access to these databases is promised to be "easy" for common people The government hopes to implement this system in 2006.

Russia 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.[401] The Russian Federation has signed the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) but has not ratified it.[402]

Russia participated in the negotiations on the CoE Convention on Cybercrime which was opened for signature in November 23, 2001.[403] The Convention requires Member States to establish criminal offences under their domestic laws regarding various computer or computer-related crimes, including unauthorized access to a computer system and unauthorized interception of a data transmission. As of June 2004, Russia has not yet signed the treaty.

Autonomous Russian Republics

Constitutions of 10 (out of 20) republics of Russian Federation reproduce Articles 23, 24 and 25 of the Federal Constitution. The Constitution of Bashkortostan incorporates the addendum, admitting search

---

398 *Id.*

399 *E.g.*, *see* Chris Riley, "Moscow's Heart of Darkness," NBC news, August 7, 1998, available at <http://msnbc.msn.com/id/3072234/#BODY>.

400 Mayakinfo.ru, available at <http://www.mayakinfo.ru/news.asp?msg=676>; "Gref: electronic Ids may replace passports in 6-8 years," Russia Journal Daily, June 10, 2003, available at http://www.russiajournal.com/print/russia_news_38527.html.

401 Signed 28/02/96, ratified 05/05/98, entered into force 05/05/98 <http://conventions.coe.int/>.

402 Signed November 8, 2001, available at <http://conventions.coe.int/>.

403 <http://conventions.coe.int/>.

only on the basis of a judicial warrant. In other cases there are fewer privacy safeguards than in the federal Constitution, or even no safeguards at all (Karelia, Kalmykia). There are no essential differences between the constitutions of the republics and federal privacy guarantees. The Constitution of Tyva contains an interesting article providing an opportunity to introduce legal limitations to the right to home inviolability by a Republican Law.[404]

Republic of San Marino

The Act on Collection, Elaboration and Use of Computerized Personal Data was enacted in 1983 and amended in 1995.[405] The Act applies to any computerized filing system or data bank, both private and public. It prohibits the collection of personal and confidential data through fraudulent, illegal or unfair means. It requires that information is accurate, relevant and complete. Any individual is entitled both to inquire whether his or her personal data have been collected or processed, to obtain a copy, and to require that inaccurate, outdated, incomplete or ambiguous data, or data whose collection, processing, transmission or preservation is forbidden, be rectified, integrated, clarified, updated or canceled. The creation of a data bank requires the prior authorization of both the State Congress (the Government) and the Guarantor for the Safeguard of Confidential and Personal Data. There are additional rules for sensitive information. Infringements can be punished by means of administrative sanctions or penalties. There were a number of Regency's Decrees issued under the 1983 Act that remained in force after the 1995 revisions.[406] The Regulation on Statistical Data Collection and Public Competence in Data Processing[407] regulates data processing within the Public Administration.

The Guarantor enforces the Act for the Safeguard of Confidential and Personal Data, a judge of the Administrative Court. The Guarantor can examine any claim or petition relating to the application of the above-mentioned law and pass judgment whenever the confidentiality of personal data is violated. His judgment can be appealed to a higher court. The release of information to other countries is conditioned on the prior authorization of the Guarantor, who must verify that the country to which confidential information is being transmitted ensures the same level of protection of personal data as that established in Sammarinese legislation.

Under pressure from the Organization for Economic Co-operation and Development (OECD), San Marino has recently agreed to amend its tax laws and if necessary weaken financial privacy standards, in order to facilitate better "exchange of information in tax matters."[408]

San Marino is a member of the Council of Europe but has not signed nor ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108). It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[409]

---

404 Human Rights Network, Privacy in the Russian Internet (Human Rights Publishers, 2003), available at <http://www.russianlaw.net/english/ae05.htm>.

405 Regulating the Computerized Collection of Personal Data, Law No. 70 of May 23, 1995 revising Law No. 27 of March 1, 1983, amended by Law No. 70/95.

406 Decree No. 7 of March 13, 1984, Establishment of a State Data Bank as provided for by Article 5 of Law No. 27 of March 1, 1983; Decree No. 7 of June 3, 1986, Integration to Decree No. 7 of March 13, 1984, Establishing a State Data Bank; Decree No. 140 of November 26, 1987, Procedures for the Establishment of Private Data Banks.

407 Regulation on Statistical Data Collection and Public Competence in Data Processing, Law No. 71 of 23 May 1995.

408 "The War on Tax Havens," The National Post, September 4, 2001.

409 Signed November 16, 1988; ratified March 22, 1989; entered into force March 22, 1989.

Republic of Singapore

The Singapore Constitution is based on the British system and does not contain any explicit right to privacy.[410] The High Court has ruled that personal information may be protected from disclosure under a duty of confidences.[411]
There is no general data protection or privacy law in Singapore.[412] The government has been aggressive in using surveillance to promote social control and limit domestic opposition.[413]

Singapore has no governmental authority affiliated with privacy or data protection, except for a small privacy division within the Ministry of Finance.[414] The idea of data protection legislation had been officially "under review" by the government for twelve years. A Straits Times survey revealed that 80 percent of readers feel that personal information contained in databases is too freely accessible.[415] For purposes of e-commerce, the National Internet Advisory Committee proposed the Model Data Protection Code for the Private Sector in February 2002[416] and the National Trust Council will decide whether to implement it later in the year, though businesses will not be required to adopt its provisions.[417]

In September 1998, the National Internet Advisory Board released an industry-based self-regulatory "E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce."[418] The Code encourages providers to ensure the confidentiality of business records and personal information of users, including details of usage or transactions. It prohibits the disclosure of personal information, and requires providers not to intercept communications unless required by law. The Code also limits information collection and prohibits the disclosure of personal information without informing the consumer and giving them an option to stop the transfer, ensures accuracy of records, and provides a right to correct or delete data.[419] In 1999 the Code was adopted by CaseTrust -- a joint project operated by the Consumers Association of Singapore, CommerceNet Singapore Limited and the Retail Promotion Centre in Singapore –and incorporated into its Code of Practice as part of an accreditation scheme promoting good business practices among store-based and web-based retailers (CaseTrust is).[420] The Info-Communications Development Authority (IDA), the lead agency in charge of e-commerce regulation, announced in March 2000 that it would endorse the TRUSTe system as "an industry 'trustmark' seal."[421]

Development of anti-spam legislation was initiated in May 2004. The IDA announced a multifaceted approach including legislation, public education and self-regulation of the marketing industry.[422] The IDA and the Attorney-General's Chambers of Singapore (AGC) issued a joint report proposing the legislative strategy for anti-spam legislation and recommended an opt-out approach.[423] The report also

---

410 Constitution of the Republic of Singapore, September 1963, available at <http://www.oefre.unibe.ch/law/icl/sn00000_.html>.

411 X v. CDE1992 2 SLR 996.

412 *See* <http://bakerinfo.com/apec/singapec_main.htm#Privacy>.

413 *See* Christophen Tremewan, The Political Economy of Social Control in Singapore (St. Martin's Press, 1994).

414 Report of the National Internet Advisory Board 1997/1998, September 1998. *See also* Susan Long, "Guess Who's Reading Your Personal Data Today?" Singapore Press Holdings, May 18, 2002.

415 Long, *supra*.

416 "Consultation on Protection Regime," BNA World Data Protection Report, Volume 2, Issue 4, April 2002.

417 "Voluntary Singapore Web Codes to Protect Privacy," Reuters, February 5, 2002.

418 Kien Keong Wong and Ken Chia (Baker & McKenzie Singapore), "E-com Legal Guide, Singapore,", January 2001, available at <http://www.bakerinfo.com/apec/singapec_main.htm#Privacy>.

419 *Id.*

420 *Id.*

421 "Infocomm Development Authority Helping Singaporeans Go Online," March 2000, available at <http://www.ida.gov.sg>.

422 *See* Infocomm Development Authority of Singapore, Multi-Pronged Measures Developed to Curb E-Mail Spam in Singapore, press Release, May 25, 2004 <http://www.ida.gov.sg/idaweb/marketing/infopage.jsp?infopagecategory=&infopageid=I2884>.
Id.

recommends requiring advertisers to label marketing email as such and prohibiting fake return email addresses.[424] The laws are expected to be finalized in 2005.[425]

The Singapore AntiSpam Resource Centre website was launched in May 2004 "to provide a central anti-spam repository for the public and industry." The site includes information for consumers, including reviews of antispam software and free software downloads, and information about Singapore's proposed anti-spam legislation and how consumers can comment on the proposal.[426] The Singapore Information Technology Federation, a group of technology security companies such as Brightmail and Symantec, held an antispam forum on June 22, bringing together government, industry and trade associations, IT companies and academics to discuss legal, policy and technical anti-spam solutions.[427]

In 2002, the Singapore government created the Media Development Authority (MDA) to regulate media content – including Internet, radio, television, and radio.[428] The MDA formed through a merger of the existing Singapore Broadcasting Authority (SBA), the Films and Publications Department (FPD), and the Singapore Film Commission (SFC) with the goal of uniting of various forms of media under a single authority.[429]

Like its predecessor the SBA, the MDA has assumed the strict approach towards regulating the Internet. All Internet Service Providers (ISPs) and Internet Content Providers are required to comply with the Internet Code of Practice[430] and the Class License Provisions.[431] ISPs are required to register with the MDA, along with ICPs who promote the discussion of political or religious topics relating to Singapore.[432] ISPs are required to deny access to sites identified by the MDA as containing prohibited material.[433] Likewise, ICPs may not broadcast prohibited material or entertain discussion on prohibited themes.[434] Prohibited material includes pornography, material that "advocates homosexuality or lesbianism," and material that "glorifies, incites or endorses ethnic, racial or religious hatred, strife or intolerance," among other prohibitions.[435] Political content, especially during elections, is regulated.[436] "Over the boundary markers" – religion, race and government criticism – is strictly enforced while other issues, while still subject to regulation, has not traditionally been enforced as strictly.[437]

The Minister of Information, Communication, and the Arts appointed a Censorship Review Committee in 2002 to examine censorship policies related to broadcast media and to make recommendations.[438] The Committee released their report in July 2003. The findings recognized that young and artistic communities are restricted by current censorship rules, but reported that the majority of Singaporeans are

---

424 Joint Infocomm Development of Authority of Singapore and Attorney-General Chambers of Singapore Report, Proposed Legislative Framework for the Control of Email Spam, <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=infoecon:pnr&versionid=1&infopageid=I2883>.

425 "Singapore Drawing Up Neew Anti-Spam Laws," Channel NewsAsia, May 25, 2004.

426 See <http://www.antispam.org.sg/>.

427 <http://ssc.sitf.org.sg/default.aspx>.

428 Media Development Authority of Singapore Act (Act 34 of 2002), available at <http://statutes.agc.gov.sg>. This statutory board operates under the authority of the Ministry of Information and the Arts.

429 <http://www.mda.gov.sg/aboutus/index.html>.

430 Internet Code of Practice, available at <http://www.mda.gov.sg/medium/internet/i_codenpractice.html>.

431 Class License Provisions, available at<http://www.mda.gov.sg/medium/internet/i_classlicence.html>.

432 *Id.* at § 2-3.

433 Internet Code of Practice, *supra* at § 3.

434 *Id.* at § 3(3).

435 *Id.* at § 4.

436 John O'Callaghan, "Singapore Calls November 3 Election," Reuters, October 24, 2001, available at <http://www.thinkcentre.org/article.cfm?ArticleID=1183>.

437 Email from Milagros Rivera to Patrick Mueller, EPIC Clerk, Electronic Privacy Information Center, July 2, 2004 (on file with the Electronic Privacy Information Center).

438 *See* the Censorship Review Committee's webpage, at <http://www.mda.gov.sg/content/CRC_executive.html>.

satisfied with the censorhip regime.[439] The report recommended increased access to films under a more granular rating system and additional television programming allowing relaxed content restrictions after prime time.[440] Although the report recognized that the Internet has wrought significant changes to access to media, it recommended that ISPs "should develop and subscribe to a code of conduct and put greater effort in protecting the young by developing an effective filtering system within a period of two years."[441] Prominent members of the arts community call the recommendations "cosmestic," demanding a shift away from censorship – through editing or banning – and towards regulation of the audience permitted to view the work.[442]

In July 1998, the Singapore government enacted three major bills concerning computer networks. They are the Computer Misuse (Amendment) Act (CMA), the Electronic Transactions Act and the National Computer Board (Amendment) Act. The CMA prohibits the unauthorized interception of computer communications.[443] The CMA also provides the police with additional powers of investigation, and makes in an offense to refuse to assist the police in an investigation. The CMA also grants law enforcement broad power to access data and encrypted material when conducting an investigation. In November 2003, the CMA was revised, allowing the government to arrest an individual on suspicion of hacking, with penalties up to SGD 10,000 or up to three years imprisonment.[444] This power of access requires the consent of the Public Prosecutor. The Electronic Transactions Act imposes a duty of confidentiality on records obtained under the act and imposes a maximum SGD 10,000 fine and 12-month jail sentence for disclosing those records without authorization. The IDA and the AGC began work in February 2004 to update the ETA.[445] Police have broad powers to search any computer and to require disclosure of documents for an offense related to the act without a warrant.[446] More broadly, the government has wide discretionary powers under the Internal Security Act, the Criminal Law Act, the Misuse of Drugs Act, and the Undesirable Publications Act to conduct searches without warrant, as is normally required, if it determines that national security, public safety or order, or the public interest are at issue.[447] Defendants have the right to request judicial review of such searches.

The Telecommunications Authority of Singapore (TAS) governed electronic surveillance of communications until it was merged with the National Computer Board in the late 1990s and eventually became part of IDA.[448] The government has extensive powers under the Internal Security Act and other acts to monitor anything that is considered a threat to "national security." The United States State Department in 2002 stated, "Law enforcement agencies, including the Internal Security Department and the Corrupt Practices Investigation Board, had extensive networks for gathering information and conducting surveillance, and highly sophisticated capabilities to monitor telephone and other private conversations. No court warrants were required for such operations. It was believed that the authorities

---

439 "Report of the Censorship Review Committee 2003," July 2003, available at <http://www.mda.gov.sg/MDA/documents/Censorship_Review_2003.pdf>.

440 *Id.*

441 *Id.*

442 "Arts Community Says Proposed Changes to Censorship Are Largely Cosmetic," Channel NewsAsia, September 5, 2003.

443 Computer Misuse Act (Chapter 50A), available at <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=infoecon:pnr&versionid=1&infopageid=I234>.

444 Email from Sinapan Samydorai, President, Think Centre, to Patrick Mueller, EPIC Clerk, Electronic Privacy Information Center, July 2, 2004 (on file with the Electronic Privacy Information Center); *see* "Computer Misuse [Amendment] Act," ThinkCentre, November 13, 20 <http://www.thinkcentre.org/article.cfm?ArticleID=2229>.

445 Press Release, Infocomm Development Authority of Singapore, IDA and AGC Seek Views on Proposed Amendments to the Electronic Transactions Act (February 19, 2004) <http://www.ida.gov.sg/idaweb/media/infopage.jsp?infopagecategory=infocommindustry.mr:media&versionid=1&infopageid=I2695>.

446 Electronic Transactions Act (Act 25 of 1998), available at <http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopagecategory=regulation:pnr&infopageid=I1934&versionid=1>.

447 United States Department of State, Country Reports on Human Rights Practices 2000, February 2001, available at <http://www.state.gov/g/drl/rls/hrrpt/2000/>.

448 Email from Milagros Rivera to Patrick Mueller, EPIC Clerk, Electronic Privacy Information Center, July 2, 2004 (on file with the Electronic Privacy Information Center).

routinely monitored telephone conversations and the use of the Internet; however, there were no confirmed reports of such practices during 2002 or 2003."[449] All ISPs are operated by government-owned or government-controlled companies.[450] Each person in Singapore wishing to obtain an Internet account must show their national ID card to the provider to obtain an account.[451] ISPs reportedly provide information on users to government officials without complying with legal requirements on a regular basis. In 1994, Technet – then the only Internet provider in the country serving the academic and technical community – scanned through the e-mail of its members looking for pornographic files. According to Technet, they scanned the files without opening the mails, looking for clues like large file sizes. In September 1996, a man was fined USD 43,000 for downloading sex films from the Internet. It was the first enforcement of Singapore's Internet regulation. The raid followed a tip-off from Interpol, which was investigating people exchanging pornography online. Afterwards, the SBA assured citizens that it does not monitor e-mail messages, chat groups, what sites people access, or what they download.[452]

In 1999, the Home Affairs Ministry scanned 200,000 users of SingNet ISP at the request of the company looking for the "Back Orifice" program without telling the subscribers. The TAS determined that the ISP had violated no law, but nevertheless SingNet apologized for the scans and the National Information Technology Committee announced that it would create new guidelines.[453] The IDA released guidelines in January 2000.[454] Under the guidelines, a subscriber's explicit consent must be obtained before scanning can occur. The scanning must be minimally intrusive and must not intercept web browsing or electronic communications. A November 1999 study by the Singapore Polytechnic's business administration revealed 60 percent of consumers who stated they were not ready for virtual shopping cited privacy concerns.[455]

Employer monitoring of employee phone calls, e-mails, and Internet usage is also permissible under Singapore law. Under Singapore property law, workplace e-mail, telephone and computer contents are the property of the employer. Thus, if an employee loses his job because of the contents of his communications technology, he has no grounds for defense based on an invasion of privacy.[456]

In March 2000, the Minister for Home Affairs created a "Speakers Corner" based on a similar concept in London. The "Speaker's Corner" is a designated area where individuals can publicly speak without an official permit.[457] However, pursuant to Singapore's Public Entertainments and Meeting Act, speakers are required to register with the local police station and show their national ID cards or passports.[458] As a result, speech in the "Speaker's Corner" is subject to censorship. Speakers are not allowed to discuss banned topics such as race or religion. In July 2002, Chee Soon Juan, a candidate running for office, was effectively barred from running for office for discussing religion[459] Others report that Chee was banned

---

449 United States Department of State, Country Reports on Human Rights Practices 2002, March 2003, available at <http://www.state.gov/g/drl/rls/hrrpt/2002/18263.htm>. United States Department of State, Country Reports on Human Rights Practices 2003, February 2003, available at <http://www.state.gov/g/drl/rls/hrrpt/2003/27788.htm>.

450 Garry Roday, "The Internet and Social Control in Singapore," Pol. Sci. Q. Volume 113, No. 1, Spring 1998.

451 *Id.*

452 The Straits Times, September 27, 1996.

453 "ISPs To Get Guidelines On Scanning," The Straits Times, May 12, 1999.

454 "Guidelines for IASPs on Scanning of Subscribers' Computers," Infocomm Development Authority of Singapore, for IASPs on Scanning of Subscribers' January 6, 2000, available at <http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/7c22304fecdd8affc825685e0035f9eb?OpenDocument>.

455 "Not Many Ready To Cyber-Shop, Says Poll," The Straits Times, November 18, 1999.

456 "Boss is Spying on You – And He Has the Right," The Straits Times, October 10, 2000.

457 Jake Lloyd-Smith, "Singapore's Curbs on Free Speech Look Set to Stay," November 27, 2002.

458 *Id.*

459 Agence France-Presse "Singapore Opposition Leader Barred From Polls Over Religious Speech," July 30, 2002.

for actions resulting from his failure to procure the official permit for the Speaker's Corner[460] During his speech at the Speaker's Corner, he criticized the government for banning Muslim girls from wearing headscarves in schools.[461] Furthermore, law enforcement officials hold a speaker's personal information for five years.[462] Home Affairs Minister Wong Kan Seng said that the records are kept for investigative purposes to ensure that the speaker has registered.[463] The police reportedly investigated several human rights activists, who staged a peaceful rally in Speakers Corner in December 2000, for the offense of "assembly without a permit."[464]

In March 2003, the Ministry of Finance and the Central Provident Fund Board created "SingPass," the "online equivalent of the Identity Card."[465] SingPass is a single, user-created password Singaporeans must use to access electronic government services.[466] Individuals over the age of 15 may apply for SingPass, and it will be automatically issued to individuals who register for a national identity card.[467] Singaporeans can access electronic government services through the "eCitizen portal."[468]

The Government is active in some areas normally considered private, in pursuit of what it considers the public interest. For example the Government continues to enforce ethnic ratios for publicly subsidized housing, where the majority of citizens live and own their own units, designed to achieve an ethnic mix more or less in proportion to that in the society at large.[469]

In early 2001 the Ministry of Health launched MeetDoc.com, an Internet-accessible medical database.[470] MeetDoc.com holds all patients' records from all hospitals and clinics in Singapore and is available to government and private doctors in Singapore and abroad. Because records are accessible only with a patient's username and password, physicians must obtain a patient's permission before obtaining medical information.

An extensive Electronic Road Pricing (ERP) system for monitoring road usage went into effect in 1998. The system collects information on an automobile's travel from smart cards plugged into transmitters in every car and in video surveillance cameras.[471] The service claims that the data will only be kept for 24 hours and does not maintain a central accounting system. The ERP system collects tolls. Drivers attempting to circumvent the system are monitored by video surveillance cameras; 1500 summonses were issued in a six-month period in 2003-2004 for such violations.[472] Video surveillance cameras are also commonly used for monitoring roads and preventing littering in many areas.[473] In 1995, the government proposed that cameras be placed in all public spaces in Tampines, a neighborhood in Singapore, including corridors, lifts, and open areas such as public parks, car parks and neighborhood

---

460 Email from Sinapan Samydorai, President, Think Centre, to Patrick Mueller, EPIC Clerk, Electronic Privacy Information Center, July 5, 2004 (on file with the Electronic Privacy Information Center).

461 *Id.*

462 "Singapore To Get `Speakers' Corner," Asian Wall Street Journal, April 25, 2000.

463 "Keeping Records of Speakers," The Straits Times, May 9, 2000.

464 "Police Begins Human Rights Violations," ThinkCentre, January 30, 2001 <http://www.thinkcentre.org/article.cfm?ArticleID=410>.

465 "Singpass: One Password for E-Services," February 24, 2003, available at <http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/e7641f18ddbcf75848256ced003710d3?OpenDocument>.

466 "SingPass Opens the Door to E-Services," Business Times (Singapore), February 25, 2003.

467 *Id.*

468 <http://www.ecitizen.gov.sg>.

469 United States Department of State, Country Reports on Human Rights Practices 2000, February 2001, available at <http://www.state.gov/g/drl/rls/hrrpt/2001/eap/8375.htm>.

470 Edmund Tee, "Get All Your Medical Data Online," The Straits Times, February 17, 2001.

471 "You're on Candid Camera," The Straits Times, September 2, 1998.

472 "Surveillance Cameras Pick Up More Motorists Trying to Avoid ERP Charges," Channel NewsAsia, April 27, 2004.

473 "Video Cameras To Monitor Traffic at 15 Junctions," The Straits Times, March 12, 1995; "Surveillance System Set Up in Jurong East," The Straits Times, July 16, 1996.

centers and broadcast on the public cable television channel.[474] On the other hand, a man was prosecuted under the Films Act in May 1999 for filming women in bathrooms.[475]

The Banking Act prohibits disclosure of financial information without the permission of the customer.[476] Numbered accounts can also be opened with the permission of the authority. The High Court can require the disclosure of records to investigate drug trafficking and other serious crimes. The Monetary Authority of Singapore (MAS) issued new "Know Your Customer" guidelines to banks in May 1998 on money laundering. Banks are required to clarify the economic background and purpose of any transactions of which the form or amount appear unusual in relation to the customer, finance company or branch office concerned, or whenever the economic purpose and the legality of the transaction are not immediately evident.[477] Banks must report suspicious transactions to the MAS. In 2002, the Credit Bureau asked CaseTrust to accredit its procedures and systems to allay consumer financial privacy concerns.[478]

Despite the extensive and arguably invasive monitoring, most Singaporeans support placing surveillance cameras in public places, according to a 2000 survey conducted by The Straits Times. According to one respondent, "It's like your big brother is watching you all the time. But if having a big brother means that I am safe from robbers and thieves, then I don't mind." The privacy concerns were generally dismissed because, as one member of Parliament explained, "you shouldn't be doing anything embarrassing in public."[479]

The IDA launched a trial program in February 2004 to stimulate the development of ultra-wideband technology that will be used in products that "can see through walls and track vehicles or objects."[480]

In response to the terrorist attacks in the United States on September 11, 2001, Singapore strengthened its anti-terrorist efforts by passing laws that codified United Nations resolutions to punish criminally the funding of terrorist activities and the making of false terrorist threats.[481] In this respect, the Parliament passed the Terrorism (Suppression of Financing) Act in July 2002 punishing those found sheltering or dealing with the property of terrorists, and withholding financial information of terrorist acts.[482] In June 2002, Singapore proposed that Asian and European law enforcement agencies organize a system to share intelligence information to combat terrorism and organized crime.[483] In November 2003, the Computer Misuse Act was amended to allow authorities to launch pre-emptive actions against suspected hackers based on "credible information" linking the suspect to planned attacks on sensitive information networks.[484] Reporters Without Borders warned against potential abuses allowed by the amendment that allows continuous surveillance of suspects through real-time monitoring software.[485] In late 2003, Singapore's Home Affairs Minister urged countries to develop biometric-enabled passports in order to

---

474 "Do We Really Want an All-Seeing Camera?" The Straits Times, July 13, 1995.

475 "Peeping Tom Used Hidden Camera To Spy," The Straits Times, May 29, 1999.

476 Banking Act, Chapter 19, available at <http://www.mas.gov.sg>.

477 "Guidelines on Prevention of Money Laundering," Monetary Authority of Singapore, May 26, 1999, available at <http://www.mas.gov.sg>.

478 Leong Chan Teik, "New Bank Credit Bureau Will Get Accredited," The Straits Times, June 4, 2002.

479 "Eyes Wide Open," The Strait Times, April 12, 2000.

480 "Singapore to Test Technology that Sees Through Walls," Wall Street Journal, Februrary 25, 2004.

481 "Singapore Tightens Anti-Terrorist Laws," BBC News, November 13, 2001, available at <http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1653000/1653797.stm>.

482 Terrorism (Suppression of Financing) Act (No. 16 of 2002), available at <http://statutes.agc.gov.sg>.

483 "European Union/ASEM – Calls For Restraint in Middle East and Kashmir," European Report, June 12, 2002.

484 Amit Chanda, "New Singaporean Law to Enable 'Pre-Emptive' Action against Cyber-Terrorists," World Markets Analysis, November 11, 2003.

485 Reporters Without Borders, "The Internet Under Surveillance" (October 13, 2003).

"prevent terrorist from moving freely."[486] During his five-nation tour of Asia in 2004, US Secretary for Homeland Security Tom Ridge met with Singapore defense officials to "explore opportunities for closer cooperation as part of the international exchange and sharing of information and knowledge."[487]

In April 2003, Singapore added SARS to the Quarantine Act, a law that had previously been dormant for 27 years.[488] Measures taken to combat SARS included contact tracing and the thermal-imaging detection of body temperatures in public places.[489] To prevent violation of quarantine orders, the government ordered a 10-day quarantine on individuals suspected of having SARS.[490] Security officials installed security cameras into the home of individuals who had received quarantine orders and required them to appear before the camera at specific intervals.[491] In addition, officials would call the suspected individual's home as an additional check to enforce the quarantine, and his telephone company would be ordered to block any attempt to forward home phone calls to mobile phones to make sure that the individual does not leave the home.[492] The government also planned to use electronic wristbands if suspected individuals did not answer phone calls.[493] One man in Singapore was sentenced to six months in prison for "repeatedly flouting home quarantine orders."[494]

Radio Frequency Identification (RFID) first appeared in Singapore in 1988, when the Electronic Library Management System deployed a book management and checkout system featuring 120,000 RFID tags.[495] Later, in 2000, the National University of Singapore Library unveiled a multi-library system utilizing over two million RFID tags, making it the largest library RFID project in the world.[496] In 2004, the IDA announced a three-year $10 million plan to spur greater RFID use.[497] IDA committed itself to developing international RFID standards and initiated talks with United States RFID development leaders, including the Auto-ID Labs at the Massachusetts Institute of Technology.[498]

Slovak Republic

The 1992 Constitution provides for protections 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 honor 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) No one must violate the privacy of correspondence and the secrecy of other written documents and records,

---

[486] Johnson Choo, "Singapore Urges Use of Biometric Passports to Restrict Terrorists' Movements," Channel News Asia, November 21, 2003 <http://www.channelnewsasia.com/stories/singaporelocalnews/view/58376/1/.html>.

[487] "Singapore, US Officials Hold Talks on Terrorism," Xinhua General News Service, March 8, 2004.

[488] Julie Robotham, "Tougher Laws to Keep SARS Under Control," April 7, 2003, available at <http://www.smh.com.au/articles/2003/04/06/1049567566823.html>.

[489] Richard Paddock and Sonni Effron, "SARS Under Control in Singapore, WHO Says." Los Angeles Times, June 1, 2003 at A4.

[490] Chua Mui Hoong, "Govt's Sars Action Swift, But Shows Up Lack of Checks," Straits Times, May 10, 2003.

[491] *Id.*

[492] *Id.*

[493] *Id.*

[494] "Singapore Man Sentenced to Six Months in Jail for Violating Home Quarantine Orders," Associated Press Newswires, May 9, 2003.

[495] Tony Santiago, "Singapore Plunges into RFID Tags," Electrical Engineering Times, May 17, 2004, at 38.

[496] *Id.*

[497] Infocomm Development Authority of Singapore, RFID Identified as Next Growth Area for Singapore ICT Industry, press release (May 5, 2004) <http://www.ida.gov.sg/idaweb/marketing/infopage.jsp?infopagecategory=&infopageid=I2845>.

[498] *Id.*

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."[499]

The Act on Protection of Personal Data in Information Systems was approved in February 1998 and went into effect on March 1, 1998.[500] The Act replaces the previous 1992 Czechoslovakian legislation.[501] It limits the collection, disclosure and use of personal information by government agencies and private enterprises either in electronic or manual form. It creates duties of access, accuracy and correction, security, and confidentiality on the data processor. Processing of information on racial, ethnic, political opinions, religion, philosophical beliefs, trade union membership, health, and sexuality is forbidden. Special protections are provided for sensitive data, defined as data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life and conviction." Transfers to other countries are limited unless the country has "adequate" protection. All systems are required to be registered with the Statistical Office of the Slovak Republic.[502]

The Act created a new office, the Inspection Unit for the Protection of Personal Data, headed by the Commissioner for Personal Data Protection, to supervise and enforce the Act.[503] The Commissioner is appointed by the Government on the basis of a recommendation by the President of the Statistical Office. Mr. Pavol Husar took office as the first Commissioner in February 1999. The Commissioner 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 ascertained, and participates in the preparation of generally binding regulations in the field of personal data. The Commissioner is required, to file an annual report on the status of data protection with the Government and the National Council (parliament).

As of September 2001, the office had nine staff members.[504] In January 2001, the Commissioner said publicly that the act was going to be much more vigorously enforced and large fines imposed for violations, including non-registration. He noted that there were only 400 information systems registered when the number should really be around 20,000.[505] Since 2001 the Unit has received 82 serious complaints under the Act and prepared over 300 informational documents for citizens and public administration bodies on data protection issues.[506]

One of the top priorities for the Inspection Unit over the last few years has been to secure amendments to the Act on Protection of Personal Data in Information Systems in order to bring it into full compliance with the EU Directive.[507] In September 2001, a draft amendment to the Act was submitted to the Legislative Council of the government for approval. In November 2001, the Legislative Council reviewed the draft and made several recommendations and suggestions, including the establishment of a

---

499 Act No. 460 of September 1, 1992 Constitution of the Slovak Republic (September 1, 1992), available at <http://www.slovakia.org/sk-constitution.htm>.

500 Act No. 52 of February 3, 1998 on Protection of Personal Data in Information Systems, available at <http://www.statistics.sk/webdata/english/acts/act5298/act5298.htm>.

501 Act of April 29, 1992 on Protection of Personal Data in Information Systems (No. 256/92).

502 Registration is governed by the Decree of the Statistical Office of the Slovak Republic of 11 May 1998, available at <http://www.statistics.sk/webdata/english/acts/155decre/155decre.htm>.

503 Web site at <http://www.dataprotection.gov.sk/>.

504 E-mail from Natalia Krajcovicova, Inspection Unit for the Protection of Personal Data, Slovakia, to Sarah Andrews, Electronic Privacy Information Center, September 4, 2001 (on file with Electronic Privacy Information Center).

505 "Large Fines to be Imposed for Abuse of Personal Data in Slovakia," BBC Worldwide Monitoring, January 25, 2001.

506 E-mail from Natalia Krajcovicova, Inspection Unit for the Protection of Personal Data, Slovakia, to Sarah Andrews, Electronic Privacy Information Center, July 1, 2001 (on file with Electronic Privacy Information Center).

507 *Id.*

new independent supervisory authority, to be called the Office for Personal Data Protection. At the Council's request the Commissioner drafted a completely new Act to incorporate these changes and resubmitted it in December 2001. The new bill was approved by the Government and submitted to Parliament in February 2002. Many of the bill's provisions dealt with restructuring the supervisory authority. It also created new protections for the processing of sensitive information, defined as information relating to racial or ethnic origin, political views, religion or philosophical belief, membership in political parties, participation in political movements or trade unions, health, and sex life. It also places restrictions on the processing of the national identity number. The bill failed to pass into law, when in late June the President refused to sign it on the grounds that it did not clearly define the establishment of the new office. He also objected to the proposed implementation date of July 1, 2002, stating that it would interfere with the general election planned for September 2002. Under the election laws at the time, political parties were required to submit petition sheets containing over 10,000 signatures and including signatory's identity numbers (so called "birth numbers"), a requirement that would contradict the new law. On July 3, the Parliament passed an amended bill taking into account these objections.[508]

On September 1, 2002, a bill known as Act. No. 428 of July 3, 2002 on Protection of Personal Data, went into effect. The law establishes the Office for Personal Data Protection and purports to provide a higher degree of protection to the subjects of data collectors.[509] In particular, subjects of data collection are given the right to obtain a copy of his or her personal data from the controller.[510] Moreover, the law imposes new duties on controllers who are to secure better protection of personal data and to take safeguards to mitigate the risk of infringement of personal data. The law also allows the Office to publish/issue in specific situations binding statements (measures). The law enables the imposition of stricter sanctions[511] for violation of the act's provisions.[512]

The Addendum to the Report on Slovakia's Progress in its Integration into the European Union states:

> The National Council of the Slovak Republic adopted Personal Data Protection Act No. 428/2002 Coll. with effect from 1 September 2002. The Act ensures full compatibility with European Parliament and Council 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. The Act also accounts for written recommendations of Commission experts who examined the protection of personal data in the Slovak Republic.[513]

Since inception of the Office of Personal Data Protection in September of 2002 through April 30, 2003, the office received 36 complaints of data subjects. The office undertook nine inspections, issued five measures, referred two cases to criminal justice agencies, and registered 1,752 information systems.[514]

The Inspection Unit, now the "Office of Personal Data Protection," maintains close relations 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 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

---

508 "Slovak MPs Approve Personal Data Protection Law," BBC Worldwide Monitoring, July 3, 2002.

509509 Introduction of the Chairman of the Office, available at <http://www.dataprotection.gov.sk/buxus/generate_page.php3?page_id=423>.

510 *Id.*

511 For example, fines of up to USD 287,000.

512 *Id.*

513 "Addendum to the Report on Slovakia's Progress in its Integration into the EU" 38 (2002) available at <http://www.vlada.gov.sk/eu_en/>.

514 E-mail from Zuzana Babicová, Office for Personal Data Protection, Slovak Republic, to John Baggaley, Electronic Privacy Information Center, June 16, 2003 (on file with Electronic Privacy Information Center).

developments in their countries, and to establish a common website for more effective communication.[515]

Under the 1993 Police Law, the police are required to obtain permission from a court or prosecutor before undertaking any telephone tapping or mail surveillance.[516] This type of activity is supposed to be used only in cases of extraordinarily serious premeditated crimes or crimes involving international-treaty obligations. However, the communist-era secret police still remain in positions of power and over the years there have been many public revelations of illegal wiretapping of opposition politicians, reporters and dissidents.[517] In 2001 there were allegations that members of the SMK and SMER parties were being monitored and their telephones tapped.[518] Active monitoring of The Church of Scientology by the Ministry of the Interior was also reported.[519] Under the Criminal Code, police require a judicial search warrant to enter a private home and the court may only issue this warrant with good cause. Police are required to present the warrant before conducting the search or within 24 hours. There are continuing reports of Roma homes being entered without warrants.[520]

There are legal protections for privacy in the Civil Code. Article 11 states, "everyone has the right to the preservation of his personality, mainly of life and health, personal honor and human dignity as well as privacy, name and exhibitions of personal nature." There are also computer-related offenses linked with the protection of a person (unjustified treatment of personal data).[521] 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 organizations and churches, even when not necessary for prosecution, was unconstitutional. Court chairman 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."[522] Moreover, there are sector specific privacy provisions to protect an individual's medical, financial and tax records.[523] A draft new media law, containing provisions on the protection of privacy and rights of correction, is also moving forward.[524]

The Act 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.[525] 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

---

515 E-mail from Karel Neuwirt, President, Office for Personal Data Protection, Czech Republic, to Sarah Andrews, Research Director, Electronic Privacy Information Center, May 15, 2002 (on file with the Electronic Privacy Information Center).

516 Code of Criminal Procedure, Articles 86 to 88.

517 "Hungarian Politicians in Slovakia Are Being Bugged," CTK National News Wire, February 21, 1995, "Deputy Brings Charges Against Slovak Secret Services Spokesman," CTK National News Wire, August 21, 1997.

518 US Department of State Country Reports on Human Rights Practices – 2001, March 2002, available at <http://www.state.gov/g/drl/rls/hrrpt/2001/eur/8338.htm>.

519 *Id.*

520 *Id.*

521 European Commission, Agenda 2000 - Commission Opinion on Slovakia's Application for Membership of the European Union, Doc 97/20, July 15, 1997.

522 "Court Rules Law on Public Prosecutors Unconstitutional," CTK National News Wire, March 4, 1998.

523 Act No. 277/1994 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* "Data Protection Laws of the World," Christopher Millard and Mark Ford, Clifford Chance, Sweet & Maxwell 2000.

524 "Culture Ministry to Draft Own Media Law," BBC Worldwide Monitoring, February 9, 2001.

525 Act on Free Access to Information, available at <http://www.civil.gov.sk/SNARCHIV/uk_the_act_on_free_access_to_information.htm>.

power of the courts and law enforcement bodies;" or (j) identifies localities of protected animals and plants, minerals and fossils. The information requests to obligees must be disposed without undue delay, but not later than in 10 days. Appeals are made to higher agencies and can be reviewed by an administrative court.[526]

During the implementation of this Act in practice, some difficulties have been found in cases regarding appeals against decisions made by obligees that do not have their own superiors, e.g. municipalities, the National Property Fund of SR, etc. In these cases, it is not clear what is the appropriate appellate body. For example, in the case of municipalities, two different 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 only an executive body of the mayor, as well as the municipal council. On the other hand, the Act No. 369/1990 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 that is 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 more than the three years of implementing the Act on Free Access to Information, there has been no adjudication that would unify these two contradicting provisions of two different acts. Moreover, from January 1, 2003, several provisions in Act No. 99/1963 on Civil Court Procedure have changed. Among them are provisions that are important for proceedings of the court as an appellate body to the mayor's decision in matters of self-governance. The most important change is that the requester can file an appeal against the court adjudication to a higher court, a step that was not possible before. Courts have no obligatory time limit within which they must decide. The consequence of this change in the Act on Civil Court Procedure is that the process for obtaining information can be extended indefinitely while the value of the information originally requested declines in value.

There are also separate requirements for disclosure of environmental information that covers private organizations. It became effective January 1, 2001[527] and revoked Act 171/1998 of the National Council on Free Access to Environmental Information. In February 2001, the government approved a draft law on Protection of Confidential Information to harmonize the handling of classified documents with NATO standards, despite the Data Protection Commissioner's objections that it violated human rights.[528]

On May 30, 2001, the National Council of the Slovak Republic adopted Act. No. 241 on Protection of Confidential Information. Most of the law became effective in July, 1, 2001, the rest on November, 1, 2001. This Act was valid and effective until April 30, 2004, when it was cancelled and replaced by Act No. 215/2004 on the Protection of Confidential Information adopted by the National Council of the Slovak Republic on March 11, 2004. One of the most important changes brougth by this new Act is the method of creation of the Confidental information list. According to the old wording, this list was created by the National Security Authority in the form of a regulation. The wording of the new Act states that the Confidental information list is created by the head of each authority that deals with confidental 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

---

526 E-mail from Vlado Pirosik, Public Interest Lawyer, Environmental Lobbying Facility, Slovak Republic, to John Baggaley, Law Clerk, Electronic Privacy Information Center (EPIC), July 11, 2003 (on file with EPIC) (The Act on Free Access to Information stipulates the duty for obligees to provide info "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 (art. 19 para 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 they file a civil action, the proceeding is governed not by the Act on Free Access to Information, but by act 99/1963 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.).

527 Act on Free Access to Information, available at <http://www.elaw.org/resources/text.asp?ID=331>.

528 "Government Approves New Version of Law on Confidential Information," BBC Summary of World Broadcasts, March 2, 2001.

period of, change to, and extinction of, the security classification level. The information can be clasified as a confidental information only in fields stipulated by the Government of the Slovak Republic in regulation No. 216/2004.

On August 19, 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 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.[529]

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 April 18, 1939, to December 31, 1989. Specifically, the National Memory Act deals with documents concerning crimes committed on 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, humanity, or war crimes, and (iv) other retaliations for political reasons.[530]

Slovakia 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 (ETS No. 108).[531] In August 2001, it signed the Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows.[532] It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[533] Slovakia joined the OECD in September 2000.

Republic of Slovenia

The Constitution

The right to privacy appears in two forms in the 1991 Slovenian Constitution,[534] as an individual right of a private character, and as a human right, meaning that it also has a public nature.[535] 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 authorize action infringing on the privacy of the post or of other means of communication, or

---

529 E-mail from Zuzana Babicová, Office for Personal Data Protection, Slovak Republic, to John Baggaley, Electronic Privacy Information Center, June 16, 2003 (on file with Electronic Privacy Information Center).

530 *Id.*

531 Signed April 14, 2000, ratified September 13, 2000, entered into force January 1st, 2001, available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=1&DF=10/09/04&CL=ENG>

532 <http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/International_legal_instruments/Amendements%20to%20the%20Convention%20108.asp>

533 Signed February 21, 1991, ratified March 18, 1992, entered into force January 1st, 1993. <http://conventions.coe.int/>.

534 Constitution of the Republic of Slovenia 1991, available at <http://www.sigov.si/us/eus-usta.html>.

535 *Komentar Ustave Republike Slovenije* (Comments about the Constitution of the Republic of Slovenia) 369 (Sturm & Lovro eds., Ljubljana, *Fakulteta za podiplomske drzavne in evropske studije* 2002).

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."[536]

Protection of personal data

Since May 1, 2004, Slovenia is a new member of European Union, which means that all EU directives are effective in the country. Slovenia enacted in 1999 Personal Data Protection Act (PDPA) based on the EU Data Protection Directive and the Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108). In this law, private entities may process personal data only if they have obtained individuals' written consent, or if the data processing is regulated by law. Article 38 of the Constitution 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."[537]

In July 2001 a new Act[538] amending the PDPA came into force. The primary purpose of the amendment was to establish an independent oversight mechanism in accordance with the requirements of the 1995 EU Data Protection Directive. Previously supervision of the Act was conducted by a single Inspector within the Ministry of Justice. The new Act created an independent agency, the Inspectorate for Personal Data Protection (the Inspectorate) within the Ministry of Justice. Supervision of the Act is divided between the Inspectorate and the Human Rights Ombudsman. The Inspectorate began work in September 2001 and, as of July 2002, employed three persons. The Human Rights Ombudsman employs two persons responsible for data protection. The Ministry of Justice remains responsible for maintaining the database registry. The Home Policy Committee within the National Assembly also performs oversight of the Act.[539]

The PDPA is subject to supervision by inspection agencies. In the Inspectorate's 2003 report,[540] inspectors again have noted an increase in complaints (60 in 2003), which is probably the consequence of greater awareness of individuals about their rights. The majority of complaints concerned the sending of unsolicited commercial messages (via e-mail and ordinary mail)[541] and the publication of personal data on the Internet. Furthermore, the Inspectorate conducted 18 other inspections and supervisions of the implementation of the provisions of the DPDA. These inspections and supervisions were performed mostly in the field of health service, the educational system, public authority, employment, closed circuit television video surveillance, and the management of multi-occupied buildings and employment.[542]

---

[536] The means of communication are interpreted in the widest sense of the word: it may include telephone communications, e-mails, 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.* 395-396.

[537] Constitution of the Republic of Slovenia 1991, *supra*.*id.*

[538] Act Amending the Personal Data Protection Act (*Uradni list RS*, 57/01).

[539] E-mail from Joze Bogataj, Data Protection Inspector, to Sarah Andrews, Research Director, Electronic Privacy Information Center (EPIC), July 12, 2002 (on file with EPIC).

[540] Slovenian Data Protection Inspectorate, Annual Report 2003, available at <http://www.sigov.si/mp/index.php?vie=content&gr1=orgVSst&gr2=insVrsOsb#03>.

[541] General Consumers Inspector received 58 complaints about spam, but he was only able to take measures for spammers from Slovenia and not from abroad. Letter from the general consumers inspector Roman Kladošek to Matej Kovacic, Junior Researcher at the Faculty of Social Sciences, University of Ljubljana, Slovenia, June 24, 2004 (on file with EPIC).

[542] E-mail from Joze Bogataj, Data Protection Inspector. Slovenian Data Protection Inspectorate, to Cedric Laurant, Policy Counsel, EPIC, July 2, 2004 (on file with EPIC).

1,025 Database administrators have registered in the Joint personal data catalogue, the register of all databases containing personal data, which is within the competence of Ministry of Justice.[543]

The PDPA applies the principles contained in Convention No. 108. The Convention and the PDPA provide that everything that is not explicitly allowed in connection with personal data collection and processing is prohibited. The first version of the PDPA was enacted in 1990, with amendments dating from 1999 and 2001. Public entities may only process personal data for which they have been granted legal authorization, 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 authorized 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.

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, defense, 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 to the individual free of charge within fifteen days of receiving his or her request, as well as provide a copy of an individual's personal data within thirty days of receiving the request. If a data controller fails to fulfill 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 individualís request, the list of recipients within a thirty days deadline.

If an individual provides evidence that his or her personal data were gathered in breach of the law, the data controller must delete these 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" which is defined as data on racial or other origins, political, religious or other beliefs, trade union membership, sexual behavior, criminal convictions and medical data. This data must be specially labeled 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 adequate with the Slovenian one.

Some experts argue that the current data protection legislation is probably too strong for use on the Internet, because the PDPA requires that the private sector be able to process personal data that are not covered in the law only with an individual's written consent, which is not an easy obligation to fulfill in practice, particularly in the case of the Internet.[544] An amended version of the PDPA would replace the requirement of a written consent with unambiguous consent regardless of its form is still being debated in Parliament.

---

543 *Id.*

544 Article 15 of the Electronic Commerce and Electronic Signature Act, enacted in June 2000, stipulates that a so-called secure electronic signature, one which is confirmed by an authenticated certificate, is equivalent to a signature in one's own hand.

Video surveillance

Video surveillance, which was unregulated in the past, is now covered in the new Private Protection Act which was enacted in November 2003. Article 43 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 EUR 12,500.

Privacy of communications

The right to privacy of communication is guaranteed by the Constitution 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 unauthorized 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 unauthorized acquaintance with the content of a message transmitted by telephone or other telecommunications equipment, as well as the unauthorized forwarding of someone's letter to a third party. Article 151 further prohibits the publication of private communications without consent by the authorized 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).

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 which 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 authorized under very special circumstances by a General Police Director.[545] 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.

Electronic communications

On May 1st, 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

---

[545][5] Article 49, Law on the Police, 18 July 1998.

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 (Article 104). 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 (Article 106).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 defense, and the director of SOVA (Article 107).

On June 1st, 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 about 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.[546] Since these expenses are estimated to be between EUR 100,000 and EUR 700,000 per operator, small ISPs have 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 center to decrease the costs per operator.[547] 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 Penal Code

The Penal Code specifies sanctions for an invasion of territorial privacy in Articles 149 and 152. Article 149 prohibits unauthorized 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 unauthorized entry into, or search of, private facilities, or an attempt to do so. Intrusion into a computer system is the subject of Article 242 of the Penal Code, but according to this article, 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.[548] Furthermore, Article 154 of the Penal Code 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 unauthorized 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.

Miscellaneous developments

Police has a right to take a picture, fingerprints and saliva samples from suspects, as provided by Article 149 of the Criminal Proceeding Act. Police can use DNA samples for criminal investigations.

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 EUR 420.

---

[546] Not all Slovenian ISPs are members of SISPA.

[547] Proceedings from the meeting: Ministry of Information Society, Realisation of lawful interception of telecommunications traffic which flows over the Internet, June 1st, 2004 (on file with EPIC).

[548] 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.

Slovenia is included in the US visa waiver program and is required to produce biometric passports. However, due to technical and institutional ambiguities, authorities declared that biometric passports could not be produced until 2006.

Other regulations partially or indirectly relate to privacy. Unlawful invasions of the privacy of communications are prohibited and sanctioned. The Electronic Communications Act deals with surveillance and confidentiality of telecommunications. A court order is always required, but the legislation follows EU trends by requiring that telecommunications service providers gather extensive information. An ordinance about interfaces and software for lawful interception of telecommunications, adopted under the former Telecommunications Act, is still effective and requires from mobile operators to supply on request information about the location of a mobile telephone user. The Electronic Communications Act requires operators to provide the location of a device that has been used to make a call to emergency numbers (Article 72).

The Law on National Statistics regulates the privacy of information collected for statistical purposes.[549] In July 2000, the Health Insurance Data Collections Act came into force. The Act sets out restrictions on the collection, use and exchange of health data.[550]

Article 50 of the Postal Services Act prescribes that providers of postal services should enable an authorized 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.

The revised Consumer Protection Act (CPA) that was enacted in January 2003 incorporates the EU E-Commerce Directive (2000/31/EC). Article 45a states that companies (*e.g.*, direct marketing companies) may use the automatic telephone dialing system only with consumer's previous consent. The same is true for fax messages and e-mail 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 EUR 4,200 for physical persons and EUR 12,600 for companies. The CPA only protects individuals, but the Electronic Communications Act of 2004 also protects companies from receiving spam (Article 109).

The Labor Relations Act prohibits employers to ask employees or employment candidates questions about family matters, marital status, pregnancy, family plans or other information which is not work-related[551]

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.[552]

Probably one of the biggest recent privacy abuses took place in April 2003. Someone set up a website (www.udba.net) and published the personal data of about 1.5 million individuals from Slovenia (almost the whole population of the country). The information published was part of archives of the previous communist regime's secret service (the UDBA), later renamed National Security Service (SDV). In that archive (called "Central Active File") were persons' names, surnames, dates of birth, nationalities, secret

---

[549] Law on National Statistics, July 25, 1995.
[550] *Id.*
[551] Article 26 of the Labor Relations Act.
[552] Article 5 of the Criminal Proceedings Act.

service dossier number, and all criminal offenses that a person had only been suspected of. The persons listed were not only SDV agents, but also individuals who came in contact with the repressive organs of the previous communist regime: political opponents, traffic offenders, criminals, and even people who were just put under surveillance because of their employer's request. Among them were prominent politicians and public persons. On April 17, 2003, the Inspector for Personal Data Protection ordered Slovenian ISPs to block access to the udba.net web site. In a few days almost all the media had published how to avoid the blocking and started a wide public debate about Internet censorship. Some legal experts also claimed that the Inspector's action was unlawful,[553] because it ordered ISPs to block the access to, rather than close, the controversial web site. The Inspectorate's decision was motivated by the fact that the website is not located on a server based in Slovenia but in a country (Thailand) over which the Inspectorate does not have any jurisdiction. After a few days the Inspectorate repealed its order, explaining that it could not be enforced, and was void as a result. Regardless of the fact that the Inspectorate's action has probably been problematic in a legal sense, because inspectors ordered ISPs to block the access and not shut down the web site itself,[554] and despite the censorship debate it is obvious that there has been a great abuse of individuals' personal data.

In 2003 A Slovenian business journal sold CD-ROM containing e-mail addresses of Slovenian Internet users. Despite critics of such practice, the addresses had been collected from public sources. The Slovenian search engine Najdi.si is also collecting e-mail addresses. To allay critiques the web site enables individuals to remove their e-mail addresses from the database and took technical measures to prevent automatic harvesting of addresses by spider bots.

An international study (SIBIS2003) showed that the concern for privacy/confidentiality and also for data security among Internet users is relatively low in Slovenia if compared to 25 EU countries and the US.[555]

Past cases of importanceIn late 1998, a Slovenian journalist Tomaz Ranc wrote some articles based on confidential information. Police obtained a list of phone numbers he had dialed and a list of the telephone numbers of the people who called him to identify his sources of confidential information. The police obtained that list without court order. Ranc then complained and the court ruled that authorities had violated his human rights when they had attempted to establish his sources by acquiring the list of the telephone numbers he had called.[556]

It was reported in October 2001 that, in response to the September 11, 2001 attacks on the United States, the SOVA began monitoring the e-mails and telephone communications of prominent academics and NGO activists.[557] In June 2002, the Parliamentary Commission for the Supervision of Work of Security and Intelligence Services started inquiring into allegations that the Slovene police and SOVA were secretly wiretapping Peter ČCeferin, the lawyer of a man accused of human trafficking.[558] The same lawyer has been the target of secret observation in the beginning of 2004 when he met with a person, which should have performed polygraphic tests on Ceferin's client. The results of observation were sent to a prosecutor who tried to exclude the polygraphist. After a complaint and the publication of the case,

---

553 Makarovic Bostjan, *Ali in kako lahko drzava pravno ureja dogajanje na internetu?* (May the state regulate the Internet and how?) *Informatika in pravo* (Information Technology and Legal Issues) 4 (2003).

554 *Id.* The author claims that ISPs are not processing personal data, because they just provide access to the data, although they are not aware of the content of the data. However, since the problematic website is located outside Slovenian jurisdiction, it seems that the Inspectorate has no legal instrument to sanction that kind of a violation.

555 Vasja Vehovar, Bojana Lobe, Matej Kovacic, Confidentiality concern and on-line shopping. (Paper prepared for the "Consumer WebWatch and Consumers International First International Workshop and Roundtable on Web Credibility: Building Trust on the Web," Ljubljana, June 8-9, 2003 <http://www.ris.org/uploadi/editor/vehovar_paper_consumersinternational.doc>.

556 UNPAN report about Slovenia, available at <http://unpan1.un.org/intradoc/groups/public/documents/nispacee/unpan007961.pdf>.

557 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://www.ihf-hr.org/reports/AR2002/country%20links/Slovenia.htm>.

558 "Slovene Inquiry Commission Investigates Wiretapping Allegations," BBC Worldwide Monitoring, June 28, 2002.

the police said they received an anonymous denunciation. It turned out that the person performing the observation was a policeman who was not on duty at the time and was presumably acting as a private citizen. There were also questions as to whether SOVA had been secretly wiretapping some political activists for political purposes.[559]

Access to public information

Every person has the right to acquire information held by a public body (Article 39 of the Slovenian Constitution). In 2003 the Access to the Public Sector Information Act (APSIA) 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 of charge insight into public sector information and costs of transcript are limited only to material costs. All public sector information must also be provided on the Internet (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. The catalogue includes almost all government institutions. However,SOVA is not included, even though that agency is probably is directly bounded to APSIA.[560]

Since Slovenia has a Deputy for Access to Public Sector Information, there have been intense discussions about the right to be informed versus the right to privacy. A lot of public discussions revolved around the decision to block access to the udba.net web site. At the end of 2003, the Inspector for Personal Data Protection suggested police representatives to stop providing information which will make identification of suspects possible to the public, since there is no legal basis for the release of that information.[561] In practice, it means that the police may only provide information about the event, its location and the age of the persons involved, but no more initials of their names. That decision provoked several protests from journalists and reporters, who used that information for criminal stories.

International obligations

Slovenia is a member of the Council of Europe (CoE) and has signed and ratified Convention No. 108.[562] It has also signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms.[563] In May 2004 Slovenia ratified the CoE Convention on Cybercrime[564] and the Additional Protocol with provisions against racism and xenophobia in virtual networks.[565]

---

559 Professor Mocnik from the Faculty of Arts, University of Ljubljana, Slovenia, recently wrote a public protest based on information published on June 7, 2003 in one of the main newspapers in Slovenia (DELO). The article asserts that the Parliamentary Commission for Supervision of Security and Intelligence Services has been secretly informed about the activities of various Slovenian extremist and militant anti-globalization groups. Professor Mocnik remarks that Slovenian anti-globalization groups are not militant and violent, since all their protests have been peaceful and without a single riot, although anti-globalization groups are strongly opposing current Slovenian foreign policy, and have a remarkable influence on the public opinion and the media. Professor Mocnik concludes that the SOVA surveillance is probably politically motivated <http://www.mladina.si/tednik/200324/clanek/kolumna/>.

560 A representative from the Ministry of Information Society said it has been explicitly requested that SOVA be excluded from the catalogue (which has been adopted by the government), although this request is probably illegal (Mail from Klemen Ticar, Ministry of Information Society to Matej Kovacic, Junior Researcher at the Faculty of Social Sciences, University of Ljubljana, Slovenia, July 8, 2004 (on file with EPIC).

561 Mail from Jože Bogataj, Data Protection Inspector to Matej Kovacic, Junior Researcher at the Faculty of Social Sciences, University of Ljubljana, Slovenia, February 12, 2004 with press release of inspektro from January 15, 2004 in an attachment (on file with the Electronic Privacy Information Center).

562 Signed November 23; 1993; ratified May 27, 1994; entered into force September 1, 1994.

563 Signed May 14, 1993; ratified June 28, 1994; entered into force June 28, 1994.

564 Convention on Cybercrime (CETS No.: 185), available at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&CL=ENG>.

565 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>.

Republic of South Africa

Section 14 of the South African Constitution of 1996 states, "Everyone has the right to privacy, which includes the right not to have – (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed." Section 32 states, "(1) Everyone has the right of access to – (a) any information held by the state, and; (b) any information that is held by another person and that is required for the exercise or protection of any rights; (2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."[566] The interim Constitution contained equivalent provisions to Section 14 and Section 32.[567]

The South African Constitutional Court has delivered several judgments on the constitutional right to privacy. These deal with legislation prohibiting the possession of indecent or obscene photographs[568] and child pornography,[569] searches and seizures[570] and the criminalization of prostitution.[571] The court's interpretation of the right is a mixture of US and European jurisprudence. On the one hand, the court has emphasized that the roots of the right lie in the value of human dignity.[572] On the other hand, the court has defined the right, along US lines, as protecting an actual (or subjective) expectation of privacy that society is prepared to recognize as reasonable.[573]

The constitutional right to privacy also has application in private litigation.[574] Recent decisions have considered the effect of the right in litigation seeking to prevent the publication of intimate photographs of a quasi-celebrity,[575] and an action for damages to compensate for publication of an inaccurate report that a person had been arrested for terrorism.[576]

There is currently no general statutory protection of privacy or general data protection legislation in South Africa.

In early 2000, the South African Law Reform Commission was requested by Parliament to investigate the introduction of privacy and data protection legislation. The impetus for the request was Parliament's consideration at the time of the Promotion of Access to Information Act (the Act). Drafts of the Act contained a chapter proposing the regulation of access to, and dissemination of, personal information held in private and public "data banks." Parliament took the view that these matters would be better regulated by a comprehensive purpose-specific statute and the chapter was removed from the Access to

---

566 The Constitution of the Republic of South Africa, Act 108 of 1996, available at <http://www.info.gov.za/constitution/1996/96cons.htm>.

567 Section 13 and 23 of the *interim* Constitution (Act 200 of 1993). The Constitutional Court's jurisprudence interpreting the privacy right in the *interim* Constitution remains authoritative for the right in the 1996 Constitution. The *interim* Constitution's access to information right was however confined to information held by organs of state. The *interim* Constitution was in force between April 1994 and February 1997.

568 Case v. Minister of Safety and Security 1996 (3) SA 617 (CC) (wide and vague apartheid-era prohibition on possession of pornography a violation of right to privacy). All judgments of the South African Constitutional Court are available online at <http://www.concourt.gov.za>.

569 De Reuck v. Director of Public Prosecutions (Witwatersrand Local Division) 2004 (1) SA 406 (CC) (justifiable to limit the right to privacy to protect children from the exploitation and degradation inherent in child pornography).

570 Bernstein v. Bester NO 1996 (2) SA 751 (CC); Mistry v. Interim National Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC).

571 S v. Jordan 2002 (6) SA 642 (CC) (no significant privacy interests in the act of prostitution).

572 S v. Jordan, *supra* para 81.

573 Bernstein v. Bester *NO* 1996 (2) SA 751 (CC) para 67. Judgments of the South African Constitutional Court are available at <http://www.concourt.gov.za>.

574 The South African Bill of Rights has both direct and indirect application in so-called "horizontal" disputes (disputes not involving state actors or legislation).

575 Prinsloo v. RCP Media Ltd t/a Rapport 2003 (4) SA 456 (T) (injunction available to prevent publication of purloined photographs of notorious surgically-improved Pretoria lawyer).

576 Independent Newspapers Holdings Ltd v. Suliman (Supreme Court of Appeal, 28 May 2004) (no privacy interests in information and photographs of person publicly arrested at airport).

Information Act as finally enacted. The Law Reform Commission, having researched the matter, then published an Issue Paper on Privacy and Data Protection in August 2003.[577] The Issue Paper makes a number of preliminary recommendations that closely track the provisions of the European Union (EU) Data Protection Directive. This is to be expected since the Directive, by requiring a basic level of data protection in countries doing business with the EU, is an important impetus for the law-reform initiative. The Commission recommends that legislation be enacted to govern the collection, use and dissemination of personal information in both the public and private sectors, and calls for the creation of a specialized Commission. The Commission is likely to complete its work in the first half of 2005, and the legislative process is likely to take at least a year after that.

The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (the Interception Act) is the end-product of several proposals of the Law Reform Commission. In November 1998, the Commission recommended amendments to facilitate the monitoring of cellular phones and Internet Service providers (ISPs).[578] On July 18, 2001, a Bill was introduced into Parliament, proposing the repeal and replacement of the Interception and Monitoring Prohibition Act 127 of 1992. According to Mr Johnny de Lange, Chairperson of the Parliament's Portfolio Committee on Justice and Constitutional Development, the Bill "aims to regulate the interception and monitoring of certain communications . . . to regulate authorized telecommunications monitoring," and "to prohibit the provision of certain telecommunication services which do not have the capacity to be monitored."[579] Following 18 months of limited consultation with stakeholders, the Interception Act was enacted and entered into force in December 2002.[580]

The passage of the Interception Act had initially been delayed, pending finalization of the Council of Europe Convention on Cyber crime, which, if ratified, would require member states and non-member signatories to enact measures consistent with the Convention.[581] South Africa is one of four non-member signatories to the Convention, along with the United States, Canada and Japan.[582] The Interception Act conforms to the requirements of the Convention.

The Interception Act was considered and passed as several unathorised surveillance incidents had come to light in the last few years. In 1996, it was revealed that the South African Police Service had been monitoring thousands of international and domestic phone calls without a warrant.[583] The opposition Democratic Party announced in November 1999 that it had found surveillance devices at its parliamentary offices and national headquarters.[584] In February 2000, the government apologized to the German government after the media reported that an intelligence operative had placed spy cameras outside the German Embassy.[585]

---

577 Available at <http://wwwserver.law.wits.ac.za/salc/issue/issue.html>. An Issue Paper is the first stage in the Commission's law reform process. It consists of a document identifying the broad issues for consideration in the development of new legislation and requesting public comment on these issues. The second stage is reached when a Discussion Paper is published, containing draft legislation. This is only published to seek comment and the process is completed by the publication of a Report which contains the Commission's recommendations to the Cabinet on draft legislation.

578 Discussion Paper 78 (Project 105), Review of Security Legislation, The Interception and Monitoring Prohibition Act 127 of 1992 (November 1998), available at <http://www.law.wits.ac.za/salc/discussn/monitoring.pdf>.

579 Adv. Johnny de Lange, Press statement, available at <http://www.polity.org.za/govdocs/pr/2001/pr0718c.html>.

580 No. 70 of 2002.

581 Specifically, Chap. II; Art. 3, Council of Europe, Convention on Cybercrime. ETS No.: 185.

582 Signed November 23, 2001.

583 "Newspaper Uncovers `Unlawful' Tapping by Intelligence Units," The Star, 21 February 1996.

584 "Democratic Party Outraged by Bugging of Its Offices," Africa News, November 23, 1999.

585 "South Africa Admits to Spying on German Embassy," Reuters, February 6, 2000.

The purpose and essence of the Interception Act remains similar to all previous versions. The Act prohibits wiretaps and surveillance, except for law enforcement purposes. It requires that all telecommunications services, including ISPs, make their services capable of being intercepted before they could offer them to the public. There is a provision for the Minister to exempt ISPs from these provisions. However, while exemptions can be made from the requirement to enable a network for surveillance purposes, ISPs that are exempt will be required to contribute to a fund which will be used to purchase centrally held surveillance equipment. This equipment will be used on a rotational basis as needed by smaller ISPs who are required to comply with a surveillance request by law enforcement.

Generally, providers will be required to pay for the costs of making their systems wiretap-enabled. No model of cost sharing is proposed at this stage and the state will be responsible for the costs of connecting central interception centers to telecommunications providers. Criminal penalties are also included should a service provider refuse to comply with the provisions of the Act or assist law enforcement. Repeat offenders may in addition face the revocation of their service license granted under the Telecommunications Act.[586]

Several amendments made by Parliament during the consideration of the Interception Act widened the scope of the legislation. The definition of "communication" has been augmented to include all "direct" and "indirect" communications, which together cover all traffic, signaling and other call related information, as well as the content of such communications. Amendments include: an expanded list of grounds for obtaining a wiretap order; including a wiretap to ascertain the location of a person in the case of an emergency;[587] an expanded range of interception directions that can be granted,[588] such as decryption orders;[589] and an augmented list of offences under the Act,[590] which includes being in possession of a stolen cellular phone and failure to report a stolen, lost or damaged SIM (Subscriber Identity Module) card.

Provisionson data retention require all telecommunication service providers (TSPs) to gather detailed personal data on individuals and companies (including photocopies of identity documents) before signing contracts or selling SIM cards for pre-paid mobile services. Provisions require that such data is made available to law enforcement agencies when requested to. There is no limit specified for the length of time TSPs are required to retain personal data, but a requirement to store communication-related information is currently limited in duration to 12 months.

The Minister has several broad powers in the Interception Act, including the discretion to stipulate all technical and security requirements for networks to be capable of surveillance, including capacity, the systems to be used, the facilities and devices to be acquired, and the type of communication-related information to be stored. At this stage, consultation in developing these standards appears to be limited to the Minister, other relevant ministers and TSPs. There is no provision for public interest or technical bodies to be consulted.

---

586 Act No. 103 of 1996, as amended.

587 Section 8.

588 These include: broad interception direction; an archived communications direction (any communication related information in the possession of a telecommunications service provider (TSP) and which is being stored by that TSP for up to one year, regarding the transmission of the indirect communication) and real time (real time information on an ongoing basis without interception) or supplementary direction, or a combination thereof. Also on application are entry warrants (to rig premises and intercept postal articles) and decryption directions. All can be obtained as oral directions when urgent circumstances prevail.

589 Section 21.

590 Chapter 9.

The National Intelligence Agency (NIA) announced in February 2000 that it was creating a signals intelligence service based on the model of the United Kingdom's GCHQ.[591] The NIA will have the authority to intercept all postal, telephone and Internet communications under the auspices of crime control and national security, actual or potential threats to public health and safety, and to assist foreign law enforcement agencies with interception regarding organized crime or terrorism, under a mutual assistance agreement.[592] In January 2004, the Department of Communications put out a tender calling for proposals by technology firms to create interception centres to intercept, monitor and store email and cellphone messages.[593]

While the Act is in the early stages of implementation, several problems are beginning to emerge. Various operational requirements appear impractical and seem not to be implementable. For example, a requirement that before an Internet service contract can be concluded, ISPs are required to verify the identity of the subscriber. As many Internet users subscribe online, this creates many difficulties. Moreover, ISPs now have to verify identities and retain copies of identity documents.

Other problems pertaining to technical network issues are emerging and the Department of Communications has set up a working group with industry to examine these issues. At the time of writing, various directives were in the process of being discussed to clarify implementation difficulties.

The Electronic Communications and Transactions Act (ECTA) has been in operation since August 2002.[594] The main purpose of the Act is to facilitate e-commerce by creating legal certainty and promoting trust and confidence in electronic transactions. It provides for functional equivalence of electronic documents, recognition of contracts, digital signatures, electronic filing and evidence etc.[595] The Act also contains statutory provisions on cybercrime and creates several computer crime offences. These include: unauthorized access to data; interception of, or interference with data; computer related extortion; fraud, and forgery[596] aimed at interfering with commercial activities and hacking. Other provisionsrestrict ISP liability;[597] promote consumer rights; criminalize spam and require all websites engaged in "offering goods or services for sale, for hire or for exchanges by way of an electronic transaction" to provide information about the security and privacy policy of the website.[598] Websites that collect personal information may voluntarily subscribe to certain principles in the Act intended to protect a person's privacy, but are not required to do so.

Chapter II of the ECTA directs the Minister of Communications to develop a national "e-strategy" within two years of the commencement of the Act. Amongst the matters to be addressed by the e-strategy are the closing of the "digital divide" through programs aimed at providing Internet connectivity to disadvantaged communities and encouraging the private sector to initiate schemes to provide universal access.

---

591 "South Africa to Set up Signals Intelligence Centre," Reuters, February 7, 2000.

592 Section 13(5).

593 "Plans for Spy Centres Sought," Business Day, January 6, 2004.

594 Act 25 of 2002. Available at <http://www.info.gov.za/gazette/acts/2002/a25-02.pdf>.

595 Chapter III.

596 Chapter XIII.

597 By incorporating notice and take down procedures; mere conduit recognition and safe harbor provisions. Liability will only attach where an ISP has direct knowledge of illegal or objectionable material and fails to take effective action as required by law.

598 The Act does not require websites to have a security or privacy policy, however, nor does it prescribe what such a policy should contain. If a website does happen to have a policy, it is usually based on the codes of conduct of various associations in the data collection sector.

The ECTA provides for the registration of all cryptography providers and services and government accreditation of authentication providers. A new "cyber inspectorate" will monitor websites and public information systems and investigate complIaince by cryptography and authentication providers.[599]

Included in the ECTA is a provision authorizing the Minister to declare both public and private databases critical in the "national interest" or the "economic and social well-being of South Africa." Once declared, the Minister can require the database to be registered, including all information about its location and the types of data stored. The law also authorizes the Minister of Communications to determine technical standards and set procedures for the general management of critical data bases, their security and disaster recovery procedures.[600]

South Africa does not have a data protection authority but has a Human Rights Commission (HRC), which was established under Chapter 9 of the Constitution. The HRC's mandate is to protect, and investigate infringements of, the fundamental rights guaranteed in the Bill of Rights, and to take steps to secure appropriate redress where human rights have been violated. The Commission has limited powers to enforce the Promotion of Access to Information Act.[601]

South Africa has a well-developed financial system and banking infrastructure. Despite the sophistication of the financial sector, the privacy of financial information is weakly regulated by a code of conduct for banks issued by the Banking Council. The current Code (in place since 2000) has recently been revised and will be replaced with effect from October 1, 2004.[602] Adherence to the Code is voluntary and it is expressly declared to be not legally binding. Financial institutions subscribing to the Code undertake not to share personal information of their clients without consent except in the public or "where [banks'] interests require disclosure'. Information may be disclosed to third-party credit risk management services with prior consent, or after notice to the client.

Important new legislation – the Financial Intelligence Centre Act 38 of 2001 aimed at preventing money laundering was passed by Parliament in 2001 and the bulk of its provisions came into effect in 2003. Along the lines of similar legislation in other jurisdictions, the Act creates the Financial Intelligence Centre, a supervisory and investigative body that receives and analyzes information regarding suspected money-laundering activities supplied to it by financial institutions, and disseminates reports to the criminal investigative authorities, the intelligence services and the revenue service. Banks and other financial institutions are required to verify the identity of their customers, must maintain a considerable body of information about customers and their transactions, and must report suspicious transactions to the Centre.

The weakness of banks' data security measures were exposed in a well-publicised case of identity-theft during 2003. A hacker was able to gain access to the account and password details of the Internet banking accounts of a number of bank customers, using commercially available keystroke-logging spyware. The publicity given to the case -- unusual, since banks usually keep bank fraud cases confidential – resulted in upgrades to security by most commercial banks offering Internet banking services.[603]

---

[599] Inspectors are given investigative, search and seizure powers, subject to obtaining a warrant (which may be issued by any court). They may also exercise these powers without a warrant if they have reason to believe that a warrant would be issued to them on application, and if delaying the search to obtain a warrant would defeat its purpose.

[600] Chapter XI.

[601] Act No. 2 of 2000.

[602] *See* <http://www.banking.org.za>.

[603] "Hacker Cleans out Bank Accounts," Sunday Times, July 20, 2003.

Credit bureaux are currently self-regulated by a Code of Conduct administered by the Credit Bureau Association (CBA). After the government's Consumer Affairs Committee investigated into the ability of the CBA to enforce its code, the government has proposed legal regulation of the industry. The draft regulations were published for comment in April 2003. They propose strict limitations on the types of information that may be held by credit bureaux, and the period of time for which information can be held. They also require access to credit information by consumers to ascertain the accuracy of the information credit bureaux hold on them, and to require procedures to allow them to dispute it.[604]

The Cabinet approved a plan in March 1998 to issue a multi-purpose smart card that combines access to all government departments and services with banking facilities. In the long term, the smart card was intended to function as passport, driver's license, identity document and bankcard, linked to fingerprint information.[605]In 2003, a commission recommended major changes to the conceptualization of the project. In February 2004, the report of the transaction advisors on the feasibility of procuring the new identity document through a public private partnership recommended against the partnership. The procurement process and form of the new identity document are therefore still uncertain.

In 2004, the Department of Home Affairs began a pilot programme to issue 30,000 smart cards to refugees (persons granted political asylum). In the Department's view, this programme is an initial step towards a planned rollout of six million smart cards per year over a five-year period. The full program entails the conversion of 30 million paper-based sets of records into the Department's electronic document management system. The government agency aims to eventually produce "an integrated biometric database of all people the Department deals with – citizens, residents, refugees, illegal foreigners."[606]

The Promotion of Access to Information Act (PAIA) came into operation on March 9, 2001.[607] The Act is a general freedom of information legislation, modeled on the FOI laws of the United States and Commonwealth jurisdictions. It is however unusual and ground-breaking in at least two respects. First, it is based on, and backed up by, a specific constitutional right of access to information, entrenched in the Bill of Rights.[608] Secondly, this right, and as a consequence, the Act, is applicable not only to information in government hands but also to information held in the private sector.[609] There is no competent Commission to monitor the implementation of the Act or to provide dispute-resolution services. Instead, the South African Human Rights Commission is charged with monitoring the use of the Act, publicizing the rights that it creates, assisting members of the public to make requests, conducting research and publishing explanatory material about the Act. Disputes over alleged maladministration of the Act (*e.g.*, requests for information not answered, indexes of records not submitted as required by the Act) can be heard by the Public Protector (the South Africa's Ombudsman). Disputes over the substance of a refusal of a request for information are resolved by way of an application to the ordinary courts.[610]

Concern has been expressed from various quarters (including the Human Rights Commission) about the ineffectiveness of the Act's dispute resolution processes. Litigation is widely recognized as being too

---

[604] The draft regulations are available at <http://www.info.gov.za/gazette/notices/2003/24738b.pdf>.

[605] "Smart Cards to Replace ID Books in SA in 2001," Africa News, February 1, 2000.

[606] Deputy Minister of Home Affairs, Malusi Gigaba: Home Affairs Department Budget Vote 2004/2005.

[607] Act 2 of 2000.

[608] Section 32 of the 1996 Constitution. The section grants a right of access to "any information held by the state" and to "any information . . . held by another person and that is required for the exercise or protection of any rights."

[609] "Concerns Raised over Access to Information Act," Mail & Guardian, May 10, 2001.

[610] Application can be made either to the High Court or to a magistrates' court. The courts have wide powers to inspect the disputed records and to order disclosure of records.

inaccessible and cumbersome to be an effective way of enforcing the freedom of information rights in the Act and in the Constitution.[611]

On paper, the Act grants extensive freedom of information rights. However, it is more difficult to assess the effectiveness of these rights in practice. First, because the Act is not yet completely operational. It will not be possible to draw accurate conclusions about the success or failure of the Act until "manuals" (indexes of records)[612] are published.[613] Second, because a vital resource for researchers - the statistics on the use of the Act, to be compiled by the Human Rights Commission - have not yet been published. There are no comprehensive empirical studies available on the implementation of the Act. In the absence of such studies, much of the evidence available to researchers is anecdotal. Requesters have reported that PAIA requests are often dealt with extremely slowly or, more troublingly, are simply ignored.[614] There appears to be widespread ignorance of the requirements of the Act, and even of its existence, in the public sector.[615]

However, there have been a number of high profile cases involving use of PAIA. For example, the leader of the Opposition made a successful request to the Presidency and the Ministry of Justice for records relating to a number of controversial presidential pardons of prisoners who had been refused amnesty by the Truth and Reconciliation Commission.[616] One of the most active users of the Act – the South African History Archive (SAHA), a NGO which collects and archives apartheid-era documentation – has retrieved large quantities of classified material from military archives and documents collected by the Truth and Reconciliation Commission. While SAHA has had some important victories, the organization suggest that use of the Act has been limited because the culture of freedom of information has not taken root yet and because PAIA has been poorly publicized.[617] The Institute for Democracy in South Africa has lauched a campaign to use the access rights granted by the PAIA to require political parties to disclose the sources of their funding.[618] Predictably enough, the requests for this information were not met with transparency by political parties, and the organization has begun a court process to test the principles at stake.[619]

There appears to have been little use by requesters of the private-sector provisions of the Act, but the extent to which the Act has had an impact on the private sector is almost impossible to measure.[620] Certainly, the Act's requirements that private bodies publish indexes of their records have so far largely been ignored.[621]

---

611 "Information Law not Accessible to Public – HRC," Business Day, February 3, 2004.

612 The "manuals", or indexes of records, are intended to provide essential guidance for requesters about how to make a request and what can be requested from a particular body.

613 The deadline for public and private bodies to submit manuals has been extended on three occasions and is currently August 31, 2005.

614 "Few Groups Aware of Act on Access to Information," Business Day, October 14, 2002.

615 A survey conducted by the Open Democracy Advice Centre revealed that 54 per cent of the public bodies contacted by the Centre were unaware of the Act, 16 percent were aware of the Act but did not implement it and only 30 percent were aware of it and implementing it. "Few Groups Aware of Act on Access to Information," Business Day, October 14, 2002.

616 "Leon Set to Get Data on Pardons," Business Day, October 15, 2002.

617 *See* <http://www.wits.ac.za/saha/programme.htm>.

618 Political party funding is currently unregulated in South Africa. There are no limits on the amounts of funding a party can receive, nor are there any disclosure requirements.

619 *See* <http://www.idasa.org.za/pdf/1043.pdf>.

620 The Human Rights Commission's duty to compile statistics on the use of the Act applies only with respect to requests made to public bodies.

621 Widespread failure by both public and private bodies to comply with the Act's publication requirements resulted in the Minister of Justice granting a six-month extension on the Act's deadline for complIaince until February 2003, a second extension until August 2003 and a third (ostensibly "final") extension until August 2005. Missing from the Act is a sanction for non-complIaince with this requirement. Legislation introduced in the Parliament during 2003, but not yet enacted, proposes to correct this by granting a power to the Minister of Justice to prescribe a penaly of up to two years' imprisonment for failure to produce a manual as required by the Act. *See* the Judicial Matters Second Amendment Bill 41 of 2003.

Even before September 11, 2001, South Africa had been revising its anti-terrorism laws. A draft anti-terrorism Bill was tabled for debate in Parliament and was the subject of public hearings at the Portfolio Committee on Safety and Security. The Bill was widely criticized as unconstitutional for its far ranging provisions with regard to personal freedoms, detention, bail and wide police search and seizure powers.The proposed Bill initially defined an act of terrorism as "an unlawful act committed in or outside the Republic" while a "terrorist organization" was defined as "an organization declared as such by the Minister of Safety and Security and which is likely to intimidate the public or a segment of the public, or is likely to carry out a convention offence."[622]

This broad definition of a "terrorist" and "terrorist organization" could extend to legitimate protest activity. Interest groups have argued for a more precise definition that will reduce the chances of arbitrary state action against individuals or organizations.

Other concerns pertain to the wide powers given to the Minister of Safety and Security, the National Directorate of Public Prosecutions, and general law enforcement agencies, and the right given to the state to declare organizations as terrorist organizations.NGOs that made submissions on the Bill raised concerns that its far-ranging provisions pose a threat to personal freedom, freedom of expression and freedom of the media. In particular, the powers given to the police and prosecuting authorities to act *ex parte*[623] against individuals and organizations simply on the basis of unspecified "reasonable grounds" have been cause for concern.[624] Many submissions also noted that the new proposed Bill may also be unnecessarily duplicative of legislative resources as there are approximately 22 existing laws that can already adequately deal with "terrorism" crimes without placing constitutional freedoms at risk. Perhaps, and most significantly, the leading trade union organization the Congress of South African Trade Unions (COSATU) opposed the bill on the ground that its definition of terrorism could lead to the outlawing of legitimate strike activities.

The draft legislation was passed by the National Assembly[625] in November 2003. However, after introducing the law in a redrafted form (now titled the Protection of Constitutional Democracy against Terrorist and Related Activities Bill) in the second chamber of Parliament in February 2004, the government announced, under the threat of a nationwide strike by COSATU, that it was delaying a vote on the legislation until after the April 2004 elections. The government has re-introduced the draft legislation in July 2004.

---

[622] A "convention offence" is defined in the Bill schedule as including "interfering with or seizure or exercising control of an aircraft or damaging an aircraft, or murdering or kidnapping an internationally protected person."

[623] Note of the Editor: on behalf of one party only.

[624] The Legal Resources Centre (LRC), in a submission to Parliament, criticized a section of the Bill giving the Safety and Security Minister powers to make regulations concerning any matter that may or must be prescribed in terms of this legislation and any other matter "which is necessary or expedient" to prescribe for the proper implementation of this legislation. The LRC urged that any regulations prepared should be tabled in Parliament prior to them being published for comment in the Government Gazette.

[625] One of the chambers of Parliament.