E. Continuing Problems

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in privacy protections. In other countries, law enforcement and intelligence agencies were given significant exemptions to privacy laws. Finally, without adequate oversight and enforcement, the mere existence of a law may not provide individuals with adequate protection.

There are widespread violations of laws relating to the surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations found that over 90 countries illegally monitor the communications of political opponents, human rights workers, journalists and labor organizers. In 1996, a French government commission estimated that there were over 100,000 illegal wiretaps conducted by private parties, many of these on behalf of government agencies. There were protests in Ireland after it was revealed that the UK was monitoring all UK/Ireland communications from a base in Northern England. In Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist Party. The Echelon system is used by the U.S., UK, Australia, Canada and New Zealand to monitor communications worldwide.

Police services, even in countries with strong privacy laws, still maintain extensive files on citizens for political purposes not accused or even suspected of any crime. There are currently investigations in Sweden and Norway, two countries with the longest history of privacy protection for intelligence and police files. In Switzerland, a scandal over secret police spying led to the enactment of their data protection act. In many former Eastern Bloc countries, there are still controversies over the disposition of the files of the secret police.

Companies regularly flaunt the data protection laws, collecting and disseminating personal information. In the U.S., even with the longstanding existence of a law on consumer credit information, companies still make extensive use of such information for marketing purposes and banks sell customer information to marketers. In other countries, inadequate security has resulted in the accidental disclosure of thousands of customers' records.

II. COUNTRY REPORTS

Argentine Republic

Articles 18 and 19 of the Argentine Constitution protect the privacy of individuals. Article 43, enacted in 1994, provides a right of Habeas

Data.[41] The Supreme Court is currently reviewing a case involving Habeas Data.

In November 1998, the Senate approved a Law for the Protection of Personal Data.[42] It conforms with Article 43 of the Constitution and is based on the E.U. Data Protection Directive. The bill covers electronic and manual records. It requires express consent before information can be collected, stored, processed, or transferred. Collection of sensitive data is given additional protections and is prohibited unless authorized by law. International transfer of personal information is prohibited to countries without adequate protection. Individuals have an express right of Habeas Data to access information about themselves held by government or private entities. The bill sets up an independent commission within the Ministry of Justice to enforce the law. The U.S. Direct Marketing Association launched a lobbying effort against the bill in December 1998 urging Argentinean companies to oppose efforts to enact the law.[43] Previously, in December 1996, the Congress approved a data protection law.[44] However, upon request of the Central Bank, the law was subsequently vetoed by the President.[45]

Under the Code of Penal Procedure, "[a] judge may arrange, for the purposes of building a case, the intervention of telephone communications or whatever other means of communication." The Penal Code provides penalties for publishing private communications.[46] In April 1999, a judge ruled that those provisions also applied to electronic mail.[47] The National Defense Law prohibits domestic surveillance by military personnel. Two Army colonels and two non-commissioned officers were relieved of duty in May 1999, after testifying that they conducted domestic surveillance on "orders from above" to interfere with investigations into human rights abuses during the dictatorship.[48] Illegal wiretapping has been common since the transition to civilian rule. In 1990, the entire telephone switchboard of the President's official residence was extensively bugged and a major government scandal ensued.[49] In 1996, the

41. CONST. ARG., Arts. 18, 19, 43 (1994).

42. S. 577/98, Ley de Protección de los Datos Personales, 26 Nov. 1998. *See also* S.0684/98, S.1582/98, S.1094/98, S. 277/98.

43. *Argentina Wars on the Direct Practice*, PRECISION MARKETING, Jan. 11, 1999.

44. Law No. 24.745 (Dec. 23, 1996) (Arg.) (Data Protection Act).

45. D. 1616, Dec. 30, 1996, Bs. As. 12.23.96 (vetoed by President Menen).

46. CÓD. PEN., Art 153-157.

47. *Un fallo protégé la privacidad de los correos electrónicos*, CLARÍN DIGITAL, April 13, 1999.

48. *Two Army Officers, Others Relieved of Duty Over Intelligence Scandal*, BBC SUMMARY OF WORLD BROADCASTS, May 1999.

49. Richard Jarvie, *Argentine President's Telephones Bugged*, REUTERS NEWS SERVICE, Jan. 29, 1990.

telephones of the Archdiocese of Formosa were found to be wiretapped.[50] Also that year, former Economy Minister Domingo Cavallo accused Interior Minister Carlos Corach of ordering the telephone bugging of a federal prosecutor.[51] In 1998, the Mayor of Buenos Aires and 1999 presidential candidate Fernando de la Rua lodged a criminal complaint against two city councilors and another party member, accusing them of tapping his family's telephone for years and recording 3000 hours of conversation.[52] He also accused the secret police, known as SIDE, of complicity with the wiretaps.[53] The UN Human Rights Committee expressed concern that the judicial authorization for wiretaps was too broad.[54]

The Civil Code prohibits "that which arbitrarily interferes in another person's life: publishing photos, divulging correspondence, mortifying another's customs or sentiments or disturbing his privacy by whatever means."[55]

In 1996, the national government began a new crackdown on tax evaders. Measures included reviewing citizens' credit card, insurance, and tax records. One bill allowed citizens whose credit card records were obtained to sue for invasion of privacy.[56] The same year, the Argentina Passport and Federal Police Identification System, developed by Raytheon E-Systems, was inaugurated at the Buenos Aires airport. The system combines personal data, color photos and fingerprints.[57]

In 1994, Argentina adopted the American Convention on Human Rights into domestic law. Since that date, the Argentine Supreme Court has used international human law to determine domestic cases.[58]

COMMONWEALTH OF AUSTRALIA

Neither the Australian Federal Constitution nor the Constitutions of the six States contain any express provisions relating to privacy. There is periodic debate about the value of a Bill of Rights, but no current

---

50. LA NACION, Buenos Aires, Sept. 8, 1996.

51. *Cavallo's Circus*, THE ECONOMIST, Nov. 23, 1996.

52. Jason Webb, *Argentine Candidate Says Own Party Men Bugged Him*, REUTERS NEWS SERVICE, June 2, 1998.

53. *See id.*

54. U.N. Human Rights Comm, *19th Annual Report of the Human Rights Committee*, U.N. Doc. A/50/40 (Oct. 3, 1995).

55. COD. CIV., Art. 1071bis, incorporated by Law No. 21.173.

56. Calvin Sims, *A New Crackdown Pinches Tax Resistant in Argentina*, N.Y. TIMES, June 10, 1996, at A8.

57. *Argentina Now Equipped with Cutting Edge Passport and I.D. Document Security from Raytheon*, BUS. WIRE, Sept. 12, 1996.

58. *See* Janet Koven Levit, *The Constitutionalization of Human Rights in Argentina: Problem or Promise?*, 37 COLUM. J. OF TRANSNAT'L L. 281, 282, 293 (1999).

proposals.[59]

The principal federal statute is the Privacy Act of 1988.[60] It creates a set of eleven Information Privacy Principles (IPPs), based on those in the OECD Guidelines, that apply to the activities of most federal government agencies. A separate set of rules about the handling of consumer credit information, added to the law in 1989, applies to all private and public sector organizations. The third area of coverage is the use of the government issued Tax File Number (TFN), where the entire community is subject to Guidelines issued by the Privacy Commissioner, which take effect as subordinate legislation. The origins of the Privacy Act were the protests in the mid-1980s against the Australia Card scheme – a proposal for a universal national identity card and number. The controversial proposal was dropped, but use of the tax file number was enhanced to match income from different sources with the Privacy Act providing some safeguards. The use of the tax file number has been further extended by law to include benefits administration as well as taxation. Some controls over this matching activity were introduced in 1990.[61]

In December 1998, the reelected conservative government reversed its opposition to legislative privacy protection in the private sector, and as of June 1999, a bill was being drafted, based on a set of National Principles developed by the Privacy Commissioner during 1997 and 1998, originally as a self-regulatory substitute for legislation. The bill is described as a "light touch legislative regime" and will be based on industry codes. It should be introduced in mid-late 1999 or early in the year 2000.

The Office of Privacy Commissioner[62] has a wide range of functions, including handling complaints, auditing compliance, promoting community awareness, and advising the government and others on privacy matters. The Commissioner's office, which was initially well funded, suffered major budget cutbacks in 1997, at the same time the Commissioner's range of responsibilities under several laws and in response to government requests were expanding. Between 1998-99, the Commissioners Office received 128 complaints, closed 90 complaints and conducted 20 audits.[63]

The Telecommunications (Interception) Act of 1979[64] strictly regulates the interception of telecommunications. A warrant is required under the Act, which also provides for detailed monitoring and reporting,

59. *See* AUSTL. CONST. (Commonwealth of Australia Constitution Act, 1900).

60. *See* Privacy Act, 1988 (Austl.).

61. *See* Data-matching Program (Assistance and Tax) Act, 1990 (Austl.).

62. *See The Australian Privacy Commissioner's Website* (visited Nov. 4, 1999) <http:// www. Privacy.gov.au/>.

63. Letter from Bernard Silva, *Office of the Federal Privacy Commissioner* (Aug. 6, 1999).

64. Telecommunications (Interception) Act, 1979 (Austl.).

but in 1997 the authority for issuing warrants was extended from federal court judges to designated members of the Administrative Appeals Tribunal, who are on term appointments rather than tenure. The Interception Act's safeguards also need to be read alongside Part 15 of the Telecommunications Act of 1997, which places obligations on telecommunications providers to provide an interception capability and to positively assist law enforcement agencies with interception. There were a total of 675 warrants issued in the year 1997-1998.[65] This number excludes an undisclosed number of interception warrants issued to the Australian Security Intelligence Organisation by the Attorney General. In June 1999, the Australian government publicly admitted its role in the Echelon international surveillance system. In May, the Parliamentary Committee that oversees intelligence agencies approved the Australian Security Intelligence Organisation Legislation Amendment Bill 1999. The bill gives ASIO new powers to access e-mails and data inside computers, use tracking devices on vehicles, obtain tax and cash transaction information and intercept mail items carried by couriers.[66]

The Crimes Act[67] also contains a range of other privacy related measures, such as offenses relating to unauthorized access to computers, unauthorized interception of mail and telecommunications and the unauthorized disclosure of Commonwealth government information.[68] It also contains provisions relating to spent convictions, allowing individuals convicted of minor offenses to lawfully 'deny' them in most circumstances after a period of time. The Telecommunications Act of 1997[69] contains a detailed list of "exceptions" from a basic presumption of confidentiality of customer records.[70] A privacy code of practice was drafted under the new co-regulatory system for telecommunications and is expected to be adopted by the Australian Communications Authority after a period of public consultation.[71] In June 1999, Justice Minister Amanda Vanstone proposed a national DNA databank.[72]

The Australian States and Territories have varying privacy laws. In Victoria, a Data Protection Bill was introduced in May 1999 and is ex-

65. Attorney General's Department, *Report on the Telecommunications (Interception) Act for the year ending 30 June 1998.*

66. *Spy Watchdog Committee says new ASIO Legislation is OK*, AUSTRALIAN ASSOCIATED PRESS, May 13, 1999.

67. Crimes Act of 1914-SECT 85ZL (Austl.).

68. Crimes Act of 1914 (Austl.).

69. Telecommunications Act of 1997, 1997 (Austl.).

70. *See supra* note 62.

71. *See The Australian Communications Industry Forum* (visited Nov. 4, 1999) <http://www.acif.org.au/ccrp_wc1/>.

72. *Vastone Seeks to Allay Privacy Concerns over DNA File*, AUSTRALIAN ASSOCIATED PRESS, June 23, 1999.

pected to be enacted later in the year.[73] It covers both the public and private sectors although the Victorian government is proposing to disapply the private sector provisions in favor of the federal legislation.[74] New South Wales, the most populous state, had a Privacy Committee Act since 1975, but this only provided for a committee of part time members to advise government and to act as an "ombudsman." A small staff deals with inquiries from the public and attempts to resolve complaints, but has no determinative powers. In December 1998, data protection legislation was enacted covering government agencies. An Office of Privacy Commissioner has been established.[75] The Australian Capital Territory (ACT) enacted a health privacy law in 1997,[76] and the Queensland government has committed to implement the April 1998 recommendation of a Parliamentary Committee for a public sector privacy law,[77] but no timetable has yet been announced. Specific privacy provisions are also found in many State laws dealing with such diverse matters as health, adoption, drug controls and registration of births, deaths and marriages. Most States and Territories also have laws relating to listening devices, although these are generally recognized as being badly in need of updating to cope with new technologies.[78]

REPUBLIC OF AUSTRIA

The Austrian Constitution does not explicitly recognize the right of privacy.[79] Some sections of the data protection law (Datenschutzgesetz – DSG) have constitutional rank. These rights may only be restricted under the conditions of Article 8 (2) of the European Convention of Human Rights (ECHR). The entire ECHR has constitutional rank and Article 8 is often cited by the constitutional court in privacy matters.

The 1978 Data Protection Law[80] concerns both persons and legal en-

---

73. *See Victorian Legislation and Parlimentary Documents Home Page* (visited Nov. 4, 1999) <http://www.dms.dpc.vic.gov.au/>.

74. Privacy and Personal Information Protection Act 1998 (Austl.) (updated July 13, 1999).

75. *See Office of the New South Wales Privacy Commissioner*, NEW SOUTH WALES ATTORNEY GENERAL'S DEPARTMENT (visited Nov. 4, 1999) <http://www.lawlink.nsw.gov.au/pc.nsf/pages/index>.

76. Health Records (Privacy and Access) Act, 1977 (Austl.).

77. Legal, Constitutional and Administrative Review Comm., *Privacy in Queensland*, LEGISLATIVE ASSEMBLY OF QUEENSLAND, Rep. No. 9.

78. NEW SOUTH WALES LAW REFORM COMMISSION, ISSUES PAPER 12 – SURVEILLANCE AND THE LISTENING DEVICES ACT, 1997 (N.S.W.) (visited Nov. 7, 1999) <http://www.lawlink.nsw.gov.au/lrc.nsf/pages/IP12CHP5>; *see also ACIF Guideline on Participant Monitoring* (visited Nov. 7, 1999) <http://www.acif.org.au/acif/index.cfm>.

79. Landes-Verfassungsgesetz [Austrian State Constitution] [L-VG] (1929).

80. Datenschutzgesetz (Data Protection Act), BGBl 1978/565 (Aus.) (changed by 1981/314, 1982/228, 1986/370, 1987/605, 1988/233, 1989/609, 1993/91, 1994/79, 1994/632).

tities. Anybody who processes personal data automatically must notify or register at the Data Protection Commission (Datenverarbeitungsregister). Individual rights can be asserted in the courts if the processor is not a public authority, or at the Commission in all other cases. Appeals against decisions of the Data Protection Commission can be made at the administrative court (Verwaltungsgerichtshof) or the Constitutional Court (Verfassungsgerichtshof). The Commission reports that there are 100,000 Data Controllers registered. It also handles around 40 formal complaints and 30 requests for information in written form every year, as well as a large number of informal requests for information.

A new data protection law (Datenschutzgesetz 2000)[81] incorporating the E.U. Directive into Austrian law was passed in August of 1999. However, experts criticize the new law as being inadequate because it retains the cumbersome structure of the previous Act, rather than replacing it.[82]

Wiretapping, electronic eavesdropping and computer searches are regulated by the code of criminal procedure.[83] Telephone wiretapping is permitted if it is needed for investigating a crime punishable by more than one year in prison. Electronic eavesdropping and computer searches are allowed if they are needed to investigate criminal organizations or crimes punishable by more than ten years in prison. The provision concerning electronic eavesdropping and computer searches became effective between October 1, 1997, and July 1, 1998. Due to long and intensive discussion, the provisions are in effect only until December 31, 2001. Criticism of the drafts for this law has led to a number of restrictions, but whether or not these provisions can effectively prevent eavesdropping on innocent persons remains unresolved.

There are also a number of specific laws relating to privacy. The telecommunication law contains special data protection provisions for telecommunication systems, particularly problems like phone directories, unsolicited calls or ISDN calling line identification.[84] The Genetic Engineering Act of 1994 requires prior written consent for information to be used for purposes other than the original purpose. Austrians can have an anonymous "Sparbuch" bank account. The Financial Action Task Force, an anti-money laundering group coordinated by the OECD, has been pressuring Austria to change its laws to require that each account

81. Datenschutzgesetz 2000 [Data Protection Act 2000 - DSG 2000], BGBl. I Nr. 165/1999 (Aus.).

82. *See* VIKTOR MAYER-SCHOENBERGER & ERNST BRANDL, DATENSCHUTZGESETZ 2000 (1999).

83. Strafprozeßordnung [criminal procedure statute], §§ 149a-149p StPO.

84. Telekommunikationsgesetz (TKG), §§ 87 - 101 BGBl I 100/1997.

be personally identified.[85]

KINGDOM OF BELGIUM

The Belgian Constitution recognizes the right of privacy and private communications.[86] Article 22 was added to the Belgian Constitution in 1994. Prior to the constitutional amendment, the Cour de Cassation ruled that Article 8 of the European Convention applied directly to the law and prohibited government infringement on the private life of individuals.[87]

Legislation to update the Data Protection Act of 1992 to make it consistent with the E.U. Directive was approved by the Parliament in December.[88] A Royal Decree to implement the Act is currently being presented to the Council of State for advice. The new Act will come into force four months after it is published in the Official Journal. However, there is concern among independent experts that the revised act is lacking in areas relating to government files and may not be fully consistent with the Directive. In September 1998, the state security office announced that it was "cleaning" the files on 570,000 individuals that it had collected since 1944 to bring the files into compliance with the 1992 law.[89] In 1995, the Belgian Government admitted spying on the peace and environmental movements.[90]

The Commission de la Protection de la Vie Privée oversees the law.[91] The Commission investigates complaints, issues opinions and maintains the registry of personal files. The Commission received 24,000 registrations.[92] In 1998, the Commission answered 515 requests for general information and 65 requests for information about the public register. The Commission also investigated 397 complaints relative to consumer credit.

Surveillance of communications is regulated under a 1994 law.[93] Prior to its enactment, there was no specific law. The law requires permission of a juge d'instruction before wiretapping can take place. Orders

85. *Financial Action Task Force on Money Laundering Issues: a Warning about Austrian Anonymous Savings Passbooks*, Feb. 11, 1999.

86. BELG. CONST., TITLE II.

87. Cour de Cassation, Sept. 26, 1978 (Belg.).

88. Act concerning the protection of privacy with regard to the treatment of personal data files, Dec. 8, 1992 (Belg.).

89. La Sûreté de l'Etat trie 570.000 fiches individuelles, Le Soir, Sept. 19, 1998.

90. Statewatch Bulletin, Vol. 5 No 6, Nov. – Dec. 1995.

91. Commission de la protection de la vie privée, *Home Page* [Belgian Privacy Commission] (visited Nov. 7, 1999) <http://www.privacy.tgov.be/>.

92. Email from Commission de la protection de la vie privée, July, 1999.

93. loi de 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (Belg.).

are limited to a length of one month. There were 114 orders issued in 1996.[94] The law was amended in 1997 to remove restrictions on encryption.[95] The Parliament also amended the law in 1998 to require greater assistance from telecommunications carriers.[96] There are also laws relating to consumer credit,[97] social security,[98] electoral rolls,[99] the national ID number,[100] professional secrets,[101] and employee rights.[102]

FEDERATIVE REPUBLIC OF BRAZIL

Article 5 of the 1988 Constitution of Brazil provides a right of privacy and access to information.[103]

A bill promoting the privacy of personal data in conformance with the OECD guidelines, to affect both public and private sector databases, was proposed in the Senate in 1996 and has yet to be voted on. The bill provides that:

> No personal data nor information shall be disclosed, communicated, or transmitted for purposes different than those that led to structuring such data registry or database, without express authorization of the owner, except in case of a court order, and for purposes of a criminal investigation or legal proceedings . . . It is forbidden to gather, register, archive, process, and transmit personal data referring to: ethnic origin, political or religious beliefs, physical or mental health, sexual life, police or penal records, family issues, except family relationship, civil status, and marriage system . . . Every citizen is entitled to, without any

94. *Ecoutes: une pratique décevante et. flamande! Le résultat judiciaire des écoutes téléphoniques est médiocre. La Chambre va modifier la donne* [Listenings: a dissappointing practice and . . . Flemish! The legal result of the phone tapping is poor. The House will modify the law.], LE SOIR, Dec. 12, 1997.

95. Chapitre 17, Loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, Dec. 19, 1997 (Belg.).

96. Loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, 10 Juin 1998 (Belg.); *Le GSM en toute sécurité? Pas sûr.* [The GSM is secure full safety? Not sure.], LE SOIR, Feb. 20, 1998.

97. La loi du 12 juin 1991 relative au crédit à la consommation. l'arrêté royal du 11 janvier 1993 modifiant l'arrêté royal du 20 novembre 1992 relatif à l'enregistrement par la Banque Nationale de Belgique des défauts de paiement en matière de crédit à la consommation (Belg.).

98. La loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale. Modified by la loi du 29 avril 1996 (Belg.).

99. la loi du 30 juillet 1991(Belg.).

100. La loi du 8 août 1993: le registre national (Belg.).

101. Art. 458 of the Penal Code (Belg.).

102. *See* Roger Blanpain, *Employee Privacy Issues: Belgian Report*, 17 COMP. LAB. L.J. 38 (1995).

103. BRAZ. CONST. art. 5, §§ X, XIV (1988).

> charge; access his/her personal data, stored in data registries or databases, and correct, supplement, or eliminate such data, and be informed by data registry or database managers of the existence of data regarding his/her person.[104]

It is expected by many that the law will move forward once legislation is approved in neighboring countries such as Argentina and Chile.

The 1990 Code of Consumer Protection and Defense allows all consumers the following:

> [A]ccess [to] any information derived from personal and consumer data stored in files, archives, registries, and databases, as well as to access their respective sources. Consumer files and data shall be objective, clear, true, and written in a manner easily understood, and shall not contain derogatory information for a period over five years. Whenever consumers find incorrect data and files concerning their person, they are entitled to require immediate correction, and the archivist shall communicate the due alterations to the incorrect information within five days. Consumer databases and registries, credit protection services, and similar institutions are considered entities of public nature. Once the consumer has settled his/her debts, Credit Protection Services shall not provide any information which may prevent or hinder further access to credit for this consumer.[105]

The Informatics Law of 1984 protects the confidentiality of stored, processed and disclosed data, and the privacy and security of physical, legal, public, and private entities. Citizens are entitled to access and correct their personal information in private or public databases.[106]

In 1996, a law regulating wiretapping was enacted.[107] Official wiretaps are permitted for 15 days, renewable on a judge's order for another 15 days, and can only be resorted to in cases where police suspect serious crimes punishable by imprisonment, such as drug smuggling, corruption, contraband smuggling, murder and kidnapping. The granting of judicial eavesdropping permits by judges was previously an ad hoc process without any legal basis.[108] Illegal wiretapping by police and intelligence agencies is still ongoing. The Agencia Brasileira de Informacoes (Abin) was suspected of wiretapping President Cardoso after tapes of his conversations were leaked to the press in May 1999.[109] Several ministers resigned in 1998 after tapes of wiretapped conversation involving the Brazilian Development Bank were disclosed in what was called the

104. 61, 1996, D.O.U., Apr. 10, 1996 (Braz.) (copy in Eng. May be found at <http://www.privacyexchange.org/legal/ppl/nat/brazilpending.html>.

105. Lei No.008078, Sept. 11, 1990, D.O.F.C.12.09.1990 (Braz.).

106. Lei No.007232, Oct. 29, 1984, D.O.F.C.30.10.84 (Braz.).

107. Lei No.009296, July 24, 1996 (Braz.).

108. *Brazil Makes Police Phone-taps Legal*, REUTERS NEWS SERVICE, July 24, 1996.

109. *Is Abin behind Telegate? New Intelligence Agency May Be Behind Wire Tapping*, LATIN AMERICA WEEKLY REPORT, June 8, 1999, at 260.

"Telegate scandal." In 1992, amid a scandal that toppled President Fernando Collor de Mello, it was discovered that Vice President Itamar Franco's phones at his official residence in Brasilia and in a Rio de Janeiro hotel room had been tapped.[110] In 1996, Abin was put under military control with the task of evaluating the background of people appointed to government posts. According to the new director, "every instrument authorized by the courts will be used to keep the president well informed, including wiretapping of phones, opening of personal mail, and infiltration of Abin agents into social movements such as the Landless Peasant's Movement (Movimento sem Terra)." Abin is the central body of an intelligence system that is spread out through federal, state, municipal and even private organizations. The intelligence system operates under the name of Sisbin (Brazilian Intelligence System).[111] The Agency's guidelines prevent it from performing police operations, and require it to obtain a judicial order to perform wiretaps.[112]

A man with AIDS charged the city of Morretes, Paraná of discrimination and invasion of privacy after a city government proclamation identifying him and his HIV status was posted in public buildings.[113]

REPUBLIC OF BULGARIA

The Bulgarian Constitution of 1991 recognizes rights of privacy, secrecy of communications and access to information.[114]

There are currently efforts to enact comprehensive data protection legislation in Bulgaria. In 1996, the government began developing data protection legislation in preparation for integration into the E.U. Internal Market under the Treaty for Association of Bulgaria to the E.U. Data protection is also a key element of the information legislation which is a priority in the National Assembly's legislative activities. The draft Law on Protection of Citizens' Personal Data sets rules on the fair and responsible handling of personal information by the public and private sector. Entities collecting personal information must do the following: inform people why their personal information is being collected and what it is to be used for; allow people reasonable access to information about themselves and the right to correct it if it is wrong; ensure that the information is securely held and cannot be tampered with, stolen or improp-

110. Rene Villegas, *Brazil Vice-president Claims his Phone was Tapped*, REUTERS NORTH AMERICAN WIRE, Sept. 9, 1992.

111. *'O Globo'*, BBC SUMMARY OF WORLD BROADCASTS, Aug. 4, 1996, *available in* LEXIS, News Library, BBC Monitoring Serv.: Latin Am., Aug. 7, 1996.

112. Agencia Estado (news agency), *President Transfers Control of New Intelligence Agency to Military*, BBC SUMMARY OF WORLD BROADCASTS, Apr. 11, 1996.

113. SEJUP (Servico Brasileiro de Justica e Paz), No.117, Feb. 17, 1994 (visited Nov. 8, 1999) <http://www.oneworld.org/sejup/117.btm>.

114. BULG. CONST., arts. 32, 33, 40 (July 13, 1991).

erly used; and limit the use of personal information, for purposes other than the original purpose, without the consent of the person affected, or in certain other circumstances. The draft law envisions a special supervising body with additional regional bodies to enforce the Act. The European Commission stated in 1997 that "considerable efforts are still needed to adopt and implement measures to meet Community requirements on data protection."[115]

Electronic surveillance used in criminal investigations is regulated by the criminal code and requires a court order.[116] The Telecommunications Law also requires that agencies must ensure the secrecy of communications.[117] The 1997 Special Surveillance Means Act regulates the use of surveillance techniques by the Interior Ministry for investigating crime, but also for loosely defined national security reasons. A court order is generally required, but in cases of emergency, an order from the Interior Minister is sufficient.[118] The head of the National Security Service, Colonel Yuli Georgiev, resigned in February 1997 after allegations of wiretapping politicians.[119] Bulgaria's military prosecutor filed a suit in December 1996 against an unidentified state official for illegally bugging telephones at the offices of the main opposition, the Union of Democratic Forces (UDF), including those of president-elect Petar Stoyanov.[120]

There are additional provisions relating to privacy in laws such as the Statistics Law, the Tax Administration Law, the Insurance Law,[121] and the Social Assistance Law.[122] The Radio and Television Act sets limits on broadcasting of personal information.[123] In conjunction with the preparation of the Law on Protection of Citizens' Personal Data, analyses of Bulgarian legal acts related to personal data of individuals are planned. Proposals of reforms and supplements in the relevant acts also can be made, if necessary.

CANADA

There is no explicit right to privacy in Canada's Constitution and

115. EUROPEAN COMMISSION, COMMISSION OPINION ON BULGARIA'S APPLICATION FOR MEMBERSHIP IN THE EUROPEAN UNION, July 15, 1997, *available at* European Commission, *Criteria for Membership: Political Criteria* (visited Nov. 24, 1999) <http://europa.eu.int/comm/dg1a/agenda2000/en/opinions/bulgaria/b1.htm>.

116. Arts. 170-171 (1) (as amended - SG, Nos. 28/1982, 10/1993).

117. Telecommunications Law, Art. 5 (Bulg.).

118. BULGARIAN HELSINKI COMMITTEE, HUMAN RIGHTS IN BULGARIA IN 1997.

119. *Security Chief Resigns: Reportedly was to be Dismissed*, BBC SUMMARY OF WORLD BROADCASTS, Feb. 7, 1997.

120. REUTERS WORLD SERVICE, Dec. 19, 1996.

121. Insurance Law, art.7 ¶ 1 (Bulg.).

122. Social Assistance Law, art. 32 ¶ 2 (Bulg.).

123. Radio and Television Act, arts. 10, 15 (Bulg.).

Charter of Rights and Freedoms.[124] However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canada's courts have recognized an individual's right to a reasonable expectation of privacy.[125]

The Privacy Act[126] provides individuals with a right of access to personal information held by the federal public sector. In addition, the Privacy Act contains provisions regulating the confidentiality, collection, correction, disclosure, retention and use of personal information. Individuals may request records directly from the institution that has the custody of the information. The Act establishes a code of fair information practices that apply to government handling of personal records.

The Privacy Act is overseen by the independent Privacy Commissioner of Canada.[127] The Commissioner has the power to investigate, mediate and make recommendations, but cannot issue binding orders. The commissioner received 2,455 complaints in 1997-1998 and completed 1,821 investigations.[128] The Commissioner can initiate a Federal Court review. In the Fall of 1998, the Commissioner asked a court to review the matching of Customs declarations of returning travelers against the Employment Insurance database. The Federal Privacy Commissioner asked the court to decide whether the Customs Act overrides the government's obligation in the Privacy Act to use personal information only for the purpose for which it is collected unless the individual consents. In February 1999, the court ruled that the matching could not be conducted without ministerial approval and the program was suspended.

The Federal Parliament is currently reviewing Bill C-6, the Personal Information Protection and Electronic Documents Act,[129] a privacy law that will cover the private sector. The proposal is based on adopting the Canadian Standards Association's privacy standard into law for areas that are under federal regulation, such as banks, telecommunications, transportation and enterprises that trade data interprovincially and internationally. In three years, it would cover other sectors that process personal information in every province unless the province enacts "substantially similar" laws, such as Quebéc's law. The bill was re-introduced in October 1999 and has the support of the Prime Minister who

124. *See generally* CAN. CONST.

125. Hunter v. Southam Inc., [1984] S.C.R. 159, 160.

126. Privacy Act, S.C., ch. P-21 (1984) (Can.).

127. *See Privacy Commissioner of Canada* (visited Nov. 8, 1999) <http://www.privcom.gc.ca>.

128. Privacy Commissioner, *1997-98 Annual Report*, PRIVACY COMMISSIONER OF CANADA, July 1998.

129. Bill C-6, Personal Information Protection and Electronic Documents Act, Oct. 15, 1999 (Can.) (first introduced as Bill C-54 on Oct. 1, 1998).

has committed to have the legislation enacted.[130] The bill was first introduced in October, 1998, however, it was not approved before the summer recess. There are also provincial efforts to adopt new laws to cover sectors that are not federally regulated.

Privacy legislation covering government bodies exists in almost all provinces and territories.[131] In the province of Québec, the Charter of Rights specifically mentions the right to privacy and the law regulates the collection and use of personal information held by private sector businesses operating in the province of Québec.[132] This law sets rules the collection, confidentiality, correction, disclosure, retention and use of personal information by these businesses. It also provides individuals with a right of access and correction. Québec holds the distinction of being the only North American jurisdiction to regulate personal information in the private sector. Nearly every province has some sort of oversight body for privacy laws, but their powers vary from province to province. The Québec Commission d'accès à l'information has broad powers over both the public and private sectors. The Information and Privacy Commissioners of British Columbia and Ontario were very active in promoting privacy through their oversight powers of public bodies and public education efforts.

Part VI of Canada's Criminal Code makes the unlawful interception of private communications a criminal offense.[133] Police are required to obtain a court order to be allowed to tap into private communications. In 1997, there were 185 orders for warrants under the Criminal Code, a decrease from 276 in 1996 and 266 in 1995.[134] Amendments to the Radiocommunication Act[135] also forbid the divulgence of intercepted radio-based telephone communications. The Canadian Security Intelligence Service Act[136] authorizes the interception of communications for national security reasons. A federal court in Ottawa ruled in 1997 that the Canadian Security Intelligence Service was required to obtain a warrant in all cases.[137] On October 1, 1998, Industry Minister John Manley announced a new liberal government policy for encryption that allows for broad development, use and dissemination of encryption products.

---

130. For more information, see Industry Canada's Task Force on Electronic Commerce (visited Nov. 8, 1999) <http://e-com.ic.gc.ca/english/privacy/632d1.html>.

131. A list of state laws and commissions is available from the Privacy Commission of Canada (visited Nov. 8, 1999) <http://privcom.gc.ca/>.

132. Commission d'accès à l'information du Québec , *Une Commission, deux loix* (visited Nov. 10, 1999) <http://www.cai.gouv.qc.ca/commiss.htm>.

133. Criminal Code, C.R.C., c. C-46, §§ 184, 184.5, 193, 193.1 (1993) (Can.).

134. Solicitor General Canada, *Annual Report on the Use of Electronic Surveillance* (1997).

135. Radiocommunication Act, R.S.C. 1985, c. R-2, § 9 (1985) (Can.).

136. Canadian Security Intelligence Service Act, R.S.C., ch. C-23 (1984) (Can.).

137. *CSIS has Wiretap Green Light*, THE HAMILTON SPECTATOR, Oct. 1, 1997.

Other federal legislation also has provisions related to privacy. The Telecommunications Act[138] has provisions to protect the privacy of individuals, including the regulation of unsolicited communications. Also, the Bank Act,[139] the Insurance Companies Act,[140] and the Trust and Loan Companies Act[141] permit regulations to be made governing the use of information provided by customers. There are sectoral laws for pensions,[142] video surveillance,[143] immigration,[144] and Social Security.[145] The Young Offenders Act[146] regulates what information can be disclosed about offenders under the age of eighteen while the Corrections and Conditional Release Act[147] speaks to what information can be disclosed to victims and victims' families. In addition, most provinces have some form of legislation protecting consumer credit information. However, the vast majority of information collected by the private sector is on the provincial level and is not currently protected by any provincial laws. A poll in April 1999 found that 88 percent of people said the government should "not allow banks to use information about their customer's bank accounts and other investments to try to sell customers insurance."[148]

Identity issues are currently under debate in Canada. There is great concern about the use of the Social Insurance Number (SIN) by the private sector and its use in identity theft. A Parliamentary committee recommended in May 1999 that the SIN be scrapped and replaced with a new smart card.[149] Québec considered creating a mandatory ID card, but dropped the idea in 1998. In April 1999, it hired DMR Consulting Group to examine the possibility of creating a central database of all government records on residents.[150] In Toronto, a system to fingerprint all welfare recipients was dropped in March 1999 after Citibank, the contractor, was unable to create a working system.[151] The UN Human

138. Telecommunications Act, R.S.C., ch. T-3.4, §§ 39, 41 (1993, c.38) (Can.).

139. Bank Act, R.S.C., ch. B-101, §§ 242, 244, 459 (1991, c.46) (Can.).

140. Insurance Companies Act, R.S.C., ch. I-11.8, §§ 489, 607 (1991, c.47) (Can.).

141. Trust and Loan Companies Act, R.S.C., ch.T-19.8, § 444 (1991, c.45) (Can.).

142. Canada Pension Plan, R.S.C., ch. C-8, § 104.07 (1985) (Can.).

143. Criminal Code, C.R.C., ch. C-46, § 487.01 (1999) (Can.).

144. Immigration Act, R.S.C., ch. I-2, § 110 (1985) (Can.).

145. Old Age Security Act, R.S.C., ch. O-9, § 33.01 (1997) (Can.).

146. Young Offenders Act, R.S.C., ch. Y-1, § 38 (1985) (Can.).

147. Corrections and Conditional Release Act, R.S.C., ch. C-44.6, §§ 26, 142.

148. *88% of Canadians Oppose Banks Target-Marketing Insurance: Compas Poll*, CANADA NEWS WIRE, Apr. 27, 1999.

149. Report of the Standing Comm. on Human Resources Development and the Status of Persons of Persons with Disabilities, *Beyond the Numbers: The Future of the Social Insurance Number System in Canada*, PARLIAMENT, May 1999 (Albina Guarnieri, M.P., Chair) (Can.).

150. Laura Lyne McMurchie, *Quebec Hires DMR to Study ID Database*, COMPUTING CANADA, Apr. 30, 1999, at 4.

151. *City Welfare Fingerprint Plan Flops*, THE TORONTO STAR, May 21, 1999.

Rights Commission was critical of the increasing use of fingerprinting in Canada and recommended in April 1999 "that Canada take steps to ensure the elimination of increasingly intrusive measures which affected the right of privacy of people relying on social assistance, including identification techniques such as fingerprinting and retinal scanning."[152]

REPUBLIC OF CHILE

Article 19 of Chile's Constitution protects privacy and secrecy of communications.[153] A comprehensive privacy law was approved by the Parliament in August 1999 following several years of debate.[154] The law covers both the public and private sectors. Information can only be collected if it is authorized by law or with the express consent of the person, who must be told of its purpose. Individuals have a right of access and can demand corrections or removal of information. Information can only be used for the purposes for which the information was provided. Information collected for journalistic purposes is exempt. Violators can be imprisoned.

Chile's transition to democratic rule in 1990 did not eliminate personal privacy violations by government agencies. The Investigations Police – a plainclothes civilian agency that functions in close collaboration with the International Criminal Police Organization (Interpol) and with the intelligence services of the army, navy, and air force – keeps records of all adult citizens and foreign residents and issues identification cards that must be carried at all times.[155] The personal data compiled during military rule was never destroyed. In January 1998, former dictator General Augusto Pinochet, threatened to use "compromising information" from secret military intelligence files against those who were trying to keep him from becoming a Senator for Life, a position which would provide him with immunity from civil suits and public accountability for crimes which took place during his dictatorship.[156] Under current law, the voter registration list is publicly disclosed and used for direct marketing purposes. In 1999, the UN Human Rights Committee criticized the requirement that hospitals report all women who receive

152. Human Rights Comm. concludes sixty-fifth session held at headquarters from 22 Mar. to 9 Apr., Apr. 12, 1999.

153. CHILE CONST. (1980).

154. BOLETIN N° 896-07, Proyecto de ley sobre protección de la vida privada, ley 19, 628 (Bill: Protection of Personal Data) (English translation of an earlier version is available at <http://www.privacyexchange.org/legal/ppl/nat/chilepending.html>).

155. CHILE: A COUNTRY REPORT, U.S. LIB. OF CONG. (1994).

156. Calvin Sims, *Chile's Ex-Dictator Tries to Dictate His Future Role*, N.Y. TIMES, Feb. 1, 1998, at A3.

abortions.[157]

A 1995 law bars obtaining information by undisclosed taping, telephone intercepts, and other surreptitious means, and bars the dissemination of such information, except by judicial order in narcotics-related cases.[158] In August 1996, the head of the Direccion de Inteligencia Policial (Dipolcar), the police intelligence service, was charged with authorizing a surveillance operation against the defense ministry official responsible for Carabineros, the militarized national police force. His resignation in disgrace allowed a greater role for the civilian security police, Investigaciones, in anti-drug operations.[159] In 1992, a surveillance center with 24-hour scanning devices was uncovered in downtown Santiago. It was run by an active army intelligence unit (DINE, incorporating former members of the secret police, the CNI) and, among other incidents, was found to have tapped into presidential candidate Sebastian Pinera's cellular phone[160] and taped the calls of President Patricio Aylwin.[161] The Army admitted to tapping telephones in order to comply with its mission, but reaffirmed that it "does not tap phones in an attempt to interfere with peoples' privacy."[162] The scandal provoked the retirement of General Ricardo Contreras, head of the Army Telecommunications Command.[163]

PEOPLE'S REPUBLIC OF CHINA

There are limited rights to privacy in the Chinese Constitution which are subject to broad exemptions for protecting state security.[164] China has no general data protection law and few laws that limit government interference with privacy. China has a long-standing policy on keeping close track of its citizens. According to expert W.J.F. Jenner,

> Chinese states by the fourth century BC at latest were often remarkably successful in keeping records of their whole populations so

157. U.N. Human Rights Comm., *Press Release, Human Rights Committee Concludes Consideration of Chile's Fourth Periodic Report*, 1734th mtg., Mar. 24, 1999.

158. Law No. 19,423 (Chile).

159. *Rows Grow Over Security Services*, SOUTHERN CONE REPORT, Sept. 12, 1996.

160. *Television Nacional de Chile*, BBC SUMMARY OF WORLD BROADCASTS, Sept. 26, 1992.

161. *Army's Bugging Centre Uncovered; State of Alert as Army Denies Invading Anyone's 'Privacy'*, LATIN AMERICA WEEKLY REPORT, Oct. 8, 1992, at 3.

162. *Navy, Air Force Deny Allegations of Telephone Tapping*, BBC SUMMARY OF WORLD BROADCASTS, Sept. 28, 1992.

163. *Chile Army to take Action Against Servicemen Involved in Telephone-tapping Case*, BBC SUMMARY OF WORLD BROADCASTS, Nov. 27, 1992.

164. CONST. P.R.C. (1993) (adopted at the 5th Sess., 5th Nat'l People's Cong., promulgated for implementation, Procl. Nat'l People's Cong., Dec. 4, 1982, as amended at the 1st Sess., 7th Nat'l People's Cong., Apr. 12, 1988, and at the 1st Sess., 7th Nat'l People's Cong., Mar. 29,1993).

> that they could be taxed and conscripted. The state had the surname, personal name, age and home place of every subject and was also able to ensure that nobody could move far from home without proper authorization.[165]

Concerns with the growing use of the Internet led to technical and legal restrictions. With the assistance of American companies such as Bay Networks, China has developed a "Great Firewall" which limits traffic to the Internet outside China to only three gateways.[166] The firewall also blocks some western news web sites such as the BBC, New York Times and the Voice of America. In February 1999, the government announced the creation of the State Information Security Appraisal and Identification Management Committee which according to the official Xinhua state news agency "will be responsible for protecting government and commercial confidential files on the Internet, identifying any net user, and defining rights and responsibilities . . . . The move is intended to guard both individual and government users, protect information by monitoring and keep them from being used without proper authorization."[167] In December 1998, a Chinese businessman was handed a two-year jail sentence for subversion for supplying 30,000 e-mail addresses of Chinese computer users to a U.S.-based electronic dissident magazine.[168]

Under Article 7 of the Computer Information Network and Internet Security, Protection and Management Regulations "the freedom and privacy of network users is protected by law. No unit or individual may, in violation of these regulations, use the Internet to violate the freedom and privacy of network users."[169] Article 8 states:

> units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the public security organization. This includes providing to the public security organization information, materials and digital document, and assisting the public security organization to discover and properly handle incidents involving law violations and criminal activities involving computer information networks.[170]

---

165. W.J.F Jenner, *China and Freedom*, KELLY & REID, ASIAN FREEDOMS (1998).

166. Gary Chapman, *China Represents Ethical Quagmire in High-Tech Age*, L.A. TIMES, Jan. 27, 1997, at D1.

167. *China Forms Information Security Oversight Committee*, XINHUA NEWS AGENCY, Feb. 12, 1999.

168. Gus Constantine, *Beijing Convicts Internet Dissident; Businessman Sold Chinese E-mail Addresses*, WASHINGTON TIMES, Jan. 21, 1999, at A13.

169. *Chinalaw Computer Information Network and Internet Security, Protection and Management Regulations* (visited Nov. 17, 1999) <http://www.qis.net/chinalaw/prclaw54.htm> (approved by the State Council on Dec. 11, 1997, promulgated by the Ministry of Public Security, Dec. 30, 1997).

170. *Id.* at art. 8.

Articles 10 and 13 stipulate that Internet account holders must be registered with the public security organization and lending or transferring of accounts is strictly prohibited. Sections 285 to 287 of the Criminal Code prohibit intrusions into computer systems and punish violations of the regulations. There were news reports in June 1999 that the Chinese government limited the import and use of the Intel Pentium III chip because of concern over the Processor Serial Number.[171]

The secrecy of communications is named in the constitution and in law, but apparently with little effect. In practice, authorities often monitor telephone conversations, fax transmissions, electronic mail, and Internet communications of foreign visitors, businessmen, diplomats, and journalists, as well as Chinese dissidents, activists, and others.[172] UK Prime Minister Tony Blair was reported to be upset by the bugging and wiretapping of his rooms during his state visit to China in October 1998.[173]

Postal enterprises and postal staff are prohibited from providing information to any organization or individual about users' dealings with postal services except as otherwise provided for by law.[174] However, Article 21 of the Postal Law permits postal staff to examine, on the spot, the contents of non-letter postal materials. Mail handed in or posted by users must be in accordance with the stipulations concerning the content allowed to be posted; postal enterprises and their branch offices have the right to request users to take out the contents for examination, when necessary.

The Practicing Physician Law requires that doctors not reveal health information obtained during treatment. Doctors who violate the law face criminal penalties. In May of 1999, the Ministry of Health, with the approval of the State Council, published an administrative order declaring that personal information about HIV/AIDS sufferers be kept secret, and that the legal rights and interests of those people and their relatives should not be infringed. The Ministry of Health order asked all units and individuals who are in charge of diagnosis, treatment, and management work not to publish any personal information about HIV/

171. Yang Gu, *Ministry of Information Industry (MII) Advises Government Agencies on Prudent Use of PIII*, GUANGMING DAILY, June 30, 1999.

172. U.S. DEPARTMENT OF STATE, BUREAU OF DEMOCRACY, HUMAN RIGHTS, AND LABOR, China Country Report on Human Rights Practices for 1998, Feb. 26, 1999; AMNESTY INTERNATIONAL, 1999 WORLD REPORT: CHINA.

173. *Blair: I Never Want to Visit Beijing Again; Blair Claims He was Bugged by China's Secret Police*, THE MIRROR, Oct. 12, 1998.

174. Postal Law of the P.R.C. (adopted 18th mtg., Standing Comm., Nat'l People's Congress, promulgated by Order No. 47, Dec. 2, 1986, and eff. Jan. 1, 1987); *available at* CHINALAW No. 396, Chinalaw Computer-Assisted Legal Research Center, Peking University.

AIDS sufferers, such as the name or family address.[175]

Since 1984, all Chinese citizens over the age of 16 are required to carry identification cards issued by the Ministry of Public Security. Identification cards include name, sex, nationality, date of birth, address and term of validity, of which there are three. Between the ages of 16 and 25, it is 10 years, between the ages of 25 and 45, it is 20 years and for those aged 45 and over it is permanent. In carrying out their duties public security organs have the right to ask citizens to show their ID cards. In handling political, economic and social affairs, which involve rights and interests, government offices, people's organizations and enterprises may also ask citizens to show their ID cards.[176] Failure to register for an identification card, forging or otherwise altering a residence registration, or assuming another person's registration are all prohibited by law and punishable by fine. Failure to notify local authorities concerning visiting guests is also punishable by fine.[177] In 1997, the State Bureau of Technical Supervision began working on a new number system that will be used for Social Security and ID cards.[178] In December 1998, authorities began a test program requiring five hotels in Guangzhou to fax copies of the data of all customers to the Public Security Bureau to capture "unwanted elements."[179]

CZECH REPUBLIC

The 1993 Charter of Fundamental Rights and Freedoms provides for extensive privacy rights.[180] The Act on Protection of Personal Data in Information Systems was adopted in 1992.[181] The Act regulates the protection of personal data for both government and private databases con-

175. *Privacy, Right Protection for AIDS Patients Urged*, XINHUA NEWS AGENCY, May 20, 1999.

176. *Chinese Citizens to Carry Identification Cards*, XINHUA NEWS AGENCY, May 7, 1984, *available at* LEXIS, Xinhua General News Service; Regulations of the P.R.C. Concerning Resident Identity Cards (adopted at the 12th mtg. of the Standing Committee of the Sixth National People's Congress, promulgated for implementation by Order No. 29 of the President of the People's Republic of China on Sept. 6, 1985, and effective as of Sept. 6, 1985), *available in* CHINALAW No. 304., Chinalaw Computer-Assisted Legal Research Center, Peking University.

177. Regulations of P.R.C. on Administrative Penalties for Public Security (adopted at the 17th mtg., Standing Comm., 6th Nat'l People's Cong., promulgated by Order No. 43, Sept. 5, 1986, eff. Jan. 1, 1987), *available in* CHINALAW No. 368, Chinalaw Computer-Assisted Legal Research Center, Peking University.

178. *China: Numbering System Aids Social Security*, CHINA DAILY, Nov. 27, 1997.

179. *Guangzhou Hotels Send Personal Data on Guests To Police*, HONG KONG STANDARD, Dec. 30, 1998.

180. Charter of Fundamental Rights and Freedoms (1993) (Czech Rep.), *available at* (visited Nov. 2, 1999) <http://www.psp.cz/cgi-bin/eng/docs/laws/charter.html>.

181. Protection of Personal Data in Information Systems, 256/1992 Sb. (Apr. 29, 1992) (Czech Rep.).

tained in an information system. The Act covers systems containing personal information relating to race, nationality, political attitudes and membership, criminal records, health, sexuality and property. The Act requires legal authority to collect information and limits use to the purpose for which it was established, unless another law provides otherwise. Operators of systems must register. There is no independent oversight agency to enforce the Act. The Council of Ministers rejected a proposal by the Ministry of Economy to create an independent body in 1996, opting for a small office under the Council of Ministers.

The bill is considered weak and there were a number of high profile scandals involving abuse of personal information. In 1992, the Interior Ministry sold the addresses of all children under the age of two and all women between 15 and 35 – a total of two million people – to Procter & Gamble. The company used the information for a direct marketing campaign for Pampers diapers and Always brands. One official was charged with violating the law. In 1995, Prague City Police Chief Rudolf Blazek admitted his men had access to information about criminal suspects that is by law available only to the Czech Republic Police.[182] In 1996, a black-market CD-ROM that listed all telephone numbers in the Czech Republic, including President Vaclav Havel's home number, appeared on the market. Also in 1996, Internet service providers handed over data about their users in response to a police investigation of a bomb found inside a ketchup bottle. Police believe the information was obtained from the Internet and were attempting to determine who accessed it.[183] A poll conducted in January 1997 found that seventy-nine percent of Czechs cite undisturbed privacy as a top personal priority[184] while one released in October 1998 found that seventy-five percent believe that their personal data is misused and two thirds consider data protection a serious problem.[185]

There are currently efforts to update the law as part of the Czech effort to join the European Union. The Office for the State Information System ("USIS") was appointed to develop a new data protection law and create a new data protection agency.[186] The Cabinet approved a draft information policy in May 1998 calling for data protection. In January

182. Tomas Kellner, *Information Protection Laws Must Be Passed Now*, THE PRAGUE POST, Jan. 11, 1995.

183. Marion Blackburn, *Ketchup-Bottle Bomb Sparks Internet Privacy Row*, THE PRAGUE POST, Sept. 25, 1996.

184. *Undisturbed Privacy Top Priority-Poll*, CTK NATIONAL NEWS WIRE, Jan. 23, 1997.

185. *Most People Believe that their Personal Data is Misused – Poll*, CTK NATIONAL NEWS WIRE, Oct. 6, 1998.

186. The Czech Republic Government, *Resolution No. 467, July 1, 1998* (Czech Rep.), *available at* (visited Nov. 10, 1999) <http://www.usiscr.cz/en/dokumenty/domaci/u1998_467.html>.

1999, the government announced its intention to adopt new legislation compatible with the E.U. Directive.[187] The draft Act on Personal Data Protection and on the Competence of the Office Supervising the Personal Data Protection is currently being reviewed by the Government Legislation Council and is expected to be approved by the government in September or October 1999. The E.U. has been pressuring the Republic to move quicker in adopting new legislation. In February 1998, the European Commission set as a "medium term goal" for the Czech Republic to join the Union the establishment of an independent body for supervision of data protection.[188] In November 1998, the Commission was critical of the slow pace of adopting a new data protection law[189] and in April 1999, the European Parliament issued a resolution urging the Czech Republic to put more effort in adopting a new law on data protection.

Wiretapping is regulated under the criminal process law.[190] Police must obtain permission from a judge to conduct a wiretap. The judge can approve an initial order for up to six months. There are special rules for intelligence services. In 1996, the Czech secret service ("BIS") was accused of monitoring politicians, civic and environmental groups such as Greenpeace, including the use of illegal wiretaps.[191] In 1993, Justice Minister Jiri Novak's telephone was reportedly tapped. A secret service employee found a bugging device in the ministry's central telephone switchboard in the middle of September 1993.

The Penal Code covers the infringement of the right to privacy in the definitions of criminal acts of infringement of the home,[192] slander[193] and infringement of the confidentiality of mail.[194] There are also sectoral acts concerning statistics, medical personal data, banking law, taxation, social security and police data. Unauthorized use of personal data systems is considered a crime.[195]

KINGDOM OF DENMARK

The Danish Constitution of 1953 contains two provisions relating to privacy and data protection.[196] The European Convention on Human

187. Resolution No. 70 of 27, Jan. 1999 (Czech Rep.).

188. *E.U. Enlargement: What the Accession Agreements Contain, Country by Country*, EUROPEAN REPORT, Feb. 11, 1998, at 2290.

189. Quentin Peel, *E.U. Warns Applicants on Slow Preparations*, FINANCIAL TIMES, Nov. 5, 1998, at 3.

190. Criminal Process Law, art. 88 (Czech Rep.).

191. CTK NATIONAL NEWS WIRE, Nov. 8, 1996.

192. PENAL CODE § 238 (Czech Rep.).

193. *Id.* § 206.

194. *Id.* § 239.

195. Centre de Recherches Informatique et Droit, *Legal Aspects of Information Services and Intellectual Property Rights in Central and Eastern Europe*, Feb. 1995.

196. DEN. CONST. (adopt. Jun. 5, 1953).

Rights was formally incorporated into Danish law in 1992.

The central rules on data protection in Denmark are found in two Acts. The Private Registers Act of 1978 governs the private sector.[197] The Public Authorities' Registers Act of 1978 governs the public sector.[198] The Private Registers Act not only regulates the registration and further processing of data on natural/physical persons, but also regulates data on legal persons, such as private corporations. A bill for a new Data Protection Act to replace the above two Acts was debated by the Parliament,[199] but was not approved before the end of the session due to opposition from the conservative "Venstre" party, which felt that the legislation was not strong enough. The legislation will be introduced again in October when Parliament returns.

An independent agency, the Data Surveillance Agency (Registertilsynet), enforces both Acts.[200] The Agency supervises registries established by public authorities and private enterprises in Denmark. It ensures that the conditions for registration, disclosure and storage of data on individuals – and to a certain extent also on private enterprises – are complied with. It mainly deals with specific cases on the basis of inquiries from public authorities or private individuals, or cases taken up by the agency on its own initiative.

Wiretapping is regulated by the Penal Code.[201] Other pieces of legislation with rules relating to privacy and data protection include the Criminal Code of 1930,[202] Act on Video Surveillance,[203] the Administrative Procedures Act of 1985,[204] the Payment Cards Act of 1994,[205] and the Access to Health Information Act of 1993.[206] All citizens in Denmark are provided with a Central Personal Registration ("CPR") number that is used to identify them in public registers.

197. Lov nr 293 af 8 juni 1978 om private registre mv [Private Registers Act of 1978] (June 8, 1978, eff. Jan. 1, 1979) (Den.).

198. Lov nr 294 af 8 juni 1978 om offentlige myndigheders registre [Public Authorities' Registers Act of 1978] (June 8, 1978, eff. Jan. 1, 1979).

199. Behandling af personoplysninger [Processing of personal data], Bet. 1345 (1997) (Den.).

200. *Home Page* <http://www.registreilsynet.dk/eng/index.html>.

201. Penal Code § 263 (Den.).

202. Borgerlig Straffelov (Den.).

203. Act No. 278 respecting the prohibiting against video surveillance by private persons, etc, June 9, 1982 (Lovtidende A, No. 44, 1982, p. 644) (Den.).

204. lov nr 571 af 19 desember 1985 om forvaltning (Dec. 19, 1985) (Den.).

205. ovbekendtgørelse nr 811 af 12 september 1994 om betalingskort mv (Sept. 12, 1994) (Den.).

206. lov nr 504 af 30 juni 1993 om aktindsigt i helbredsoplysninger [Data Surveillance Authority] (June 30, 1993) (Den.).

GREENLAND

The original Danish Public and Private Registers Acts of 1979 continue to apply within Greenland, a self-governing territory. The 1988 amendments that brought Denmark into compliance with the Council of Europe's Convention 108 do not apply to Greenland. Greenland is not part of the European Union and therefore has not adopted the E.U. Privacy Directive. Greenland's data protection requirements are much less stringent than those of Denmark and the other nations of the E.U.

REPUBLIC OF ESTONIA

Articles 42, 43 and 44 of the 1992 Estonia Constitution enshrine the right of privacy, secrecy of communications, and data protection.[207] The Riigikogu, Estonia's Parliament, enacted the Personal Data Protection Act in June 1996.[208] The Act protects the fundamental rights and freedoms of persons with respect to processing personal data and in accordance with the right of individuals to obtain freely any information which is disseminated for public use. The Personal Data Protection Act divides personal data into two groups – non-sensitive and sensitive personal data. Sensitive personal data is data which reveals political opinions, religious or philosophical beliefs, ethnic or racial origin, health, sexual life, criminal convictions, legal punishments and involvement in criminal proceedings. Processing of non-sensitive personal data is permitted without the consent of the respective individual if it occurs under the terms set out in the Personal Data Protection Act. Processed personal data is protected by organizational and technical measures that must be documented. Chief processors must register the processing of sensitive personal data with the data protection supervision authority.

In April 1997, the Riigikogu passed the Databases Act.[209] The Databases Act is a procedural law for the establishment of national databases. The law sets out the general principles for the maintenance of databases, prescribes requirements and protection measures for data processing, and unifies the terminology to be used in the maintenance of databases. Pursuant to the Databases Act, the statutes of state registers or databases that were created before the law took effect must comply with the Act within two years. The Databases Act also mandates the establishment of a state register of databases that registers state and local government databases, as well as databases containing sensitive personal data which are maintained by persons in private law. The chief processor of the register has the right to make proposals to the government, to the chief processors of various databases, and to the state infor-

207. EST. CONST.

208. Law on the protection of personal data, RT I 1996, 48, 944 (1996) (Est.).

209. Databases Act, RT* I 1997, 28, 423 (1997) (Est.).

mation systems. He or she would also be responsible for coordinating authority with respect to the expansion, merger or liquidation of databases, interbase cross-usage, or the organization of data processing or data acquisition in a manner aimed at avoiding duplication of effort or substantially repetitive databases.

The Data Protection Department of the Ministry of Internal Affairs is the supervisory authority for the Personal Data Protection Act and the Databases Act. Currently there are only four staff members in the department – the head of department, an IT technology specialist, an organizational specialist, and a legal specialist.[210] The Legal Committee of Parliament exercises supervision over the Data Protection Supervision Authority. The Data Protection Department is currently developing legislation that would make it independent and in compliance with the E.U. Directive.[211]

According to Estonian press reports in November 1996, databases of the financial and police records of thousands of Estonians are easily available on the black market. The records were available on CD-ROM and sold for $4,000 each, and included details of individual's bank loans and police files.[212]

On February 22, 1994, the Riigikogu adopted a law on electronic eavesdropping. The punishment for such activity is a fine and three years imprisonment for general surveillance activity, and five years imprisonment for special measures like opening correspondence or telephone bugging.[213] In May 16, 1996, the Estonian Intelligence Service started an inquiry on the involvement of former Vice Prime Minister Edgar Saavisar in a politically motivated wiretapping scandal. It eventually led to a change of government.[214] At the end of 1997, the intelligence service and parliament were continuing to investigate the Savisaar case.[215] There is a telecommunications bill that will adopt the E.U. telecommunications privacy directive and take effect the beginning of next year. A Digital Signature Law is also being drafted which will be introduced in 1999.

REPUBLIC OF FINLAND

Section 8 of The Constitution Act of Finland provides for protection

210. Ministry of Internal Affairs, Data Protection Department, *Home Page* (visited Nov. 21, 1999) <http://www.sisemin.gov.ee/ako/eng/about.html>.

211. *Id.*

212. THE BALTICS WORLDWIDE, Spr. 1997.

213. Criminal Code, art. 134 (Est.).

214. *Estonian Intelligence Begins Probe into Former Premier Saavisar*, DEUTSCHE PRESSE-AGENTUR, May 16, 1996.

215. La Cour Europeenne des Droits de L'homme [The European Court of the Rights of Man], Affaire Hertel c. Suisse, Arret No. 59/1997/843/1049 (Aug. 25, 1998).

of privacy, secrecy of communications, and data protection.[216] The Personal Data Protection Act 1999 went into effect on June 1, 1999.[217] The law replaced the 1987 Personal Data File Act[218] to make Finnish law consistent with the E.U. Data Protection Directive.

The Data Protection Ombudsman ("DPO") enforces the Act and receives complaints. The office received 450 complaints and conducted 10 investigations in 1998. It also receives 5,000-8,000 requests for advice each year.[219] A Data Protection Board resolves disputes and hears appeals of decisions rendered by the DPO. It also determines if personal information can be exported.[220]

The Finnish government enacted special ordinances that apply to particular personal data systems. These include those operated by the police, such as criminal information systems,[221] the national health service, passport systems, population registers, farm registers, and the agency responsible for motor vehicle registration.[222]

Electronic surveillance and telephone tapping are governed by the Criminal Law. A judge can give permission to tap the telephone lines of a suspect if the suspect is liable for a jail sentence for crimes that are exhaustively listed in the Coercive Criminal Investigations Means Act. Transactional data of a suspect's telecommunications activity can be obtained if the suspect faces at least four months of jail. Electronic surveillance is possible, with the permission of the judge, if the suspect is accused of a drug related crime or a crime that can be punished with more than four years in jail. There were twelve orders for wiretapping in 1997.

Although cases of political telecommunications eavesdropping are rare in Finland, there have been published reports that the Finnish military has either supported Western signals intelligence operations, via its large base at Santahamina on the outskirts of Helsinki, or acquiesced to a Swedish/U.S. eavesdropping collaborative effort from the Swedish embassy in downtown Helsinki.[223] In 1996, the PENET anonymous remailer was forced to shut down after Scientologists demanded that the identity of the users posting critical messages be revealed to the Church.

---

216. FIN. CONST.

217. Personal Data Act, 523/99 (1999) (Fin.).

218. Personal Data Files Act, Law No. 471/87 (1987) (Fin.).

219. Privacy and Office of the Data Protection Ombudsman, *Home Page* (visited Nov. 16, 1999) <http://www.tietosuoja.fi/engl.html>.

220. *Id.*

221. Criminal Records Act, 770/93 (1993) (Fin.).

222. Jorma Kuopus, *Data Protection Regulatory System*, DATA TRANSMISSION AND PRIVACY, (D. Campbell & J. Fisher, eds., 1994).

223. *See* <http://www.qainfo.se/~lb.>.

The court order was later enjoined by the Court of Appeals.[224]

ALAND ISLANDS

The Parliament of the self-governing Aland Islands ("Landsting") passed its own Data Protection Act in 1991 and independently ratified the Council of Europe's Convention 108.[225] Although the Aland Act makes reference to the Finnish Data Protection Act, there was always some resistance by the Aland Swedish-speaking majority to following orders from Helsinki. Constitutionally, the Aland Parliament may nullify Finnish laws on its territory.[226]

FRENCH REPUBLIC

The right of privacy is not explicitly protected in the French Constitution of 1958. The Constitutional Court ruled in 1994 that the right of privacy was implicit in the Constitution.[227]

The Data Protection Act was enacted in 1978 and covers personal information held by government agencies and private entities.[228] Anyone wishing to process personal data must register and obtain permission in many cases relating to processing by public bodies and for medical research. Individuals must be informed of the reasons for collecting information and may object to its processing. Individuals have the right to access and demand corrections. Fines and imprisonment can be imposed for violations. The law is currently being amended to make it consistent with the E.U. Directive. A report was issued in February 1998 by M. Guy Braibant setting out the plan for the changes.[229] The Interministerial Committee on the Information Society on January 19, 1999, announced a legislative framework to protect exchanges and privacy. Under the framework, the law will be modified to incorporate the European directive in law and to strengthen the role of the CNIL. The committee also announced the relaxation of controls on encryption in

224. *See* Temporary Injunction in the Anonymous Remailer Case, *available at* (visited Nov. 11, 1999) <http://www.penet.fi/injunct.html>.

225. *See* Kuopus *supra* note 222.

226. *See* MADSEN, *infra* note 355.

227. FRA. CONST., Jan. 18, 1995, Dèc. 94-352 (1995).

228. Law No. 78-17 of Jan. 7, 1978, J.O., Jan. 25, 1978 (relating to information privacy and freedom) (modified by Law No. 88-227 of Mar. 11, 1988, art. 13, relating to the financial information of politicians, J.O., Mar. 12, 1988; Law No. 92-1336 of Dec. 16, 1992, J.O., Dec. 23, 1992; and Law No. 94-548 of July 1, 1994, J.O., July 2, 1994) (Fra.).

229. Guy Braibant, *Donnees Personnelles et Societe De 'Information: Rapport au Premier Ministre sur la transposition en droit français de la directive no 95/46* [Privacy & The Information Society: Report to the Prime Minister on the change in France's law according to Directive 95/46] Mar. 3, 1998.

France.[230]

The Commission Nationale de L'informatique et des Libertés ("CNIL") is an independent agency which enforces the Data Protection Act and other related laws.[231] The Commission takes complaints, issues rulings, sets rules, conducts audits and issues reports. It reported in its 1998 annual report that it registered 668,000 data processings since 1978.[232] It received 2,900 complaints (up 13% from 1997) and 1,115 written requests (up 35% from 1997) for advice in 1998.[233]

Electronic surveillance is regulated by a 1991 law requiring permission of an investigating judge before a wiretap is installed. The duration of the tap is limited to four months and can be renewed.[234] There were 4,746 orders for national security taps and 1,684 renewals in 1998.[235] The number of taps has been between 4,500 and 4,800 since 1995. The number of judicial wiretaps for criminal cases declined from 11,453 in 1994 to 9,230 in 1997. The law created the Commission National de Contrôl des Interceptions de Sécurité ("CNCIS"), which sets rules and reviews wiretaps each year.

The European Court of Human Rights ruled against France a number of times for violations of Article 8 of the Convention. The Court's 1990 decision in *Kruslin v. France* resulted in the enactment of the 1991 law.[236] Most recently, the court fined France 25,000 francs for wiretap law violations.[237] There were many cases of illegal wiretapping, including most notably a long running scandal over an anti-terrorist group in the office of President Mitterand monitoring the calls of journalists and opposition politicians.[238] The CNCIS estimated that there were over 100,000 illegal taps conducted by private companies and individuals in 1996, many on the behalf of government agencies. A decree was issued in

230. Comité interministériel pour la société de l'information ("CISI"), Jan. 19, 1999, *available at* (visited Nov. 11, 1999) <http://www.internet.gouv.fr/francais/index.html>.

231. Commission Nationale del'informatique et des Libertés ("CNIL"), *Home Page* (visited Nov. 11, 1999) <http://www.cnil.fr>. The web page contains extensive materials on the applications of the law and other international materials.

232. The CNIL's 18th Report 1998, Commission Nationale de l'informatique et des Libertés, July 1999.

233. *Id.*

234. Law No. 91-636 of July 10, 1991(relating to telecommunications privacy) (Fra.).

235. 7e rapport d' activité 1998, Commission Nationale de contrôl des interceptions de sécurité, May 1999 (Fra.).

236. Kruslin v. France, 176-A, Eur. Ct. H.R. (ser. A) (1990).

237. *la France condamnée par la Cour européenne des droits de l'homme* (France comdenmmed by the European Court of Human Rights), LE MONDE, Aug. 27, 1998.

238. *See* CAPITAINE PAUL BARRIL, GUERRES SECRÈTES À L'ÉLYSÉE (Albin Michel ed., 1996); FRANCIS ZAMPONI, LES RG À L'ÉCOUTE DE LA FRANCE: POLICE ET POLITIQUE DE 1981 À 1997 (1998).

1997 to limit the dissemination of tapping equipment.[239]

The tort of privacy was first recognized in France as far back as 1858,[240] and was added to the Civil Code in 1970.[241] There are additional specific laws on administrative documents,[242] archives,[243] video surveillance,[244] correspondence,[245] and employment.[246] There are also protections incorporated in the Penal Code.[247]

There is currently a major debate over the creation of the Système de Traitement des Infractions Constatées ("STIC"). Civil rights groups in April 1999 called for the dismantling of database, an initiative by the Minister of Interior to merge police and other records.

FEDERAL REPUBLIC OF GERMANY

Article 10 of the Basic Law protects the secrecy of communications. Attempts to amend the Basic Law to include a right to data protection were discussed after reunification when the constitution was revised and were successfully opposed by the then-conservative political majority. In 1983, the Federal Constitutional Court, in a case against a government census law, acknowledged formally an individual's "right of informational self-determination" which is limited by the "predominant public interest." The central part of the verdict stated,

> Who can not certainly overlook which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be essentially hindered in his capability to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens could not know any longer who what and when in what situa-

239. 5e rapport d' activité 1997, Commission national de contrôl des interceptions de sécurité, May 1998 (Fra.).

240. *See supra* note 20.

241. C. CIV., Art. 9, Stat. No. 70-643 [Civil Code] (July 17, 1970) (Fra.).

242. Law No. 78-753 of July 17, 1978, J.O., July 18, 1978, p. 2851, *available at* (visited Nov. 11, 1999) <http://www.cnil.fr/textes/text05.htm> (administrative documents).

243. Law No. 79-18 of Jan. 3, 1979, J.O., Jan. 5, 1979, p. 43, rectificatif au J.O., Jan. . 6, 1979, p. 55, *available at* (visited Nov. 11, 1999) <http://www.cnil.fr/textes/text052.htm> (archives).

244. Law No. 95-73 of Jan. 21, 1995, J.O., Jan. 24, 1995, p. 1249, *available at* (visited Nov. 11, 1999) <http://www.cnil.fr/textes/text054.htm> (video surveillance); *see also* Decree No. 96-926 of Oct. 17, 1996, J.O., Oct. 20, 1996, p. 15432, *available at* (visited Nov. 11, 1999) <http://www.cnil.fr/textes/text055.htm>; Circular of Oct. 22, 1996, J.O. Dec. 7, 1996, p. 17835, *available at* <http://www.cnil.fr /textes/text056.htm> (relating to the application of the article of law no. 95-73 of Jan. 21, 1995 on video surveillance) (Fra.).

245. Code of Post and Telecommunications, L. 41 (Fra.).

246. Law No. 92-1446 of Dec. 31, 1992, J.O., Jan. . 1, 1993, p. 19, *available at* (visited Nov. 11, 1999) <http://www.cnil.fr/textes/text053.htm> (relating to employment) (Fra.).

247. C. PÉN. [Penal Code], art. 368 (Fra.).

tions knows about them.[248]

This landmark court decision derived the "right of informational self-determination" directly from Article 2 of the German Constitution that declares protective personal rights (Persönlichkeitsrechte).

In Germany, the first data protection law was passed in the Land of Hessen in 1970. It was the first data protection law worldwide. In 1977, a Federal Data Protection Law followed, which was reviewed in 1990.[249] The general purpose of this law is "to protect the individual against violations of his personal right (Persönlichkeitsrecht) by handling person-related data." The law covers collection, processing and use of personal data collected by public federal and state authorities, as long as there is no state-regulation, and of non-public offices, as long as they process and use data for commercial or professional aims. Changes to make the law consistent with the E.U. Directive are currently being developed by the government. All of the 16 Länder have their own specific data protection regulations that cover the public sector of the Länder administrations.

The Federal Data Protection Commission (Bundesbeauftragter für den Datenschutz) is responsible for supervision of the Data Protection Act.[250] There are also commissions in each of the Länders who enforce the Länder data protection acts.[251] Supervision, however, is carried out for the private sector by the Land authority designated by the Land data protection law (usually the Land Data Protection Commissioner). In 1996, the Berlin Data Protection Commissioner reached an agreement with Citibank on the use of Railway Cards as Visa cards. The agreement may be an important precursor for trans-border data flows to the U.S. and other countries without privacy laws when the E.U. Directive goes into effect in October 1998.[252]

Wiretapping is regulated by the "G10-Law" and requires a court order for criminal cases.[253] In July 1999, the Supreme Court issued a deci-

248. BverfGE 65,1.

249. Federal Act on Data Protection, Jan. 27 1977 (Bundesgesetzblatt, Part I, No 7, 1 Feb. 1977, amended 1990), *available at* Datenschutz und Recht (visited Nov. 12, 1999) <http://www. datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm>.

250. Resolution of the Conference of Data Protection Commissioners of the Federation and the Laender, Apr. 29, 1996, *available at* Datenschutz und Recht <http://www.datenschutz-berlin.de/sonstige/behoerde/bundes.htm>.

251. Links to the Ländesbeauftragten für den Datenschutz [Data Protection Laws for all of the Länder] are available at Daten Schutz Berlin, *Die Landesbeauftragen für den Datenschutz* (visited Nov. 7, 1999) <http://www.datenschutz-berlin.de/sonstige/behoerde/ldbauf.htm>.

252. Alexander Dix, *Case Study: North America and the European Directive - The German RailwayCard: A model contractual solution of the "adequate level of protection" issue?*, DATEN SCHUTZ BERLIN, Sept. 1996.

253. Gesetz zur Beschraenkung des Brief-, Post- und Fernmeldegeheimnisses - Gesetz zu Artikel 10 des Grundgesetzes (GG10) [Law on restriction of the right of secrecy of let-

sion on a 1994 law which authorizes warrantless automated wiretaps (screening method) of international communications by the intelligence service ("BND") for purposes of preventing terrorism and the illegal trade in drugs and weapons.[254] The court ruled that the procedure did violate privacy rights protected by the Basic Law, but that screening could continue as long as the intelligence service did not pass on the information to the local police and the Parliament must enact new rules by June 2001. It was reported that the BND has 1,400 operatives listening in on satellite communications.[255]

After a fiercely fought six-year political debate, a two-third majority of the German parliament eventually approved a change to Section 13 of the Constitution in April 1998, making it legal for police authorities to place bugging devices even in private homes, provided there is a court order. The change was the provision for the "Law for the enhancement of the fight against organized crime," which became effective on May 9, 1998.

In addition, wherever they deal with the handling of personal information on natural persons either directly or by amendments, nearly all German laws contain references to the respective data protection law or carry special sections on the handling of personal data that reflect the right to privacy. Most recently there were a number of laws relating to communications privacy. The Telecommunications Carriers Data Protection Ordinance of 1996 protects privacy of telecommunications information.[256] The Information and Communication Services (Multimedia) Act of 1997 sets protections for information used in computer networks.[257] The Act also sets out the legal requirements for digital signatures. The German Federal Supreme Court ruled in March 1999 that Commerzbank AG could not include a clause in their contracts that clients agree to receive telephone "consulting." In April 1998, a law was passed that allows the Bundeskrimalamt to run a nationwide data-bank of genetic profiles related to criminal investigations and convicted offenders. One month later, the Bundesgrenzschutz, originally a para-military border police force, and now responsible among other tasks for railways and

---

ters, mail and telecommunication - Law applying to article 10 of the constitution], G10 BGBl. I, p. 949 (Aug. 13, 1968) (amended by BGBl. I, p.3186ff (Oct. 10, 1994)); Verbrechensbekaempfungsgesetz [Crime-fighting law].

254. BverfGE 93, 181 – Rasterfahndung (July 5, 1995).

255. Imre Karacs, *German Phone Taps are Routine*, THE INDEPENDENT, July 15, 1999.

256. Telecommunications Carriers Data Protection Ordinance ("TDSV"), as of July 12, 1996 (Federal Law Gazette I p 982), Federal Ministry of Posts and Telecommunications.

257. Federal Act Establishing the General Conditions for Information and Communication Services - Information and Communication Services Act (Informations - und Kommunikationsdienste - Gesetz - IuKDG) 13 June 1997; *see also* Resolution of the Conference of Data Protection Commissioners of the Federation and the Länder of Apr. 29, 1996, on key points for the regulation in matters of data protection of online services.

stations, received permission to check persons' identities and baggage without any concrete suspicion.

HELLENIC REPUBLIC (GREECE)

Articles 9 and 19 of the Constitution of Greece protect the rights of privacy and secrecy of communications.[258] The Law on the Protection of Individuals with regard to the Processing of Personal Data was approved in 1997.[259] Not only was Greece the last member of the E.U. to adopt a data protection law, but its law was written to apply the E.U. Directive into Greek law. There were major protests during the ratification of the Schengen Agreement for border controls and information sharing. According to news reports, police used tear gas to disperse a group of about 1,000 protesters, including Orthodox priests, when they tried to push their way into Parliament as the pact was being debated.[260]

The Protection of Personal Data Authority is an independent public authority set up under the law. Its mission is to supervise the implementation of the law and other rulings that pertain to the protection of individuals against the processing of personal data. It also exercises other powers delegated to it from time to time.

The law requires that police wishing to conduct telephone taps obtain court permission.[261] However, there are continuing reports of government surveillance of human rights groups, Orthodox religious groups, and activist members of minority groups by government agents who are conducting illegal wiretapping and interception of mail.[262] In June 1994, a parliamentary investigation committee recommended the indictment of former Prime Minister Mitsotakis and 30 persons from his administration on charges of wiretapping political opponents from 1989 to 1991. In January 1995, the Parliament voted to drop all charges against Mitsotakis, and the Supreme Court ordered the dismissal of other charges in April 1995. The late Greek Prime Minister Andrea Papandreou was also investigated for illegally wiretapping his political opponents.[263]

The law of 1599/1986 regulates the use of the Single Register Code

---

258. CONST. GREECE (June 11, 1975), *available at* <http://www.uni-wuerzburg.de/law/gr00000_.html>.

259. Law no. 2472 on the Protection of Individuals with regard to the Processing of Personal Data.

260. *The Reuters European Community Report*, REUTERS, June 10, 1997.

261. Law no. 2225/94.

262. U.S. DEPARTMENT OF STATE, GREECE COUNTRY REPORT ON HUMAN RIGHTS PRACTICES FOR 1997 (Jan. 30, 1998). *See also* GREECE REPORT, HUMAN RIGHTS WATCH WORLD REPORT (1998).

263. REUTERS WORLD SERVICE, Nov. 20, 1996.

Number ("EKAM").[264] The number is the official national ID number for the population register, ID card, voting register, passport number, tax number, driver's license number, and other registers. Until the 1997 data protection law was enacted, this protected the privacy of information in those registers. The European Parliament passed a resolution in 1993 calling on the Greek government not to place religion on its national ID cards.[265]

Greece 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).[266]

SPECIAL ADMINISTRATIVE REGION OF HONG KONG

Following the Peoples' Republic of China's resumption of sovereignty over Hong Kong on July 1, 1997, the constitutional protections of privacy are contained in the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China. Also relevant is Article 17 of the International Covenant on Civil and Political Rights, which was incorporated into Hong Kong's domestic law with the enactment of the Bill of Rights Ordinance.[267] Article 39 of the Basic Law provides that the Covenant, as applied to Hong Kong, shall remain in force and implemented through the laws of Hong Kong.

In 1995, Hong Kong enacted its Personal Data (Privacy) Ordinance,[268] and most of its provisions took effect in December 1996. The legislation enacts most of the recommendations made by the Hong Kong Law Reform Commission following its six-year comparative study.[269] The statutory provisions adopt features of a variety of existing data protection laws, and the draft version of the E.U. Directive is also reflected in several provisions. The Ordinance does not differentiate between the public and private sectors, although many of the exemptions will more readily apply to the former. A broad definition of "personal data" is

264. Law no 1599/1986 on the relationship of a new type of identification card and other provisions.

265. *The Reuters European Community Report*, REUTERS, Apr. 23, 1993.

266. Council of Europe, *Chart of Signatures and Ratifications: ETS No. 108* (signed Feb. 17, 1983, enacted Aug. 11, 1995, entered into force Dec. 01, 1995), *available at* <http://www.coe.fr/tablconv/108t.htm>; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Jan. 28, 1981.

267. Chapter of Laws (Cap) 383: 288, *available at* (visited Nov. 11, 1999) <http://www.justice.gov.hk>.

268. Chapter of Laws (Cap) 486, *available at* (visited Nov. 11, 1999) <http://www.justice.gov.hk>; *see generally* M. Berthold & R. Wacks, *Data Privacy Law in Hong Kong*, FT LAW & TAX (1997).

269. HONG KONG LAW REFORM COMMISSION, 1994 Report on the Law Relating To The Protection of Personal Data. Information on the Hong Kong Law Reform Commission is available at (visited Nov. 11, 1999) <http://www.info.gov.hk>.

adopted so as to encompass all readily retrievable data recorded in all media that relates to an identifiable individual. The Ordinance does not attempt to differentiate personal data according to its sensitivity. The processing of personal data must conform to data protection principles based on those of the OECD. The six principles regulate the collection, accuracy, use and security of personal data, as well as requiring data users to be open about data processing, and conferring on data subjects the right to be provided a copy of their personal data and to effect corrections. The Ordinance imposes additional restrictions on certain processing, namely data matching, trans-border data transfers, and direct marketing. Data matching requires the prior approval of the Privacy Commissioner. The transfer of data to other jurisdictions is subject to restrictions that mirror those of the E.U. Directive. Also based on the directive is the requirement that upon first use of personal data for direct marketing purposes, a data user must inform the data subject of the opportunity to opt-out from further approaches.

The Ordinance establishes the Office of the Privacy Commissioner to promote and enforce compliance with statutory requirements.[270] The Commissioner is given strong enforcement powers based on those contained in the UK Data Protection Act. In addition to investigating complaints, the Commissioner may initiate his own investigations of reasonably suspected contraventions. He may also conduct audits of selected data users. A contravention of any provision other than a data protection principle is a criminal offense. A contravention causing the data subject damage, including injured feelings, is a basis for claiming compensation. The Commissioner is empowered to designate classes of data users required to publicly register the main features of their data processing. The Commissioner may issue codes of conduct to provide guidance on compliance with the Ordinance's necessarily general provisions. The provisions of a code are legally subordinate, but have evidential relevance in determining whether a contravention of the Ordinance has occurred. To date, the Commissioner issued two codes: the code on the use of personal identifiers[271] and of credit information.[272] As of

270. *See* PRIVACY COMMISSIONER, FIRST ANNUAL REPORT 1996-97. The Office of the Privacy Commissioner was established with a very small staff with only four officers investigating complaints and compliance issues under the direction of the assistant commissioner. *Id. See* SOUTH CHINA MORNING POST, Jan. 15, 1997. In the first 6 months of operation, the Commissioner received 52 complaints and had publicly expressed concern that his staff may be unable to cope. *Id.*

271. The Code of Practice on the Identity Card Number and other Personal Identifiers were gazetted on Dec. 19, 1997. With the exception of the requirement restricting the issue of a card with an identity card number printed on it (which will take effect on Dec. 19, 1998), the requirements of the code will take effect on June 19, 1998.

272. The Code of Practice on Consumer Credit Data was issued on Feb. 27, 1998, and will take effect on Nov. 27, 1998. A summary is available at the commissioner's website at

March 31, 1999, the Office has received 35,968 inquiries (19,994 in 1998-1999), heard 723 complaints (418 in 1998-1999) and conducted 119 formal investigations, and ruled in 62 cases that there was a violation of the Act. The Office also issued 147 advisory/warning notices, 14 enforcement notices and referred 18 cases to the police for prosecution.[273]

A Hong Kong court ruled in June 1999 against attempts to subject Xinhua, the Chinese News agency, which acted as the Chinese government representative in Hong Kong, to the Privacy Ordinance. In December 1996, pro-democracy legislator Emily Lao demanded access to the secret dossier that Xinhua maintained on her. Xinhua refused to respond and the Hong Kong government declined to take action. She filed suit, but the court quashed her attempt to subpoena the director.[274]

Presently the interception of communications is regulated by the Telecommunications Ordinance[275] and the Post Office Ordinance.[276] These enactments provide sweeping powers of interception upon public interest grounds. The vagueness of powers and lack of procedural safeguards are inconsistent with the International Covenant of Civil and Political Rights and the Basic Law. No official figures are released on the number of intercepts, which are believed to be widespread and efforts to make the numbers public were rebuffed in the name of confidentiality.[277] A detailed set of reform proposals released by the Hong Kong Law Reform Commission[278] in 1996, resulted in two legislative initiatives. In early 1997, the government released a draft bill for public consultation regulating the interception of communications. When that initiative stalled, James To, an independent legislator, introduced a private members bill, the last enactment passed by the colonial legislature prior to July 1, 1997. That enactment has yet to be brought into force and, to date, the government has declined to indicate when any legislation regulating the interception of communications will take effect. In January 1999, Mr. To introduced another bill to force the ordinance to go into effect.

Privacy Commissioner's Office (United Kingdon) (visited Nov. 7, 1999) <http://www.pco.org.uk>.

273. Operations Division, Office of the Privacy Commissioner for Personal Data, May 1999.

274. *HK Court Blocks Lawsuit Against China News Agency*, REUTERS, Jun 8, 1999.

275. Section 33, Chapter of Laws (Cap) 106.

276. Section 13, Chapter of Laws (Cap) 98.

277. *Phone Tap Figures to Remain Secret*, SOUTH CHINA MORNING POST, Oct. 1, 1998.

278. Hong Kong Law Reform Commission, Hong Kong Law Reform Commission's 1996 Report on Privacy: Regulating the Interception of Communications. Information on the Hong Kong Law Reform Commission is available at <http://www.info.gov.hk>.

REPUBLIC OF HUNGARY

Article 59 of the Constitution of the Republic of Hungary provides for privacy, data protection and secrecy of communications.[279] In 1991, the Supreme Court ruled that a law creating a multi-use personal identification number violated the constitutional right of privacy.[280]

Act No. LXIII of 1992 on the Protection of Personal Data and Disclosure of Data of Public Interest covers the collection and use of personal information in both the public sector and private sector. It is a combined Data Protection and Freedom of Information Act. Its basic principle is informational self-determination.[281] Hungary is an applicant for E.U. membership and it is anticipated that only minor changes are required to make the Act compliant with the E.U. Directive. In June 1999, the Parliament amended the Act to treat "data controllers" and "data processors" differently like in the E.U. Directive. In the year 2000, the whole Act will be revised and made consistent with the Directive.

The Parliamentary Commissioner for Data Protection and Freedom of Information oversees the 1992 Act.[282] Besides acting as an ombudsman for both data protection and freedom of information, the Commissioner's tasks include: maintaining the Data Protection Register, and providing opinions on DP and FOI-related draft legislation as well as each category of official secrets. The Commissioner, along with the two other Parliamentary Commissioners – one for human rights in general, the other for the ethnic minorities, was elected for the first time on June 30, 1995, for a six year term.

The Commission was very active reviewing cases involving personal information.[283] When reviewing unlawful national security controls in 1995, in 797 cases, unlawful information gathering practices were found and the files had to be destroyed. In 1995, the names and addresses of the winners of the largest lottery jackpot were broadcast on television against the will of the individuals. In a case involving unlawful gathering of personal data of patients of voluntary drug treatment institutions in 1997, the police had to return the lists to the hospital. The Commission registered 19,376 databases and conducts about 1,000 examinations each year.[284]

279. A MAGYAR KÖZTRÁRSASÁG ALKOTOMÁNYA [Const. of the Rep. of Hung.].

280. 30 MK. 805 (Dec. No. 15-AB) (Apr. 13, 1991) (Hung.).

281. Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest, Act LXIII PTK. (1992) (Hung.).

282. Parliamentary Commissioners' Office (Hung.), *Home Page* (visited Nov. 19, 1999) <http://www.obh.hu/>.

283. *See* HUNGARIAN CIVIL LIBERTIES UNION, DATA PROTECTION AND FREEDOM OF INFORMATION, 1997.

284. Letter from László Majtényi, *Parliamentary Commissioner for Data Protection and Freedom of Information*, Aug. 4, 1999.

Surveillance by police requires a court order and is limited to cases investigating crimes punishable by more than five years imprisonment.[285] Surveillance by national security services requires the permission of a specially appointed judge or the Minister of Justice who can authorize surveillance for up to 90 days.[286] There were a number of scandals involving secret service spying on political opponents, environmental activists and ethnic minorities. The Parliamentary National Security Committee is currently investigating the illegal surveillance of members of the political party Fidesz, after documents were found by the government. Prime Minister Viktor Orbán said the surveillance was conducted by former members of the secret service now employed by private companies.[287] In April 1998, the government issued a decree ordering phone companies that offer cellular service to modify their systems to ensure that they could be intercepted. The cost was estimated to be HUF ten billion.[288]

Many laws contain rules for handling personal data including addresses,[289] marketing records,[290] universal identifiers,[291] medical information,[292] police information,[293] public records,[294] employment,[295] telecommunications,[296] and national security services.[297] The Criminal Code also has provisions on privacy.[298]

285. Act XXXIV Tv. (1994) (Hung.) (regarding Police procedure).

286. Act LXXV Tv. (1995) (Hung.) (regarding the National Security Services).

287. *Fidesz 'Bugging' Probe Underway*, THE BUDAPEST SUN, Sept. 3, 1998.

288. *Technical costs of phone tapping estimated at HUF 10bn*, MTI ECONEWS, Apr. 17, 1998.

289. Act LXVI Tv. (1992) (Hung.) (regarding the register of personal data and addresses of citizens).

290. Act CXIX Tv. (1995) (Hung.) (regarding the use of name and address information serving the purposes of research and direct marketing).

291. Act XX Tv. (1996) (Hung.) (regarding the identification methods replacing the universal personal identification number, and the use of identification codes).

292. Act XLVII Tv. (1997) (Hung.) (regarding the use and protection of medical and related data).

293. Act XXXIV Tv. (1994) (Hung.) (regarding the Police Chapter VIII: "Data handling by the Police").

294. Act LXVI Tv. (1995) (Hung.) (regarding public records, public archives, and the protection of private archives, restricting rules on the publicity of documents containing personal data).

295. Act IV Tv. (1991) (Hung.) (regarding furthering employment and provisions for the unemployed).

296. Act LXXII Tv. (1992) (Hung.) (regarding telecommunications).

297. Act CXXV Tv. (1995) (Hung.) (regarding the National Security Services etc.).

298. Criminal Code, Sections 177-178. *available at* Privacy International, *Hungarian Criminal Code Privacy Excerpts* (visited Nov. 17, 1999) <http://www.privacy.org/pi/countries/hungary /hungary_criminal_code.html>.

REPUBLIC OF ICELAND

Section 72 of the Constitution protects privacy and the secrecy of communications.[299] The Act on the Registration and Handling on Personal Data applies to government agencies and the private sector for physical and electronic files.[300] All persons wishing to process personal data must register.

There are limitations on processing sensitive data, disclosing information and linking databases. Individuals have a right to access and correct information. There are additional rules for credit information and marketing. Video surveillance and recording is also covered under the act. A government commission headed by the Minister of Industry and Commerce released a report in 1997 calling for an update of the current legislation to make it consistent with the E.U. Directive. The report also suggested that the legislation should address issues raised by digital identity cards and sharing of government information.[301]

In June 1999, there was a formal decision to incorporate the E.U. Data Protection Directive into European Economic Area. Legislation to amend the Icelandic law is expected to be introduced into the Parliament in October 1999. The Icelandic Data Protection Commission enforces the Act. The Commission maintains the registry of activities and can investigate and issue rulings. In 1998, the Commission registered 509 activities.

In December 1998, the Parliament approved a bill that would allow the creation of a nationwide centralized health database.[302] The Government plans give an exclusive 12-year license for the database to American bio-tech company deCODE Genetics which will create a nationwide genetic database of the entire Icelandic population based on 30 years of patients records. The company is spending $200 million over the next five years for research. Patients were required to opt out of the database by June 1999. After that date, their information could not be removed. The Privacy Commission is currently drafting requirements on technical, security and organizational requirements and will be maintaining the keys to identify individuals.[303] This proposal was very controversial both in Iceland and with medical and privacy experts around

299. CONST. ICE. (June 5, 1953).

300. Act on the Registration and Handling on Personal Data, No. 121, Dec. 28, 1989. The law was originally introduced in 1979 and renewed in 1984 and 1989 after the law automatically expired after five years because of the 'sunset' provisions attached to laws by Iceland's Parliament.

301. Icelandic Government's Vision of the Information Society, *Guidance and Vigilance in the Fields of Law and Ethics* (Feb., 1997) <http://eldur.stjr.is/framt/vision05.htm>.

302. Act on a Health Sector Database no. 139/1998 (Ice.) (Dec. 17, 1998).

303. *See generally* MANNVERND, Association for Ethics in Science and Medicine, *Home Page* (visited Nov. 19, 1999) <http://simnet.is/mannvernd/english/home.html>; Eliot

the world. The Icelandic Medical Association is opposing the effort and many doctors are refusing to hand over their patients' records without consent. The World Medical Association in April 1999 supported the Icelandic Medical Association's opposition to the database.[304] Security experts examined the database and found that the encryption does not protect the identity of the individuals.[305] At their annual meeting in Santiago de Compostela, Spain, in September 1998, the other European Data Protection Commissioners recommended that the Icelandic authorities reconsider the project in light of the fundamental principles laid down in the European Convention on Human Rights, the Council of Europe Convention, Recommendation (97)5 on medical data, and the EC Directive.

Under the Law on Criminal Procedure, wiretapping, tape recording or photographing without consent requires a court order and must be limited to a short time. After the recording is complete, the target must be informed and the recordings destroyed after they are no longer needed.[306] There were 42 wiretaps authorized between 1992 and February 1996.[307] Complaints against the orders can be submitted to the Supreme Court. Chapter XXV of the Penal Code also penalizes violations of privacy such as violating the secrecy of letters and revealing secrets to the public.

REPUBLIC OF INDIA

The Constitution of 1950 does not expressly recognize the right to privacy.[308] However, the Supreme Court first recognized in 1964, that there is a right of privacy implicit in the Constitution under Article 21 of the Constitution which states, "No person shall be deprived of his life or personal liberty except according to procedure established by law."[309]

There is also a right of privacy guaranteed by Indian laws. Unlawful attacks on the honor and reputation of a person can invite an action in tort and/or criminal law.[310] The Public Financial Institutions Act of

---

Marshall, *Iceland's Blond Ambition: A Nordic Country Cashes in on its Isolated Gene Pool*, MOTHER JONES, May/June 1998.

304. Nigel Duncan, *World Medical Association Opposes Icelantic Gene Database*, EBMJ, Apr. 24, 1999.

305. Ross Anderson, *Icelantic Medical Database is Insecure*, EBMJ, July 3, 1999.

306. Articles 86-87, Law on Criminal Procedure.

307. *Fotry-two Telephone Taps Since 1992*, DAILY NEWS FROM ICELAND, (Feb. 9, 1996) <http://www.icenews.is/daily/1996/09feb96.html>.

308. CONST. INDIA (Nov. 1949).

309. Kharak Singh vs State of UP, 1 SCR 332 (1964); *see* Mr. R.C. Jain, National Human Rights Commission, India, Indian Supreme Court on Right to Privacy, July, 1997.

310. UN, Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Third periodic reports of States parties due in 1992 Addendum -India/1, June 17, 1996.

1993 codifies India's tradition of maintaining confidentiality in bank transactions.

There is no general data protection law in India. The National Task Force on IT and Software Development, set up by the Prime Minster's Office in May 1998, submitted an "IT Action Plan" to Prime Minister Vajpayee in July 1998 calling for the creation of a "National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data." It examined the UK Data Protection Act as a model and recommended a number of cyber-laws including ones on privacy and encryption.[311] The Act was expected to be drafted by the end of 1998.[312]

Wiretapping is regulated under the Indian Telegraph Act of 1885. An order for a tap can be issued only by the Union home secretary or his counterparts in the states. A copy of the order must be sent to a review committee and directed to be set up by the high court. Tapped phone calls are not accepted as primary evidence in India's courts. There have been numerous phone tap scandals in India, resulting in the 1996 decision by the Supreme Court, which required the government to promulgate rules regulating taps. The Court ruled in 1996 that wiretaps are a "serious invasion of an individual's privacy."[313] However, illegal wiretapping by government agencies appears to be continuing. According to prominent Non-Government Organizations, the mail of many NGOs in Delhi and in strife-torn areas continues to be subjected to interception and censorship.[314] There was considerable discussion about a rumored new government proposal on Internet surveillance. The plan would require Internet service providers to connect their routers to state security agencies such as the Intelligence Bureau and the Research and Analysis Wing so their traffic can be monitored.[315]

IRELAND

The Constitution of Ireland does not explicitly recognize the right to privacy.[316] The High and Supreme Courts ruled that privacy is pro-

311. NATIONAL TASK FORCE ON IT & SD, BASIC BACKGROUND REPORT, June 9, 1998, *available at* <http://it-taskforce.nic.in/it-taskforce/bgnew.htm>.

312. *India: Taskforce Suggests Slew of Measures*, THE HINDU, July 7, 1998.

313. Peoples Union for Civil Liberties ("PUCL") vs. The Union of India & Another, Dec. 18, 1996, on Writ Petition (C) No. 256 of 1991.

314. SOUTH ASIA HUMAN RIGHTS DOCUMENTATION CENTRE, ALTERNATE REPORT AND COMMENTARY TO THE UNITED NATIONS HUMAN RIGHTS COMMITTEE ON INDIA'S THIRD PERIODIC REPORT UNDER ARTICLE 40 OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, (July, 1997).

315. *See* Bhvana Vig, *New Law to let Govt Intercept Net Mail,* INTERNET EDITION OF INDIAN EXPRESS, Dec. 14, 1998.

316. CONST. IR.

tected under Article 40.3.1 and other provisions.[317] The Supreme Court ruled in 1987 that the warrantless wiretapping of two journalists was a violation of the Constitution, finding,

> The right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State .... The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This cannot be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with.[318]

The Data Protection Act of 1988 covers both the private and public sectors. It regulates the collection, processing, keeping, use and disclosure of personal information that is processed automatically. Individuals have a right to access and correct incorrect information. Information can only be used for specified and lawful purposes and cannot be used or disclosed. Additional protections can be ordered for sensitive data. Criminal penalties can be imposed for violations. There are broad exemptions for national security, tax, and criminal purposes. A draft bill is currently being reviewed by the Attorney General that would revise the Act to make it consistent with the E.U. Directive. The Ministry of Justice announced that they are delaying the introduction of the bill until the fall of 1999.[319] Misuse of data is also criminalized by the Criminal Damage Act 1991.

The Act is enforced by the Data Protection Commissioner. The Commission can investigate complaints, prosecute offenders, sponsor codes of practice, and supervise the registration process. The Commission generally receives about 1,700 inquiries each year and reviews between twenty and thirty complaints.[320] In 1996, the Commissioner criticized a proposal to introduce a social services card to all citizens that could become a national ID card.[321]

Wiretapping and electronic surveillance is regulated under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act. The Act followed a 1987 decision of the Supreme Court ruling that wiretaps of journalists violated the constitution (see above). In April 1998, the Garda investigated allegations that several journalists who uncovered a scandal at the National Irish Bank had their cellular

317. *See* The Law Reform Commission of Ireland, *Consultation Paper on Privacy: Surveillance and the Interception of Communications*, Sept., 1996.

318. Kennedy, et al.v. Ireland [1987] I.R. 587.

319. Karlin Lillington, *Data Protection Law to be Delayed Until Autumn*, THE IRISH TIMES, July 19, 1999.

320. Karlin Lillington, *EU and US at Odds Over Privacy*, THE IRISH TIMES, July 17, 1998, at 58.

321. Alison O'Connor, *Social Services Card Opposed by Data Commissioner*, THE IRISH TIMES, Oct. 1, 1996, at 3.

phone conversations intercepted.[322] The Law Reform Commission recommended a new bill in July 1998 that would make illegal the invasion of a person's privacy through secret filming, taping and eavesdropping and the publication of information received from the surveillance.[323] There were protests in the Irish Parliament in June 1999 after reports that the British government tapped all telephone calls, email, telexes and faxes between Ireland and Britain from a thirteen-story tower in Capenhurst, Cheshire, from 1989 until 1999. The Irish government asked its ambassador in the UK to demand more information on the acts.[324]

STATE OF ISRAEL

Section 7 of The Basic Law: Human Dignity and Freedom protects privacy and the secrecy of communications.[325] According to Supreme Court Justice Mishael Cheshin, this elevated the right of privacy to the level of a basic right.[326]

The Protection of Privacy Law regulates the processing of personal information in computer data banks.[327] The law set out 11 types of activities that violated the law and could subject the person to criminal or civil penalties. Holders of data banks of over 10,000 names must register. Information in the database is limited to purposes for which it was intended and must provide access to the subject. There are broad exceptions for police and security services. It also sets up basic privacy laws relating to spying, publication of photographs and other traditional privacy features. The law was amended in 1996 to broaden the databases covered such as those used for direct marketing purposes and also increases penalties.[328]

The Registrar of Databases within the Ministry of Justice enforces the Act. The Registrar maintains the register of databases and can deny registration if he believes that it is used for illegal activities. The regis-

---

322. Catherine Cleary, *Garda to Investigate Surveillance Allegations*, THE IRISH TIMES, Apr. 18, 1998.

323. Mark Brennock, *Report Recommends Outlawing Secret Filming and Surveillance*, THE IRISH TIMES, July 30, 1998, at 8.

324. Alan Murdoch & Andrew Buncombe, *Dublin Wants to Know Why UK Snooped*, THE INDEPENDENT , July 17, 1999, at 5.

325. The Basic Law: Human Dignity and Freedom (5752 - 1992). Passed by the Knesset on the 21st Adar, 5754 (Mar. 9, 1994), *available at* (visited Nov. 11, 1999) <http://www.israel-mfa.gov.il/gov/laws/dignity.html>.

326. ISRAELI BUSINESS LAW AN ESSENTIAL GUIDE at 30.01.

327. The Protection of Privacy Law 5741-1981, 1011 Laws of the State of Israel 128. Amended by the Protection of Privacy Law (Amendment) 5745-1985.

328. Law of Apr. 11, 1996.

trar can also investigate and enforce the Act.[329] As of mid-1998, 5,200 databases were registered.[330] A public council for the protection of privacy was also set up to advise the Justice Minister on legislative matters related to the Protection of Privacy Law and its subsidiary regulations and orders, sets guidelines for the protection of computerized databases, and guides the Registrar of Databases in his work. Under the 1996 amendments, a more independent supervisory authority is being created.

Interception of communications is governed by the Secret Monitoring Law of 1979, which was amended in 1995 to tighten procedures and cover new technologies such as cellular phones and email. It also increased penalties for illegal taps and allowed interception of privileged communications such as with a lawyer or doctor.[331] The police must receive permission from the President of the District Court in order to intercept any form of wire or electronic communications or plant microphones for a period up to three months, which can be renewed. According to the Israeli government, "The number of wiretap permits given to the Police has averaged roughly 1,000 - 1,100 annually over the last several years. Roughly half of these wiretap permits are given in connection with drug-related offences."[332] Intelligence agencies may wiretap people suspected of endangering national security, after receiving written permission from the Prime Minister or Defense Minister. The agencies must present an annual report to the Knesset. The Chief Military Censor may also intercept international conversations to or from Israel for purposes of censorship. A 1991 report by the State Comptroller found that the police were abusing the procedures and that led to the 1995 amendments. In 1996 a Defense Forces employee was tried for misusing the phone records of a journalist.[333] Several people, including Ma'ariv publisher Opher Nimrodi, were convicted in 1998 of ordering wiretaps on business people and media personalities, including Science Minister Silvan Shalom in 1994.[334] In November 1998, wiretaps were discovered on the phone of Labor and Social Affairs Minister Eli Yishai. It was suspected that he was wiretapped by a rival political faction inside the Shas

329. *See* Government of Israel, *Government Ministries* (visited Nov. 19, 1999) <http://israel.org/gov/justice.html>.

330. U.N. Human Rights Comm., *Initial report of States parties due in 1993: Israel.* 09/04/98. CCPR/C/81/Add.13 (State Party Report), Apr. 9 1998.

331. The Secret Monitoring Law, 5739-1979, Laws of the State of Israel, vol. 33, pp. 141-46.

332. U.N. Human Rights Comm., *Initial report of States parties due in 1993: Israel.* 09/04/98. CCPR/C/81/Add.13 (State Party Report), Apr. 9, 1998.

333. Evelyn Gordon, *IDF Officer Involved in Phone Record Scandal Accuses Others of Involvement*, THE JERUSALEM POST, July 11, 1996.

334. *Media Wiretapper Found Guilty*, THE JERUSALEM POST, Sept. 4, 1998.

party.[335]

Unauthorized access to computers is punished by the 1995 Computer Law.[336] The Postal and Telegraph Censor, which operates as a civil department within the Ministry of Defense has the power to open any postal letter or package to prevent harm to state security or public order.[337] The 1996 Patient Rights Law imposes a duty of confidentiality on all medical personnel.[338] The Health Ministry issued regulations on using video surveillance in hospitals in September 1989 after it was disclosed that cameras were moved to watch patients undress.[339] Criminal records are governed by the Criminal Register and Rehabilitation Law that allows 30 government agencies to access the records.[340]

Finance Minister Yaakov Ne'eman issued an authorization in March 1998 giving the director of the Bureau for Counterterrorism full access to the databases of all Israeli taxation authorities, including the Income Tax Authorities and Customs. It gives the Bureau access to the financial records of any citizen in Israel, including the status of their bank account "for urgent cases of preventing terrorist acts."[341]

ITALIAN REPUBLIC

Articles 14 and 15 of the 1948 Constitution protect privacy and the secrecy of communications. The Italian Data Protection Act was enacted in 1996 after twenty years of debate.[342] The Act is intended to fully implement the E.U. Data Protection Directive. It covers both electronic and manual files for both government agencies and the private sector. Italy first attempted to enact data protection legislation in 1981.

The Supervisory Authority ("Garante") for Personal Data Protection enforces the Act. The Garante maintains a register, conducts audits and

335. Herb Keinon, *Shas Disputes Linking Wiretap to Yishai-Deri Rivalry*, THE JERUSALEM POST, Nov. 27, 1998.

336. The Computer Law (5755-1995), 1534 Laws of the State of Israel 366; *see* Miguel Deutch, *Computer Legislation: Israel's New Codified Approach*, 14 J. MARSHALL J. COMPUTER & INFO. L. 461 (1996).

337. Regulation 89 of the Mandatory Defence (Emergency) Regulations, 1945.

338. Patient's Rights Law, 5756-1996.

339. Judy Siegel, *Embarrassed by Ichilov Disclosure: Ministry Issues Regulations for Hospital Cameras*, THE JERUSALEM POST, Sept. 10, 1998.

340. Criminal Register and Rehabilitation Law, 5741-1981.

341. Yossi Melman, *Anti-terror Chief to See All Ttax Files*, HA'ARETZ, May 29, 1998.

342. Legge '31 dicembre 1996 n. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Amended by Legislative Decree No. 123 of 09.05.97 and 255 of 28.07.97, available at <http://elj.strath.ac.uk/jilt/dp/material/L675-eng.htm> (Unofficial translation). LEGGE 31 DICEMBRE 1996, N. 676, Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. <http://www.privacy.it/legge96676.html>. For a list of decrees, see <http://www.privacy.it/normativ.html>.

enforces the laws and can also audit databanks not under its jurisdiction such as those relating to intelligence activities. The Decree on the internal organization of the Authority was published in the Official Journal on February 1, 1999, a year after it was submitted. The Decree establishes the procedures for keeping the Register of Data Processes, access to the register by citizens, investigations, registrations and inspections.[343] The Garante ruled in October 1998 that phone companies need not mask the phone numbers on bills and that phone companies should allow for anonymous phone cards to protect privacy.[344]

Wiretapping is regulated under the penal procedure code and penal code.[345] It requires a court order that can last for 15 days in most cases. There are more lenient procedures for anti-Mafia cases. Some 44,000 orders were approved in 1996, up from 15,000 in 1992.[346] The law on computer crime includes penalties on interception of electronic communications.[347] In March 1998, the Parliament issued a legislative decree adopting the provisions of the E.U. Telecommunications Privacy Directive.[348]

There are also sectoral laws relating to workplace surveillance,[349] statistical information, electronic files, and digital signatures.[350] The Workers Charter prohibits employers from investigating the political, religious or trade union opinions of their workers, and in general, on any matter that is irrelevant for the purposes of assessing their professional skills and aptitudes.[351] The 1993 computer crime law prohibits unlawfully using a computer system and intercepting computer

343. DECRETO DEL PRESIDENTE DELLA REPUBBLICA 31 marzo 1998, n.501 Regolamento recante norme per l'organizzazione ed il funzionamento dell'Ufficio del Garante per la protezione dei dati personali, a norma dell'articolo 33, comma 3, della legge 31 dicembre 1996, n. 675. (GU n. 25 del 1-2-1999) <http://193.207.119.193/MV/menugazettaufficiale.htm>.

344. www.Privacy.it, *Comunicato Stampa* (visited Jan. 1, 2000) <http://www.privacy.it/garantes981006.html>.

345. Intercettazioni di conversoni o comunicazioni, Art 266-271, Codice di Procedura Penale, and Art 614-623, Codice di Penale.

346. French Commission National de Control des Interceptions de securite, Annual Report 1996.

347. Legge 23 dicembre 1993 n. 547.

348. DECRETO LEGISLATIVO 13 maggio 1998, n. 171. Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica <http://www.privacy.it/dl98171.html>.

349. Legge 29 marzo 1983, n. 93 - Legge quadro sul pubblico, ITNTDI, p. 296, § 1114.

350. Presidential Decree No. 513 of 10 Nov. 1997, *Regulations establishing criteria and means for implementing Section 15(2) of Law No. 59 of Mar. 15, 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems*, <http://www.aipa.it/english[4/law[3/pdecree51397.asp>.

351. Section 8 of Law No. 300 of May 20, 1970.

communications.[352]

JAPAN

Article 21 of the 1946 Constitution prohibits censorship and protects the secrecy of communications.[353] The 1988 Act for the Protection of Computer Processed Personal Data Held by Administrative Organs governs the use of personal information in computerized files held by government agencies.[354] It is based on the OECD guidelines and imposes duties of security, access, and correction. Agencies must limit their collection to relevant information and publish a public notice listing their files systems. Information collected for one purpose cannot be used for a purpose "other than the file holding purpose." The Act is enforced by the Government Information Systems Planning Division of the Management and Coordination Agency. The Prefecture of Kanagawa also has legislation protecting privacy in both the public and private sectors.[355]

The Japanese government follows a policy of self-regulation for the private sector, especially relating to electronic commerce. In June 1998, former Prime Minister Ryutaro Hashimoto announced that he had signed an agreement with U.S. President Clinton for self-regulation for privacy measures on the Internet except for certain sensitive data. "If data in a certain industry is highly confidential, legal methods can be considered for that industry."[356] On March 4, 1997, the Ministry of International Trade and Industry ("MITI") issued Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector. In February 1998, MITI established a Supervisory Authority for the Protection of Personal Data to monitor a new system for the granting of "privacy marks" to businesses committing to the handling of the personal data in accordance with the MITI guidelines, and to promote awareness of privacy protection for consumers. The "privacy mark" system was introduced on April 1, and is administered by the Japan Information Processing Development Center ("JIPDEC") – a joint public/private agency. Companies that do not comply with the industry guidelines will be excluded from relevant industry bodies and not granted the privacy

352. Law No. 547 of Dec. 23, 1993.

353. Nihonkoku Kenpo [Constitution of Japan] [KENPO, art. 21] (Nov. 3, 1946), *available at* <http://www.ntt.co.jp/japan/constitution/ english-Constitution.html>.

354. The Act for the Protection of Computer Processed Personal Data held by Administrative Organs, Act No. 95, 16 Dec. 1988 (Kampoo, Dec. 16, 1988). For the text, see WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION (McMillian Publishers Ltd., 1992).

355. Kanagawa Prefecture Ordinance on the Protection of Personal Data, Ordinance No. 6, dated Mar. 30, 1990. *See* Michael R. Nelson, IBM, "Building Trust in Cyberspace," Speech at The Better Business Bureau on Ethical Electronic Commerce (Oct. 14, 1999)

356. U.S.-Japan Joint Statement on Electronic Commerce, May 15, 1998. <http://www.ecommerce.gov/usjapan.htm>.

protection mark. It is assumed that they will then be penalized by market forces. However, in addition, the new Supervisory Authority will investigate violations and make suggestions as necessary to the relevant administrative authorities.[357] An analysis of the marks done for the European Union by four academic experts in privacy found that there were serious shortcomings in the system.[358]

Wiretapping is considered a violation of the Constitution's right of privacy and was only authorized a few times. Wiretapping is also prohibited under article 104 of the Telecommunications Business Law and Article 14 of the Wire Telecommunications Law.[359] A bill authorizing wiretapping for narcotics, guns, gang-related murders and large-scale smuggling of foreigners cases was approved by the Diet in August 1999 following strong pressure by the United States government.[360] In June 1997, the Tokyo High Court upheld a lower court's finding that the Kanagawa Prefectural Police had illegally wiretapped the telephone at the home of a senior member of the Japanese Communist Party. The court imposed a fine of four million yen.[361] A number of NTT employees were also caught recently selling information about customers.[362]

A bill which would create a 10 digit number for all residents was approved by the Diet in August 1999.[363] This would allow centralized control by the Ministry of Home Affairs of information on residents currently held by local governments. The bill was held up for a year, but in June 1999 the opposition New Komeito party agreed to support the bill if a law a new law on privacy protection was enacted. A committee has been set up to develop a bill to be introduced within three years.

The Ministry of Finance and Ministry of International Trade and Industry announced plans to introduce legislation to protect individuals credit data in the next Parliament after a task force issues proposals.[364]

---

357. Nigel Waters, "Reviewing the adequacy of privacy protection in the Asia Pacific Region," Speech at the IIR Conference Information Privacy - Data Protection in Sydney (June 15, 1998); *see also* Ministry of International Trade and Industry ("MITI"), *Japan's views on the protection of personal data* (Apr. 1998).

358. Raab, Bennett, Gellman & Waters, European Commission Tender No XV/97/18/D, Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, Sept. 1998.

359. Telecommunications Business Law, LAW No. 86 of 25 Dec. 1984, as amended last by Law No. 97 of June 20, 1997 <http://www.mpt.go.jp/policyreports/english/laws/Tb_index.html>.

360. REUTERS, June 1, 1999. *See also* <http://www.jca.ax.apc.org/~toshi/cen/wiretap.intr.html>.

361. *Police Wiretapping*, MAINICHI DAILY NEWS, June 29, 1997.

362. *NTT Staffers Leaking Customer Information*, NEWSBYTES, July 2, 1999.

363. *Gov't Planning New ID System for All Residents*, MAINICHI DAILY NEWS, Jan. 5, 1998.

364. *Japan Ministries To Compile Credit Data Protection Bill*, NIKKEI, July 4, 1999.

Japan's Ministry of Posts and Telecommunications ("MPT") announced plans in June 1998 to study privacy in telecommunications services, establishing a study group to look into the matter.[365]

The Ministry of Transportation announced in June a plan to issue "Smart Plates" license plates with embedded IC chips by 2001. The chips will contain driver and vehicle information and be used for road tolls and traffic control.[366] The National Police Agency also operates a comprehensive video surveillance system called the "N-system" with 400 locations on expressways and major highways throughout the country, which was automatically recording the license plate number of every passing car for the last 11 years. Whenever a "wanted" car is detected, the system immediately issues a notice to police.[367]

REPUBLIC OF KOREA (SOUTH KOREA)

Articles 16, 17 and 18 of the Constitution provide for protection of privacy and secrecy of communications.[368] The Act on the Protection of Personal Information Managed by Public Agencies of 1994 sets rules for managing computer-based personal information held by government agencies and is based on the OECD privacy guidelines.[369] Under the Act, government agencies must limit data collected, ensure their accuracy, keep a public register of files, ensure the security of the information, and limit its use to the purposes for which it was collected. The Minister of Government Administration enforces the Act.

Promoting electronic commerce was a major impetus for recent developments. In May 1998 the Ministry of Commerce, Industry and Energy ("MoCIE") proposed a set of guidelines for electronic commerce legislation, including protecting privacy in the digital trade environment.[370] The Basic Act on Electronic Commerce was approved in January 1999. Chapter III of the Act requires that "electronic traders shall not use, nor provide to any third party, the personal information collected through electronic commerce beyond the alleged purpose for collection thereof without prior consent of the person of such information or except as specifically provided in any other law." Individuals also have rights of access, correction and deletion and data holders have a duty of security.[371] In March 1999 the Ministry of Information and Communica-

365. NEWSBYTES, June 1, 1998.

366. *License Plates to Bear IC Chips with Driver, Auto Info*, COMLINE, June 9, 1999.

367. CHRISTIAN SCIENCE MONITOR, Apr. 8, 1997.

368. Constitution of the Republic of Korea, Adopted: July 17, 1948, *available at* <http://www.ccourt.go.kr/english/et.html>.

369. Act of Jan. 7, 1994.

370. Nikkei BP AsiaBizTech - 29-Jun-98.

371. Basic Law on Electronic Commerce (1999) <http://www.mbc.com/legis/south_korea.html>.

tions announced that it was planning to introduce a bill that regulates password systems to activate electronic commerce and safe document transfers on the Internet and other bills to regulate privacy and electronic money transfers.[372] The Ministry also announced that it had enacted a digital signature ordinance.

The cabinet approved a bill in March 1999 creating a National Human Rights Commission which would, among its powers, investigate illegal wiretapping. The proposal was criticized by Amnesty International and local groups who held a week-long hunger strike to protest the bill. Amnesty said that the bill "seems designed to set up a commission which lacks independence and has weak investigative powers over a limited range of violations."[373]

The Law on Protection of Privacy of Communications regulates wiretapping. The Law requires a court order to place a tap. Intelligence agencies are required to obtain permission from the Chief Judge of the High Court or approval from the President for national security cases.[374] Article 54 of the Telecommunication Business Act, prohibits persons who are or were engaged in telecommunication services, from releasing private correspondence. There were 6,638 taps authorized in 1998, 1,073 of those were "emergency taps" which are done without prior court permission. In 1997, there were a reported 6,002 legal taps up from 2,067 in 1996.[375] Rep. Kim Hyong-o of the opposition Grand National Party ("GNP") stated that he believed that over 10,000 taps were actually placed in 1998.[376] Under previous administrations, there were widespread surveillance and wiretapping abuses by intelligence and police officials. In October 1998, President Kim Dae-jung ordered a full-scale probe into illegal wiretapping. The wiretap law was amended in December 1998. The revisions limit the time frame that a tap can be placed before getting permission from a court and places additional procedural requirements, but allows taps to be placed without court permission for investigations of "gangs and criminal organizations."

The Act Relating to Use and Protection of Credit Information of 1995 protects credit reports.[377] The Postal Services Act protects postal

372. *Bill Due to Regulate Password for E-Commerce*, KOREA TIMES, Mar. 3, 1999.

373. Amnesty International, *South Korea – Gov't proposal will set up a weak National Human Rights Commission*, Apr. 12, 1999.

374. Communications Privacy Act, Dec. 27, 1993, revised Dec. 13, 1997. A list of all telecommunications laws in Korea is available at <http://www.kisdi.re.kr/kisdi/event/acts.htm>.

375. *Wiretappings Number 6,638 Last Yr.*, KOREA TIMES, Feb. 10, 1999.

376. *Kim Hyong-o Says More Than 10,000 May Be Exposed to Gov't Taps*, KOREA TIMES, Feb. 13, 1999.

377. Act Relating to Use and Protection of Credit Information, Law No. 4866, Jan. 5, 1995 <http://www.visas-usa.com/korealaw/library/cinfo-a-trn.htm>. Enforcement Decree

privacy.[378]

In 1997, the government announced the creation of an "Electronic National Identification Card Project." The plan was based on a smart card system and according to a local human rights group would "include universal ID card, driver's license, medical insurance card, national pension card, proof of residence, and a scanned fingerprint, among other things."[379] The government was scheduled to issue cards to all citizens by 1999.[380] On November 17, a law on the ID card project passed the National Assembly. In December 1997, Kim Dae Jung won the Presidential election. He publicly opposed the ID card project in his campaign and appears to have stopped it. However, activists believe that government agencies are continuing to quietly develop the proposals.

REPUBLIC OF LATVIA

Article 17 of the Constitutional Law on Rights and Obligations of a Citizen and a Person protect the secrecy of communications.[381] Legislation protecting personal data is being prepared by a working group operating under the Department of Informatics, Ministry of Transportation. Another working group operating under the Ministry of Culture is preparing legislation protecting databases maintained by the government sector.[382]

The Law on Freedom of Information was adopted by the Saiema in October 1998 and signed into law by the State President in November 1998.[383] It guarantees public access to all information in "any technically feasible form" not specifically restricted by law. Individuals may use it to obtain their own records. Information can only be limited if there is a law; the information is for internal use of an institution; trade secrets; information about the private life of an individual, and certification, examination, project, tender and similar evaluation procedures.

In January 1999, the National Human Rights Office (NHRO) threatened to sue the National Compulsory Health Insurance Central

---

for the Act Relating to Use and Protection of Credit Information <http://www.visas-usa.com/korealaw/library/cinfo-d-trn.htm>.

378. Amended by Law No. 2372, Dec. 16, 1972; Law No.3602, Dec. 31, 1982. <http://www.mic.go.kr/english/intro/rule/post12.htm>.

379. Korean NGO Task Force, *NO! Electronic Personal ID Card* (visited Jan. 2, 2000) <http://kpd.sing-kr.org/idcard/main-e.html>.

380. Joohoan Kim, Ph.D., *Digitized Personal Information and the Crisis of Privacy: The Problems of Electronic National Identification Card Project and Land Registry Project in South Korea* (visited Jan. 2, 2000) <http://kpd.sing-kr.org/idcard/joohoan2.html>.

381. Latvia – Constitutional Law: The Rights and Obligations of a Citizen and a Person (1991), *available at* <http://www.uni-wuerzburg.de/law/lg03000_.html>.

382. Janis Bicevskis and Girts Karnitis, *Problems in the Integration of Registers of State Significance in Latvia*, BALTIC IT REV., No. 8, p. 77.

383. Law on Freedom of Information, Adopted Oct. 29, 1998, Signed Nov. 6, 1998.

Fund (NCHICF) about the mandatory use of personal identification codes by doctors as a violation of the right to privacy in the European Convention on Human Rights.[384]

Under the new Penal Code, it is unlawful to interfere with correspondence.[385] Wiretapping or interception of postal communications requires the permission of a court.[386] On November 16, 1995, it was reported that telephones in the Latvian Defense Ministry were tapped. The Latvian Defense Ministry responded by stating Latvia's "military counterintelligence service reserves the right to ensure the security of communications at the Ministry of Defense and structures of the national armed forces."[387] In April 1994, a bugging device was found on the switchboard of the "Dienas Bizness" newspaper.[388]

REPUBLIC OF LITHUANIA

Article 22 of the Constitution protects privacy and secrecy of communications.[389] Lithuania enacted its Law on Legal Protection of Personal Data in 1996[390] and amended it in March 1998 to harmonize it with E.U. Data Protection Directive.[391] The Law regulates the processing of all types of personal data, not just in state information systems. It defines the time and general means of protecting personal data and sets rights of access and correction. It also sets rules on collecting, processing, transferring and using data. The Administrative Code defines various monetary penalties in cases infringing the process and use of data.[392] There is also a Law of State Registers[393] which governs the use and legitimacy of state data registers that contain personal information. The law also mandates that data registers may only be erased or destroyed in cooperation with the State Data Protection Inspectorate.

The State Data Protection Inspectorate was established in 1996 to enforce the provisions of the Law on Legal Protection of Personal Data and the Law on State Registers.[394] Under the 1998 Law, it is subordinated to the Minister of Public Administration Reforms and Lo-

384. BALTIC NEWS SERVICE, Jan. 5, 1999.

385. Criminal Code of Latvia, art. 132

386. Criminal Procedure Code of Latvia, arts. 168, 176, 176.1

387. *Defense Ministry Issues a Statement in Response to Reports of Bugging,* Latvian Radio, Riga, Nov. 16, 1995 (BBC Summary of World Broadcasts, Nov. 20, 1995).

388. (BBC Summary of World Broadcasts, Apr. 16, 1994).

389. Constitution of the Republic of Lithuania, *available at* <http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/CONSTITU.HTM>.

390. The Law on Legal Protection of Personal Data (No 63-1479, 1996).

391. Law No.VII-662, Mar. 12, 1998.

392. *See* Ona Jakstaite, *Regulating Data Security in Lithuania*, BALTIC IT REV..

393. The Law of the Public Registers (Aug. 13 1996, No. I-1490).

394. Resolution No. 1185, *On Establishing the State Data Protection Inspectorate*, Oct. 10, 1996 (No 100-2293).

cal Authorities from July 1998. There are efforts to make it an independent agency.

Wiretapping requires a warrant issued by the Prosecutor General.[395] On October 27, 1995, the Lithuanian State Security Department Chief, Jurgis Jurgialis, denied opposition charges that his department bugged telephones for political reasons. He said, "we resort to such actions only on the basis of the law and after receiving the prosecutor's authorization in each particular case." Jurgialis denied that his department was involved in widespread bugging, but conceded such activities were conducted throughout Lithuania "by quite different structures, including foreign intelligence services."[396] In May 1998, *Lietuvos rytas*, the country's largest daily, revealed that a top-secret surveillance unit was monitoring the media, the prosecutor general, cabinet ministers, the Prime Minister, and the President. The unit was shut down after the revelations.[397] The International Helsinki Committee raised concerns about prosecuting Audrius Butkevicius, a member of the Lithuanian parliament, on corruption charges in 1997 based on wiretaps conducted without a court order.[398]

There are specific privacy protections in laws relating to telecommunications,[399] radio communications,[400] statistics,[401] the population register,[402] and health information.[403] The Penal Code of the Republic of Lithuania provides for criminal responsibility for violations of the inviolability of a residence, infringement on secrecy of correspondence and telegram contents, privacy of telephone conversations, persecution for criticism, secrecy of adoption, slander, desecration of graves and impact on computer information. Civil laws provide compensation for moral damage because of dissemination of unlawful or false information demeaning the honor and dignity of a person in the mass media.[404]

---

395. Law on Operative Activities, 1991.

396. Vladas Burbulis, *Lithuania Security Chief Refutes Any Telephone Bugging*, ITAR-TASS, Oct. 27, 1995.

397. *Keeping an Eye on Politicians*, TRANSITIONS, Aug. 1998.

398. International Helsinki Federation for Human Rights, *Annual Report* (1999) <http://www.ihf-hr.org/reports/ar99/ar99lit.htm>.

399. The Law on Telecommunications, Nov. 30, 1995, No. I-1109.

400. Law on Radio Communication, No.I-1086 (Nov. 7, 1995) <http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/366.HTM>.

401. The Law on Statistics, Oct. 12, 1993, No.I-270.

402. Law on the Population Register, Jan. 23, 1992, No. I-2237.

403. Law on the Health System, July 19, 1994, No.I-552.

404. U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Initial reports of States parties due in 1993*, Addendum, Lithuania, 1996, *available at* <http://www.hri.ca/fortherecord1997/document ation/tbodies/ccpr-c-81-add10.htm>.

GRAND DUCHY OF LUXEMBOURG

Article 28 of the Constitution protects the secrecy of communications.[405] Luxembourg's Act Concerning the Use of Nominal Data in Computer Processing was adopted in 1979.[406] The law pertains to individually identifiable data in both public and private computer files. It also requires licensing of systems used for processing personal data. The law considers all personal data to be sensitive, although special provisions may apply to medical and criminal information. For personal data processing by the private sector, an application must first be made to the Minister for Justice who thereafter issues an authorization for such processing to take place. The Commission à la Protection des Données Nominatives, under the Ministry of Justice, oversees the law. If an application for personal data processing is granted and there is an objection raised, or if the application is refused or the original authorization is withdrawn for some reason, an appeal can be made to the Disputes Committee of the Council of State. The Minister for Justice maintains a national register of all systems containing personal information. Public sector personal data systems can only be established upon the issuance of a special law or regulation. The Advisory Board reviews such proposed laws or regulations. In 1992, the law was amended to include special protection requirements for police and medical data.

A bill that would make the law consistent with the E.U. Directive was introduced in the Parliament in 1997, but withdrawn in 1998 and was not yet reintroduced due to Parliamentary elections.[407] A project on electronic commerce that will implement the E.U. Telecommunications Privacy Directive is currently pending.[408]

Telephone tapping is regulated by the Criminal Code.[409] Under the law, a tribunal selected by the President authorizes wiretaps. There are also sectoral laws on privacy relating to telecommunications,[410] identity numbers,[411] and banking secrecy. Luxembourg's status as a financial ha-

405. Constitution of the Grand Duchy of Luxembourg, *available at* <http://www.uni-wuerzburg.de/law>.

406. Act on the Use of Nomative Data in Computer Processing, Mar. 31, 1979.

407. Act on the protection of individuals with regard to the processing of their personal data, no. 4357.

408. Projet de loi relatif au commerce électronique, document parlementaire N° 4554 <http://www.etat.lu/ECO/coel.htm>.

409. Art 88-1 - 88-4 of the Criminal Code, Law of Nov. 26, 1982, modified by the law of July 7, 1989.

410. Loi du 21 mars 1997 sur les télécommunications. <http://www.etat.lu/ILT/co/legal/loi-t.htm>, Règlement grand-ducal du 22 décembre 1997 fixant les conditions du cahier des charges pour l'établissement et l'exploitation de réseaux fixes de télécommunications. <http://www.etat.lu/ILT/co/legal/lic-b.htm>.

411. Loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales <http://www.etat.lu/ECP/30-3-79.doc>. Règlement grand-ducal du 7 juin

ven ensures that unwarranted surveillance of individuals is forbidden. This may change as Luxembourg comes under increasing pressure to amend its financial confidentiality laws to permit greater access to personal financial records by European and American investigators.

MALAYSIA

The Constitution of Malaysia does not specifically recognize the right to privacy.[412] The Ministry of Energy, Communications and Multimedia is drafting a Personal Data Protection Act that will create legal protections for personal data as part of the "National Electronic Commerce Master Plan." Secretary-general Datuk Nuraizah Abdul Hamid said the purpose of the Bill was to ensure secrecy and integrity in the collection, processing and utilization of data transmitted through the electronic network.[413] The Ministry is looking at the OECD Guidelines, E.U. Directive, UK, Hong Kong and New Zealand Acts as models for the act. The bill is expected to be introduced into Parliament in 1999.

In 1998, the Parliament approved the Communications and Multimedia Act, which has several sections on telecommunications privacy. Section 234 prohibits unlawful interception of communications. Section 249 sets rules for searches of computers and includes access to encryption keys. Section 252 authorizes police to intercept communications without a warrant if a public prosecutor considers that a communication is likely to contain information relevant to an investigation.[414] There are regular reports of illegal wiretapping, including on the former deputy premier Anwar Ibrahim. Police detained four people under the Internal Security Act on suspicion of spreading rumors of disturbances in Kuala Lumpur in August 1998. Inspector-General of Police Tan Sri Abdul Rahim Noorsaid told the media then that the suspects were detained after police tracked their Internet activities with the assistance of Internet service provider Mimos Berhad.[415] The provider said later that it did not screen private email.[416]

Several other laws relating to technology were recently approved,

---

1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales. <http://www.etat.lu/ECP/7-6-79.doc>, Règlement grand-ducal modifié du 21 décembre 1987 fixant les modalités d'application de la loi du 30 mars 1979, <http://www.etat.lu/ECP/21-12-87.doc>.

412. Constitution of Malaysia, *available at* <http://star.hsrc.ac.za/constitutions/constmalcont. html>.

413. *Draft of Bill on Personal Data Protection Ready by Year-End*, THE NEW STRAITS TIMES. Oct. 2, 1998.

414. Communications and Multimedia Bill 1998 <http://www.kttp.gov.my/mm/multimedia.htm>.

415. Tony Emmanuel, *Rumours Over Internet: Four to be Charged Soon*, THE NEW STRAITS TIMES, Sept. 24, 1998.

416. *E-Mail not Screened, Says Service Provider* E, THE STRAITS TIMES, Aug. 17, 1998.

including The Digital Signature Act of 1997,[417] and the Computer Crime Act of 1997.[418] Section 8 of the Computer Crime Act allows police to inspect and seize computing equipment of suspects without a warrant or any notice. The suspect is also required to turn over all encryption keys for any encrypted data on his equipment. Malaysia's Banking and Financial Institutions Act 1989, Pt XIII, also has provisions on privacy.

Malaysia started a pilot program for a Government Multi-Purpose Card to be ready by August 2000 for two million residents in the Multimedia Super Corridor.[419] The card will be used as a national identity card, driver's license, hold immigration, passport information, medical records, and eventually be usable as a debit card. It will contain both a photo and a thumbprint. The government signed a contract in June 1999 with several companies including Unisys and Iris Technologies. Malaysians were told in 1998 that if they do not carry their cards, they risked being detained by immigration police.[420] In January, it was announced that Muslim couples married in the Malaysian capital will be issued cards with computer chips so Islamic police can instantly verify their vows and police will be equipped with portable card readers. In December 1998, the government began requiring that cybercafes obtain name, address, and identity card information from patrons, but lifted the requirement in March 1999.[421]

UNITED MEXICAN STATES

Article 16 of the 1917 Mexican Constitution protects the secrecy of correspondence.[422] Article 214 of the Penal Code protects against disclosure of personal information held by government agencies.[423] The General Population Act regulates the National Registry of Population and Personal Identification. The Registry's purpose is to register all persons making up the country's population using data enabling their identity to be certified or attested reliably. The aim of this is ultimately to issue the citizen's identity card, which will be the official document of identification, fully endorsing the data contained in it concerning the holder.[424]

417. Digital Signature Bill 1997, *available at* <http://www.cert.org.my/digital.html>.

418. Computer Crimes Bill 1997, *available at* <http://www.cert.org.my/crime.html>.

419. Ariff Aawng, *Klang Valley Residents Will Be First to Use Multi-Purpose Card*, BUS. TIMES, June 1, 1999.

420. *Malaysians Told: Carry ICs or Risk Detention*, THE NEW STRAITS TIMES, May 14, 1998.

421. *Cabinet: Cybercafes Not Subjected to Restrictions*, THE NEW STRAITS TIMES, Mar. 18, 1999.

422. Constitucion Politica de los Estados Unidos Mexicanos [CONST.], <http://info.juridicas.unam.mx/cnsinfo/fed00.htm>.

423. Código Penal Federal, Art. 214.

424. *See* U.N. Human Rights Comm., *Question of the Follow-Up to the Guidelines for the Regulation of Computerized Personal Data Files: Report of the Secretary-General Prepared*

Chapter 6 of Mexico's Postal Code, in effect since 1888, recognizes the inviolability of correspondence and guarantees the privacy of correspondence.[425] The 1939 General Communication Law provides penalties for interrupting communications and divulging secrets.[426] The Federal Penal Code establishes penalties for the crime of revealing personal secrets by any means, including personal mail.[427] In 1981, the Penal Code was amended to include the interception of telephone calls by a third person.[428] The Law Against Organized Crime, passed in November 1996, allows for electronic surveillance with a judicial order.[429] The law prohibits electronic surveillance in cases of electoral, civil, commercial, labor, or administrative matters and expands protection against unauthorized surveillance to cover all private means of communications, not merely telephone calls.[430] The Law was widely criticized by Mexican human rights organizations as violating Article 16 of the Constitution.[431] They noted that telephone espionage had been historically used by the ruling PRI party "to keep the opposition in check."[432] In 1997, the telephones of the Jalisco State Supreme Court were found to have been wiretapped.[433] In March 1998, a large cache of government electronic eavesdropping equipment which had been used since 1991 to spy on members of opposition political parties, human rights groups and journalists was discovered in Campeche.[434] Thousands of pages of transcripts of telephone conversations were uncovered along with receipts for $1.2 million in Israeli surveillance equipment. More than a dozen other cases of government espionage in four other states were exposed, ranging from hidden microphones and cameras found in government offices in Mexico City, to tapes of a state governor's telephone calls. Every government agency identified with the electronic surveillance operations – the federal attorney general and interior ministry, the military, the national

---

Pursuant to Commission Decision 1995/114 <http://www.hri.ca/fortherecord1997/documentation/commission/e-cn4-1997-67.htm>.

425. El Código Postal de los Estados Unidos Mexicanos (1884).

426. Ley de Vías Generales de Comunicación de 30 de diciembre de 1939, Arts 571. 576, 578.

427. Código Penal Federal, Art 210.

428. *Id.*, Art. 167, part 9.

429. Ley Federal Contra la Delincuencia Organizada, 7 de noviembre de 1996, <http://info1.juridicas.unam.mx/legfed/247/1.htm>.

430. Mark Fineman, *Zedillo to Sign Sweeping Organized Crime Package,* L.A. TIMES, Oct. 30, 1996, at A4.

431. *Exigen siete ONG la renuncia del titular de Seguridad Publica*, LA JORNADA, Oct. 7, 1997.

432. *Con la reforma anticrimen, el espionaje entraría a la Constitución*, LA JORNADA, 28 de abril de 1996.

433. AP, Jan. 18, 1997.

434. Molly Moore, *Spy Network Stuns Mexicans; Raid Opens Door to Exposure of Government Snooping*, THE WASH. POST, Apr. 13, 1998, at A01.

security agency and a plethora of state institutions – denied knowing anything about them.[435]

KINGDOM OF THE NETHERLANDS

Articles 10 and 13 of the Constitution grant citizens an explicit right to privacy, secrecy of communications, and data protection.[436] The Data Registration Act 1988[437] establishes a code of fair information practices that applies to the handling of personal data files. The Act defines "personal data file" as "any organized collection of personal data relating to different persons which is operated by automated means or is systematically disposed in such a way as to facilitate access to the data therein contained." The Act generally stipulates that a personal data file must be set up only for a specific purpose that is relevant to the interests of the party controlling the personal data file. Personal data must be obtained legitimately and according to the purpose for which the file was set up. The party collecting data has a duty to ensure that it is accurate and complete. Use of the personal data must be compatible with the purpose of the data file. The party controlling the data must take appropriate measures to ensure data is secure, and can be held liable for any loss or damage resulting from failure to comply with the Act. Data can only be disclosed if the disclosure is compatible with the purpose of the data file, is required by statute, or if the data subject consents to the disclosure. Controllers of personal data files must notify every person about whom personal data was recorded. Provisions allow data subjects to have access to their data files and to request correction of their personal data. The data subject can apply to the district court for enforcement of these provisions.

The Data Registration Act establishes the Registration Chamber (Registratiekamer).[438] The Registration Chamber, which serves as the Data Protection Authority, supervises the operation of personal data files according to the Data Registration Act. The Chamber advises the government, deals with complaints submitted by data subjects, institutes investigations, and makes recommendations to controllers of personal data files. The Chamber receives around 6,000 inquiries and 300 complaints each year. There are presently over 60,000 databases regis-

435. *Anger as Big Brother Spy Tactics Exposed*, THE GUARDIAN (London), Apr. 14, 1998, at 011.

436. Grondwet [Constitution of the Kingdom of the Netherlands 1987] [GRW. NED.], *available at* <http://www.uni-wuerzburg.de/law/nl00000_.html>.

437. *The Dutch Data Registration Act of 1988*, Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties (Wet persoonsregistraties). Gepubliceerd in het Staatsblad 1988, 655. <http://www.unimaas.nl/~privacy/wpr.htm> (in Dutch only).

438. Registratiekamer (visited Jan. 2, 2000) <http://www.registratiekamer.nl>.

tered with the Chamber. It also released several reports on privacy enhancing technologies jointly produced with the Office of the Information and Privacy Commissioner of Ontario, Canada.

Two decrees were issued under the Data Registration Act. The Decree on Sensitive Data[439] sets out the limited circumstances when personal data on an individual's religious beliefs, race, political persuasion, sexuality, medical, psychological and criminal history may be included in a personal data file. The Decree on Regulated Exemption[440] exempts certain organizations from the registration requirements of the Data Registration Act.

The Data Registration Bill 1998[441] was introduced in the Lower House of the Dutch Parliament in June 1998. This bill is a revised and expanded version of the 1988 Data Registration Act that will bring Dutch law in line with the European Data Protection Directive and regulate the disclosure of personal data to countries outside of the European Union. Since June 1998, many questions arose from members of Parliament concerning the new bill, and those questions are currently being investigated and answered by the Minister of Justice. The Lower House began discussing the bill in March, but has delayed for different reasons. The Minister of Justice promised that the bill will be one of the first debated when Parliament returns in September. Passage by Parliament and entry into force is not expected before January 2000.

Interception of communications is regulated by the criminal code and requires a court order.[442] A new Telecommunications Act was approved in December 1998 that requires that Internet Service Providers have the capability by August 2000 to intercept all traffic with a court order and maintain users logs for three months.[443] In November 1997, XS4ALL, a Dutch ISP, refused to conduct a broad wiretap of electronic communications of one of their subscribers.

A survey by the Dutch Ministry of Justice in 1996 found that police in the Netherlands intercept more telephone calls than their counterparts in the United States, Germany or Britain.[444] The Parliamentary Investigations Commission into police methods released a 4,700-page report in 1996. The report was critical of legal controls on police surveil-

439. *Decree on Sensitive Data* (Mar. 5, 1993) <http://www.unimaas.nl/~privacy/bgg.htm>.

440. Besluit Genormeerde vrijstelling (July 6, 1993) <http://www.unimaas.nl/~privacy/bgv.htm>.

441. Dutch Personal Data Protection Bill (1998) <http://www.unimaas.nl/~privacy/wbp.htm> (English version now available).

442. Article 125i of the Code of Criminal Procedure.

443. *Rules Pertaining to Telecommunications* (Telecommunications Act) (Dec. 1998) <http://www.minvenw.nl/hdtp/hdtp2/wetsite/engels/index.html>.

444. *Id.*

lance[445] and found that there was a failure among judges, prosecutors and other officials to limit police abuses. The new Telecommunications Act also implements the E.U. Telecommunications Privacy Directive.

There are sectoral laws dealing with the Dutch police,[446] medical exams,[447] medical treatment,[448] social security,[449] entering private homes[450] and the employment of minorities.[451]

NEW ZEALAND

Article 21 of the Bill of Rights Act of 1990 protects privacy and correspondence.[452] The Human Rights Act of 1994 prohibits discrimination.[453]

New Zealand's Privacy Act was enacted in 1993 and amended several times.[454] It regulates the collection, use and dissemination of personal information in both the public and private sectors. It also grants individuals the right to access 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. Recent case law has held that the definition also applies to mentally processed information.[455] 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 OECD guidelines and the information privacy principles in Australia's Privacy Act 1988. In addition, the legislation includes

445. Statewatch bulletin, Vol. 6 no 1, Jan. – Feb. 1996.

446. Dutch Police Registers Act (1990), *available at* <http://www.unimaas.nl/~privacy/wpolr.htm>.

447. Dutch Medical Examinations Act (1997), *available at* <http://www.unimaas.nl/~privacy/ wmk.htm>.

448. Dutch Medical Treatment Act (1997), *available at* <http://www.unimaas.nl/~privacy /index.htm>.

449. Dutch Social Security System Act (1997), *available at* <http://www.unimaas.nl/~privacy/ osv1997.htm>; Compulsory Identification Act.

450. Dutch Act on the Entering of Buildings and Houses (1994), *available at* <http://www.unimaas.nl/~privacy/awbt.htm>.

451. Dutch Act on the Stimulation of Labor by Minorities (1994), *available at* <http://www.unimaas.nl/~privacy/samen.htm>.

452. Bill of Rights Act (1990), *available at* <http://www.uni-wuerzburg.de/law/nz01000_.html>.

453. Human Rights Commission, *Welcome to the New Zealand Human Rights Commission* (visited Jan. 2, 2000) <http://www.hrc.co.nz/welcome.htm>.

454. The Privacy Act, *available at* <http://www.knowledge-basket.co.nz/privacy/legislation/ 1993028/toc.html>; The Privacy Amendment Act (1993), *at* <http://www.knowledge-basket.co.nz/privacy/legislation/ 1993059/toc.html>; The Privacy Amendment Act (1994), *available at* <http://www.knowledge-basket.co.nz/privacy/legislation/1994070/toc.html>.

455. *See* Re Application by L [information stored in person's memory] (1997) 3 HRNZ 716 (Complaints Review Tribunal).

a new principle dealing 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 is only one complete sectoral code of practice in force, the Health Information Privacy Code 1994. There are several codes of practice altering the application of single information privacy principles: the Superannuation Schemes Unique Identifier Code 1995, the EDS Information Privacy Code 1997, and the Justice Sector Unique Identifier Code 1998.

In addition to the information privacy principles, the legislation contains principles relating to information held on public registers, sets out guidelines and procedures in respect to information matching programs run by government agencies, and makes a 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.[456] The Privacy Commissioner oversees compliance with the Act, but does not function as a central data registration or notification authority. The 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 one-off exemptions from the information privacy principles, and reviewing public sector information matching programs.

Complaints by individuals are initially filed with the Privacy Commissioner who attempts to conciliate the matter. The office received 11,141 inquiries and 1,082 complaints in the year ending June 1998 and completed 804 of the complaints. In 121 cases, a final opinion was granted.[457] If conciliation fails, the Proceedings Commissioner[458] or the complainant (if the Proceedings Commissioner is unwilling) can bring the matter before the Complaints Review Tribunal, which can issue decisions and award declaratory relief, issue restraining or remedial orders, and award special and general damages up to NZ $200,000.

The Privacy Commissioner conducted a five-year review in 1998 and recommended over 150 changes to the act, mostly minor. These included limiting use of information on public registers, creating a right to be taken off direct marketing lists, restricting requests by employers for

456. Privacy Commissioner, *Te Mana Matapono Matatapu* < http://www.privacy.org.nz/top.html>.

457. NZ Privacy Commission, Annual Report for the year ended June 30, 1998.

458. The Proceedings Commissioner is a member of the Human Rights Commission, to which the Privacy Commissioner also belongs. The Proceedings Commissioner is empowered to take civil proceedings before the Complaints Review Tribunal on behalf of a complainant if conciliation fails.

criminal and medical records, limiting exceptions to the act, and providing additional funding for the Office of the Commissioner to enforce the act.[459]

The New Zealand Crimes Act and Misuse of Drugs Act govern the use of evidence obtained by listening devices.[460] Judicial warrants may be granted for bugging premises or interception of telephonic communications. Emergency permits may be granted for bugging premises and, following the 1997 repeal of a prohibition, for telephonic interceptions. There were 22 authorizations for interceptions in the 1994-1995 year. The average duration was four days. 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 NZ$500 fine. The New Zealand Security Intelligence Service (NZSIS) is also permitted to carry out electronic interceptions under the New Zealand Security Intelligence Service Act 1969. Under the provisions of this Act, the Minister in Charge of the NZSIS is required to submit an annual report to the House of Representatives. In 1998, the minister reported 3 warrants issued to the NZSIS for intercepts. The average length of time for which these warrants were in force was 4 months and 8 days. The report further states that "the methods for interception and seizure used were listening devices and the copying of documents."[461]

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. Operating as a virtual branch of the U.S. 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 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.[462] GCSB was specifically exempted from the provisions of the

459. Office of the Privacy Commissioner, *Necessary and Desireable: Privacy Act 1993 Review*, Dec. 1998.

460. Part XIA, Crimes Act of 1961; Misuse of Drugs Act of 1978.

461. Appendix I, Report by the Privacy Commissioner to the Minister of Justice in relation to the New Zealand Security Intelligence Service Amendment Bill emphasizing the inadequacy of public reporting obligations in relation to interception warrants (Feb. 9, 1999) <http://www.privacy.org.nz/people/nzsisab.html>.

462. NICKY HAGER, SECRET POWER: NEW ZEALAND'S ROLE IN THE INTERNATIONAL SPY NETWORK (Nelson, NZ: Craig Potton, 1996).

Crimes Act in 1997.[463]

KINGDOM OF NORWAY

There is no provision in the Norwegian Constitution of 1814 dealing specifically with the protection of privacy.[464] More generally, section 110c of the Constitution places state authorities under an express duty to "respect and secure human rights." The Norwegian Supreme Court has 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 courts on a case-by-case basis. This protection was first recognized in 1952.[465]

Norway's primary data protection statute is the Personal Data Registers Act of 1978.[466] The Act regulates the establishment and use, in the public and private sectors, of automated and physical data files on both physical/natural persons and legal persons (i.e., corporations). A person wishing to set up a computerized database of personal information must apply for a license. There are stricter controls on sensitive information. In 1994, the act was amended to also cover video surveillance.[467] The Act is in the process of being overhauled. This is partly to update the legislation in the light of new technological developments, and partly to bring Norwegian law into conformity with the requirements of the EC Directive on data protection. A preliminary proposal for new data protection legislation was issued.[468] A bill based on this proposal will be introduced into the Norwegian Parliament in the summer of 1999. The proposal follows closely the EC Directive and is expected to be enacted by the Parliament before the end of 1999.

The Data Inspectorate (Datatilsynet) is an independent administration body set up under the Ministry of Justice in 1980.[469] The Inspectorate accepts applications for licenses of data registers, evaluates the licenses, enforces the privacy laws and regulations, and provides information. The Inspectorate can conduct inspections and impose sanctions.

---

463. Crimes (Exemption of Listening Device) Order 1997 (SR 1997/145)

464. The Constitution of the Kingdom of Norway, *available at* <http://odin.dep.no/ud/nornytt/uda-121.html>.

465. Supreme Court decision of Dec. 13, 1952, *reported in* Rt. 1952, p. 1217.

466. Personal Data Registers Act of 1978 (lov om personregistre mm av 9 juni 1978 nr 48), in force Jan. 1, 1980. <http://www.datatilsynet.no/eksternweb/informasjon/engelsk/lov-eng.htm>.

467. Act No. 78 of June 11, 1993. Regulations No. 536 of July 1, 1994.

468. Et bedre personvern—forslag til lov om behandling av personopplysninger [Better privacy protection—proposal for an Act on processing of personal data], NOU 1997:19).

469. The Data Inspectorate (visited Jan. 2, 2000) <http://www.datatilsynet.no/>.

As of 1996, the Inspectorate had issued 65,000 licenses. Decisions of the Inspectorate can be appealed to the Ministry of Justice.

Wiretapping requires the permission of a tribunal and is initially limited to four weeks.[470] The total number of telephones monitored was 360 in 1990, 467 in 1991, 426 in 1992, 402 in 1993, 541 in 1994, and 534 in 1995.[471] A Supervisory Board reviews the warrants to ensure the adequacy of the protections. A Parliamentary Commission of Inquiry (The Lund Commission) was set up in 1994 to investigate the post-World War II surveillance practices of Norwegian police and security services. The 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 illegal wiretapping of left wing political groups up to 1989 were instituted and/or conducted illegally, and that courts had not generally been strong enough in their oversight. A new act to monitor the secret services was approved in 1995 following the Commission's recommendations.[472] It created a new Control Committee to monitor the activities of the Police Security Services, the Defence Security Services and the Defence 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.[473] In 1997, the Parliament agreed to allow people under surveillance by the POT to review their records and obtain compensation if the surveillance was unlawful. The POT has records on over 50,000 people.[474]

A large number of other pieces of legislation contain provisions relevant to privacy and data protection. These include the Administrative Procedures Act of 1967,[475] and the Criminal Code of 1902.[476] The criminal code first prohibited the publication of information relating to the "personal or domestic affairs" in 1889.[477]

---

470. Law of Dec. 17, 1976., Law of 24 Juin 1915. Criminal Procedure Act, chapter 16 a, by Act No. 52 of June 5, 1992. *See also* Regulation No. 281 of Mar. 31, 1995 on Telephone Monitoring in Narcotics Cases.

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

472. Act No. 7 of Feb. 3, 1995 on the Control of the Secret Services.

473. *Minister Resigns*, Statewatch Bulletin, Nov.-Dec. 1996, vol 6 no 1.

474. *Parliament Says People Can See Files*, Statewatch Bulletin, May-June 1997, vol. 7 no. 3.

475. Administrative Procedures Act of 1967 (lov om behandlingsmåten i forvaltningssaker av 10 februar 1967).

476. Almindelig borgerlig Straffelov 22 mai 1902 nr 10.

477. *See* prof. dr. juris Jon Bing, Data Protection in Norway, 1996 <http://www.jus.uio.no/iri/rettsinfo/lib/papers/dp_norway/dp_norway.html>.

REPUBLIC OF THE PHILIPPINES

Article III of the 1987 Constitution protects the right of privacy, communications and freedom of information.[478] There is no general data protection law, but there is a recognized right of privacy in civil law.[479] Bank records are protected by the Bank Secrecy Act.[480] The Senate debated a proposal in March to force three million citizens to file an annual "Statement of Assets and Liabilities (SAL)."[481]

The Anti-Wiretapping Law requires a court order to obtain a telephone tap.[482] In April 1999, the National Bureau of Investigation and the Ombudsman started investigations after reports that police had tapped at least 3,000 telephone lines including top government officials, politicians, religious leaders, businessmen and print and television journalists. In May 1998, Director Gen. Santiago Alino, chief of the Philippine National Police, ordered an investigation of the alleged electioneering and illegal wiretapping activities by members of the National Police's Special Project Alpha (SPA). Matillano said that his office received information that the former SPA men were using the office as their "monitoring center" against Vice-President Estrada's political opponents. Five recorders used to monitor wiretaps were found at the offices.[483] The House and the Senate held investigations in August 1997 after officials of the telephone company admitted that their employees were being paid to conduct illegal wiretaps.[484]

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 said that the order, "will put our people's right to privacy in clear and present danger . . . No one will refuse to get this ID for no one can avoid dealing with government. It is thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges." Government lawyers asked the court to reconsider its decision in August,[485] and President Joseph Estrada reiterated his support for using a national identification system in August

478. Constitution of the Republic of the Philippines, *available at* <http://pdx.rpnet.com/consti/index.htm>.

479. Cordero v. Buigasco, 34130-R, Apr. 17, 1972, 17 CAR (2s) 539; Jaworski v. Jadwani, CV-66405, Dec. 15, 1983.

480. Republic Act 7653.

481. House Bill 5345.

482. Republic Act 4300, June 19, 1965; Penal Code, Articles 290-292.

483. BALITA NEWS SERVICE, May 7, 1998.

484. *Wiretapping Probe*, BUSINESSWORLD (Manila), Aug. 26, 1997.

485. *Gov't Lawyers Ask Supreme Court to Reconsider Decision*, BUSINESSWORLD, Aug. 12, 1998.

1998 stating that only criminals are against a national ID.[486] 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.[487]

REPUBLIC OF PERU

Article 2 of the 1993 Constitution provides for extensive privacy, data protection and freedom of information rights.[488] The Constitution was amended in 1993 to include a "constitutional guarantee of habeas data" in Article 200.

Article 154 of the Penal Code 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 more than two years."[489]

Article 151 of the Penal Code states "that a person who unlawfully opens a letter, document, telegram, radiotelegram, 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 2 years and to 60 to 90 days' fine."[490] 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 3 or more than 5 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 20 to 52 days' community service."

However, there have been constant abuses of wiretap authority by the government Peru's National Intelligence Service (Servicio Nacional de Inteligencia or SIN), headed by a close adviser to the president Vladimiro Montesinos. The SIN conducted widespread surveillance and illegal phone tapping of government ministers and judges assigned to constitutional cases, beginning in the early 1990s. Army agents used sophisticated Israeli phone-tapping equipment to monitor telephone con-

486. *Erap Wants Nat'l ID System (Only criminals disagree with it, says the President)*, BUSINESSWORLD, Aug. 12, 1998.

487. Op. No. 91. *See Foundation Laid for Proposed Nat'l ID*, BUSINESSWORLD, Aug. 14, 1998.

488. Political Constitution of Peru (1993). CONSTITUTIONS OF THE COUNTRIES OF THE WORLD (Jan. 1995).

489. The U.N. High Commissioner for Human Rights. *Third periodic report of Peru: Peru.* 21/03/95. CCPR/C/83/Add.1. Para. 260.

490. *Id.* para. 268.

versations, and copies of the conversations were delivered to Montesinos.[491] The SIN maintains close ties with the U.S. Central Intelligence Agency, including a covert assistance program to combat drug trafficking.[492] The SIN allegedly conducted a nationwide surveillance campaign with the sole purpose of intimidating political opposition figures. In 1990, an opposition congressman's house was blown up after he delivered a congressional report on domestic surveillance of opposition politicians, journalists, human rights workers and companies suspected of tax evasion.[493] In August, 1997 former UN Secretary General Javier Perez de Cuellar Monday filed charges against the SIN with the Peruvian Attorney General and the Inter-American Human Rights Commission for taping 1,000 conversations he made from his home telephone between October 1994 and August 1995 while he ran for President against Alberto Fujimori.[494] President Fujimori absolved the SIN of the accusations against it, asserting that private individuals with commercial scanners had carried out the wiretapping.[495] The allegations prompted the resignation of the Defense Minister and a special prosecutor was appointed to investigate the incident.[496] The Defense Commission's three-month inquiry confirmed accusations of the widespread phonetapping, but concluded that there was no evidence the intelligence services carried out the spying.[497] A Member of Congress and several journalists filed a suit on grounds that their constitutional rights were violated (an *acción de amparo*), and to put an end to the tapping of their telephone calls.[498]

The Organic Law of the National Identification Registry and Civil Society (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 registered." The Law also requires all persons to carry a National Identity Document featuring a corresponding number, photograph and finger-

491. *Former Agent Accuses Peru Spy Chief*, AP, Mar. 17, 1998.

492. Human Rights Watch, *Human Rights Watch Report* (1998) <http://www.hrw.org/hrw/worldreport/Americas.htm>.

493. *As Lima Talks Hit Snag, Some Ex-Hostages Are Complaining*, N.Y. TIMES, Jan. 13, 1997.

494. *Former U.N. Chief Charges Peru Tapped His Phone*, REUTERS, Aug. 4, 1997.

495. *President Fujimori Denies Intelligence Behind Phone-Tapping Services*, America Television, Lima (BBC Summary of World Broadcasts, July 19, 1997).

496. *Peru Defense Head Resigns in Crisis*, REUTERS, July 17, 1997.

497. *Peru Congress Probe Fails to Catch Phonetappers*, REUTERS WORLD REPORT, May 29, 1998.

498. International Freedom of Expression eXchange (IFEX) Clearing House (Toronto), July 21, 1997 <http://www.ifex.org/alert/00002190.html>.

print.[499] The court must provide all personal data kept on file at the Public Registry upon request within 15 days.[500]

REPUBLIC OF POLAND

Articles 47 and 51 of the Polish Constitution recognize the rights of privacy and data protection.[501] The Law on the Protection of Personal Data Protection was approved in October 1997 and took effect in April 1998.[502] The law is based on the European Union data protection directive. Under the Law, personal information may only be processed with the consent of the party. Everyone has the right to verify his or her personal records held by government agencies or private companies. Every citizen has the right to be informed whether such databases exist and who administers them; queries should be answered within 30 days. Upon finding out that data is incorrect, inaccurate, outdated or collected in a way that constitutes a violation of the Act, citizens will have the right to request that the data be corrected, filled in or withheld from processing.[503] Personal information cannot generally be transferred outside of Poland unless the country has "comparable" protections.

The recently created Bureau of Inspector General for the Protection of Personal Data enforces the Act. The Bureau maintains a register of data files and can make checks on the basis of a complaint or by random inspections. Another responsibility is to register databases. 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.[504] The office will monitor the activities of all central government, local government and private institutions, individuals and corporations. In its first year, the office received 402 complaints, of which it considered 258 and issued 15 decisions, issued 147 opinions on bills and ordinances, and conducted 19 site visits. It estimates that it will register between 100,000 and 150,000 databases by October 1999.[505] 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.

Interception of communications is regulated by the new code of pe-

499. Ley Organica Del Registro Nacional De Identificacion y Estado Civil, Ley No. 26497, July 11, 1995 <http://www.congreso.gob.pe/ccd/leyes/cronos/1995/ley26497.htm>.

500. Ley de aplicación de la acción constitucional del habeas data, Ley No. 26301 (Nov. 13, 1995) <http://www.asesor.com.pe/teleley/bull505.htm>.

501. The Constitutional Act of 1997, *available at* <http://www.sejm.gov.pl/eng/konst/kon1.htm>.

502. Law on Protection of Personal Data, Dz.U. nr 133, poz. 833, Oct. 29, 1997.

503. Pawel Kligo, *The Info Boom's Murky Side*, WARSAW VOICE, Nov. 9, 1997.

504. *A One-Woman Orchestra*, WARSAW VOICE, June 21, 1998.

505. Letter from the Bureau of Inspector General (July 1, 1999).

nal procedure that took effect September 1, 1998.[506] The main difference between this and the previous code is that under the new regime, it is specified in the law in which cases tapping of communications are admissible. Telephones can be tapped only after the person in charge of the investigation obtains permission from a court. In special instances, the prosecutor will have the right to authorize a wiretap, but the decision must be confirmed by a court within five days.[507] According to official data released by the Internal Affairs Ministry in 1995, wiretapping and correspondence control were ordered in approximately 3,000 instances.[508] In April 1999, Minister Janusz Palubicki admitted that the Office of State Security (UOP) conducted surveillance of left and right political parties from 1992 until 1997.[509] An inquiry into the surveillance is ongoing. The Ministry of Justice asked former Prime Ministers Waldemar Pawlak, Jozef Oleksy and Wlodzimierz Cimoszewicz to give testimony in the case.[510] The Sejm Committee on Special Services rejected the Military Information Services (WSI) bill in March 1999 saying that it failed to adequately restrict surveillance by military agencies.[511]

Controversy still surrounds efforts to create an expanded national id system. The Electronic Census System (PESEL) number, which was issued since the mid-1970s, is the biggest collection of personal data in Poland. Every identity card contains a PESEL number, which confirms the owner's date of birth and sex. The system is fully computerized. A Tax Identification Number (NIP) is also being developed. This system will be fully computerized in the near future.

REPUBLIC OF PORTUGAL

The Portuguese Constitution has extensive provisions on protecting privacy, secrecy of communications and data protection. In 1997, Article 35 of the Constitutional was amended to give citizens a right to data protection.

The 1998 Act on the Protection of Personal Data adopts the E.U. Data Protection requirements into Portuguese law.[512] It limits the col-

506. Art. 237.

507. Konrad Niklewicz, *Bugged About Wiretapping*, WARSAW VOICE, May 26, 1996.

508. *Id.*

509. *UOP Head Confirms Political Surveillance*, POLISH NEWS BULL., Apr. 8, 1999.

510. *Former Prime Ministers to Testify in Surveillance Case*, POLISH NEWS BULL., Apr. 8, 1999.

511. *Military Intelligence Bill Criticized*, POLISH NEWS BULL., Feb. 17, 1999.

512. Act n° 67/98 of 26 October. 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) <http://www.cnpd.pt/Leis/lei_6798en.htm>.

lection, 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.[513]

The Act is enforced by the National Data Protection Commission (Comissão Nacional de Protecção de Dados - CNPD).[514] The Commission is an independent Parliament-based agency that registers databases, authorizes and controls databases, issues directives, and oversees the Schengen information system.[515] In 1997, the commission conducted 35 investigations, mostly banks and other financial institutions, information and business companies and filed seven complaints with the Attorney General's Office. It also authorized 507 databases.[516] In June 1997, the Supreme Administrative Tribunal upheld the Commission in a case against a shoe company that used smart cards to control employees' bathroom visits.

The penal code has provisions against unlawful surveillance and interference with privacy.[517] Evidence obtained by any violation of privacy, the home, correspondence or telecommunications without the consent of the interested party is null and void.[518] 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.[519] The Portuguese government ordered cellular telephone companies to assist with surveillance in October 1996.[520]

There are also specific laws on the Schengen Information System,[521] computer crime,[522] and counseling centers.[523]

---

513. Lei n° 10/91 - Lei da Protecção de Dados Pessoais face à Informática, <http://www.cnpdpi.pt/Leis/lei_1091.htm>. Amended by Lei n.° 28/94, de 29 de Agosto. Aprova medidas de reforço da protecção de dados pessoais <http://www.cnpdpi.pt/>.

514. Comissão Nacional De Protecção De Dados (visited Nov. 11, 1999) <http://www.cnpd.pt/>.

515. Compentencias (visited Jan. 2, 1999) <http://www.cnpdpi.pt/bin/competencias.htm>.

516. National Commission for the Protection of Computerised Personal Data ("NCPCPD"), *1997 Report* (visited Nov. 11, 1999) <http://www.cnpd.pt/bin/rel97ing.htm>.

517. Chapter VI, Penal Code, Section 179-183.

518. Article 126 of the Code of Penal Procedure para. 3. *See* U.N., Committee Against Torture, *Consideration of Reports Submitted by States Parties Under Article 19 of the Convention*, Addendum, Portugal, June 10, 1997.

519. *Bug Found in Portuguese State Prosecutor's Office*, THE REUTERS EUROPEAN BUSINESS REPORT, Apr. 27, 1994.

520. *Portugal to Tap Mobile Phones in Drugs War*, REUTERS WORLD SERVICE, Oct. 9, 1996.

521. Lei n.° 2/94, de 19 de Fevereiro Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen <http://www.cnpdpi.pt/Leis/lei_294.htm>.

522. Lei n° 109/91 - Sobre a criminalidade informática <http://www.cnpdpi.pt/Leis/lei_10991.htm>.

RUSSIAN FEDERATION

Articles 23, 24 and 25 of the Constitution of the Russian Federation recognizes rights of privacy, data protection and secrecy of communications.[524] The Duma approved the Law of the Russian Federation on Information, Informatization, and Information Protection in January 1995.[525] The law covers both the government and private sectors and licenses the processing of personal information by the private sector. It prohibits using personal information to "inflict economic or moral damage on citizens." Using sensitive information (social origin, race, nationality, language, religion or party membership) is also prohibited. Citizens and organizations have the right to access the documented information about them, correct it, and supplement it.

The Russian law does not establish a central regulatory body for data protection and it is not clear that it was effective. The law specifies that responsibility for data protection rests with the data controllers. The Committee of the State Duma on Information and Informatization and the State Committee on Information and Informatization under the Russian President Authority oversee the law.

There are currently efforts by the two oversight committees to update the data protection law to make it more compliant with the Council of Europe's Convention 108 and the E.U. Directive.

Secrecy of communications is protected by the 1995 Communications Act. The tapping of telephone conversations, scrutiny of electric-communications messages, delay, inspection and seizure of postal mailings and documentary correspondence, receipt of information thereon, and other restriction of communications secrets are allowed only on the basis of a judicial decision.[526] The Law on Operational Investigation Activity regulates surveillance methods of the secret services and requires a warrant.[527] This law was amended in December 1998 by the State Duma: guarantees for the protection of privacy were stressed and additional controls imposed on prosecutors. Previously, there were numerous reports that the security services conducted illegal wiretaps of politicians throughout Russia. In June 1998, it was publicly revealed that the Federal Security Service was drafting a ministerial act code-named SORM-2

523. Act No. 3/84 of 24 Mar.

524. Konstitutsiia RF [Constitution of the Russian Federation] [Konst. RF] (1993), *available at* <http://www.friends-partners.org/oldfriends/constitution/russian-const-ch2.html>.

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

526. *RF Communications Act Russian Federation Federal Act No. 15-FZ Adopted* by *the State Duma on Jan. 20, 1995*, RUSLEGIS LINE, Feb. 16, 1995.

527. *Yeltsin Signs Law Regulating Criminal Investigations*, OMRI, Aug. 16, 1995.

(Systems for Ensuring Investigative Activity) that would require Internet Service Providers to install surveillance devices and high speed links to the Federal Security Service in their systems agencies which would allow police direct access to the communications of Internet users without a warrant.[528] By the end of summer 1999 this document was still not signed and published in open media, but Russian secret services pressed on ISPs to install SORM systems as an alternative of loosing licenses. The only Russian provider opposing the illegal wiretapping proposals was cut from the Internet and is now under threat of being shut down.[529]

There are also privacy protections in the Civil Code[530] and Criminal Code.[531] The United Nations Human Rights Committee expressed concerns over the state of privacy in Russia in 1995 and recommended enacting 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 a 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."[532]

REPUBLIC OF SAN MARINO

The Act Regulating the Computerized Collection of Personal Data was enacted in 1983 and amended in 1995.[533] The Act applies to any computerized filing system or data bank, both private and public. It prohibits collecting personal and confidential data through fraudulent, illegal or unfair means. It requires that information be accurate, relevant

528. *Russia Prepares To Police Internet*, THE MOSCOW TIMES, July 29, 1998. English translation of bill is available at <http://www.fe.msk.ru/libertarium/sorm/sormdocengl.html>.

529. Marina Moudrak, *Russian ISP Refuses To Spy On Customers*, DATA COMMUNICATIONS, July 26, 1999.

530. *Civil Code, Article 19. RF Act No. 51-FZ Adopted By The State Duma on Oct. 21, 1994*, RUSLEGISLINE, July 8, 1994.

531. The Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996.

532. U.N. Human Rights Comm., *Comments on Russian Federation*, U.N. Doc. CCPR/C/79/Add.54 (1995), July 26, 1995 <http://www.law.wits.ac.za//humanrts/hrcommittee/RUSSIA.htm>.

533. Regulating the Computerized Collection of Personal Data, Law N. 70 of 23 May 1995 revising Law N. 27 of 1 Mar. 1983. Amended by law 70/95, *available at* <http://www.hri.ca/fortherecord1997/ documentation/commission/e-cn4-1997-67.htm>.

and complete. Any individual is entitled both to inquire whether his or her personal data was collected or processed, obtain a copy, and 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.[534] The Regulation on Statistical Data Collection and Public Competence in Data Processing[535] regulates data processing within the Public Administration.

The Act is enforced by the Guarantor 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. Releasing 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.

REPUBLIC OF SINGAPORE

The Singapore Constitution is based on the British system and does not contain any explicit right to privacy.[536] The High Court has ruled that personal information may be protected from disclosure under a duty of confidences.[537]

There is no general data protection or privacy law in Singapore. The government has been aggressive in using surveillance to promote social control and limit domestic opposition.[538] In 1986, then-Prime Minister

534. Decree N. 7 of 13 Mar. 1984, *Establishment of a State Data Bank as provided for by Article 5 of Law N. 27 of 1 Mar. 1983*; Decree N. 7 of 3 June 1986, *Integration to Decree N. 7 of 13 Mar. 1984, Establishing a State Data Bank*; Decree N. 140 of 26 Nov. 1987, *Procedures for the Establishment of Private Data Banks*.

535. *Regulation on Statistical Data Collection and Public Competence in Data Processing*, LAW N. 71 of May 23, 1995.

536. Constitution of the Republic of Singapore, Sept. 16, 1963, *available at* <http://www.uni-wuerzburg.de/law/sn000_.html>.

537. X v CDE [1992] 2 SLR 996.

538. *See* CHRISTOPHEN TREMEWAN, THE POLITICAL ECONOMY OF SOCIAL CONTROL IN SINGAPORE (St. Martin's Press, 1994).

and founder of modern Singapore Lee Kwan Yew proudly described his stance on privacy:

> I am often accused of interfering in the private lives of citizens. Yet, if I did not, had I not done that, we wouldn't be here today. And I say without the slightest remorse, that we wouldn't be here, we would not have made economic progress, if we had not intervened on very personal matters – who your neighbor is, how you live, the noise you make, how you spit, or what language you use. We decide what is right, never mind what the people think. That's another problem.[539]

In September 1998, the National Internet Advisory Board proposed an industry-based self-regulatory "E Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce."[540] The code would oblige providers to ensure confidentiality of business records and personal information of users, including details of usage or transactions, would prohibit the disclosure of personal information, and would require providers not to intercept communications unless required by law. The code would also limit collection and prohibit disclosure of personal information without informing the consumer and giving them an option to stop the transfer, ensure accuracy of records and provide a right to correct or delete data. The Code would be enforced by an industry-run Compliance Authority. Providers that complied could use a "Privacy Code Compliance Symbol." The regulatory authority for the electronic medium in Singapore is the Singapore Broadcasting Authority (SBA). SBA is a statutory board under the Ministry of Information and the Arts (MITA).

In July 1998, the Singapore government passed three major bills concerning computer networks. They are the Computer Misuse (Amendment) Act, Electronic Transactions Act and National Computer Board (Amendment) Act. The CMA prohibits the unauthorized interception of computer communications.[541] The CMA also provides the Police with additional powers of investigations. Under the amended Act, it is now an offense to refuse to assist the Police in an investigation. Amendments also widened the provisions allowing the Police lawful access to data and encrypted material in their investigations of offenses under the CMA as well as other offenses disclosed during their investigations. Such 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 SG$10,000 fine and 12 month jail

539. Lee Kwan Yew's Speech at National Day Rally, 1986, STRAIGHTS TIMES, Apr. 20, 1987, Cited in *The Political Economy of Social Control in Singapore.*

540. REPORT OF THE NATIONAL INTERNET ADVISORY BOARD (1997/1998) <http://www.sba.gov.sg/work/sba/internet.nsf/>.

541. Computer Misuse Act (Ch. 50A) (Aug. 30, 1993) <http://www.lawnet.com.sg/freeaccess/ CMA.htm>.

sentence for disclosing those records without authorization. Police have broad powers to search any computer to require disclosure of documents for an offense related to the act without a warrant.[542]

Electronic surveillance of communications is governed by the Telecommunications Authority of Singapore (TAS). 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 U.S. State Department in 1998 stated, "Divisions of the Government's law enforcement agencies, including the Internal Security Department and the Corrupt Practices Investigation Board, have wide networks for gathering information. It is believed that the authorities routinely monitor citizens' telephone conversations and use of the Internet. While there were no proven allegations that they did so in 1997, it is widely believed that the authorities routinely conduct surveillance on some opposition politicians and other critics of the Government."[543] All of the Internet Services Providers are operated by government-owned or government-controlled companies.[544] Each person in Singapore wishing to obtain an Internet account must show their national ID card to the provider to obtain an account.[545] ISPs reportedly provide information on users to government officials without 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 email 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 US$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, sites people access, or download.[546] 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 Telecommunications Authority of Singapore said that the ISP had violated no law, but SingNet apologized for the scans and the National Information Technology Committee announced that it would create new

542. Electronic Transactions Act (Act 25) (1998) <http://www.lawnet.com.sg/freeaccess/ETA.htm>.

543. U.S. Department of State, *Singapore Country Report on Human Rights Practices for 1997* (Jan. 30, 1998).

544. Garry Roday, *The Internet and Social Control in Singapore*, POL. SCI. Q. Vol. 113, No. 1, Spring 1998.

545. *Id.*

546. THE STRAITS TIMES, Sept. 27, 1996.

guidelines.[547]

An extensive Electronic Road Pricing 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.[548] The service claims that the data will only be kept for 24 hours and does not maintain a central accounting system. Video surveillance cameras are also commonly used for monitoring roads and preventing littering in many areas.[549] It was proposed in Tampines in 1995 that cameras be placed in all public spaces including corridors, lifts, and open areas such as public parks, car parks and neighborhood centers and broadcast on the public cable television channel.[550] A man was prosecuted under the Films Act in May 1999 for filming women in bathrooms.[551]

The Banking Act prohibits disclosure of financial information without the permission of the customer.[552] Numbered accounts can also be opened with the permission of the authority. The High Court can require disclosure of records to investigate drug trafficking and other serious crimes. The Monetary Authority of Singapore 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.[553] Banks must report suspicious transactions to the MAS.

SLOVAK REPUBLIC

Articles 16, 19 and 22 of the 1992 Constitution provides for protections for privacy, data protection and secrecy of communications.[554] The Act on Protection of Personal Data in Information Systems was approved

547. *ISPs to Get Guidelines on Scanning*, THE STRAITS TIMES, May 12, 1999.

548. *You're on Candid Camera*, THE STRAITS TIMES, Sept. 2, 1998.

549. *Video Cameras to Monitor Traffic at 15 Junctions*, THE STRAITS TIMES, Mar. 12, 1995; *Surveillance System Set up in Jurong East*, THE STRAITS TIMES, July 16, 1996.

550. Ravi Veloo, *Do We Really Want an All-Seeing Camera?*, THE STRAITS TIMES, July 13, 1995.

551. Elena Chong, *Peeping Tom Used Hidden Camera to Spy*, THE STRAITS TIMES, May 29, 1999, at 73.

552. Banking Act, Ch. 19 (Rev. edition 1999) <http://www.mas.gov.sg/statutes/BankingAct-c.html>.

553. Monetary Authority of Singapore, *Guidelines On Prevention Of Money Laundering* (May 26, 1999) <http://www.mas.gov.sg/regulations/notices_MAS824-c.html>.

554. SLOVK CONST. of 1992, art. 16, 19, 22 <http://www.sanet.sk/Slovakia/Court/const.html>.

in February 1998.[555] The Act replaces the previous 1992 Czechoslovakian legislation (see Czech Republic report for information). The new act closely tracks the E.U. Data Protection Directive and limit 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 information on racial, ethnic, political opinions, religion, philosophical beliefs, trade union membership, health, and sexuality is forbidden. Transfers to other countries are limited unless the country has "adequate" protection. All systems are required to register with the Statistical Office of the Slovak Republic.[556] The Act creates a new office for a Commissioner for the Protection of Personal Data in Information Systems who will supervise and enforce the Act.

Under the Code of Criminal Procedure, the police are required to obtain permission from a court or prosecutor before undertaking any telephone tapping.[557] However, the communist-era secret police remain unreformed and there were many public revelations of illegal wiretapping of opposition politicians, reporters and dissidents.[558] In 1997, the UN Human Rights Committee recommended that the government: "ensure control, by an independent judicial authority, of the interception of confidential communications – related to, for example, wire-tapping and protection of the right to privacy."[559]

There are also other legal protections. Article 11 of the Civil Code states "everyone shall have the right to be free from unjustified interference in his or her privacy and family life." There are also computer-related offenses linked with the protection of a person (unjustified treatment of a personal data).[560] 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 if this is 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

555. Act No. 52 of Feb. 3, 1998 on Protection of Personal Data in Information Systems. <http://www.statistics.sk/webdata/english/acts/act5298/acts5298.htm>.

556. Statistical Office of the Slovak Republic <http://www.statistics.sk/webdata/ english/index2.htm>.

557. Code of Criminal Procedure, § 86 to 88.

558. *Hungarian Politicians in Slovakia are Being Bugged*, CTK NATIONAL NEWS WIRE, Feb. 21, 1995. *Deputy Brings Charges Against Slovak Secret Services Spokesman*, CTK NATIONAL NEWS WIRE, Aug. 21, 1997.

559. U.N. Human Rights Comm., *July/Aug. 1997 Session* <http://www.hri.ca/fortherecord1997/ vol5/slovakia.htm>.

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

peoples' basic rights and their right to privacy."[561]

REPUBLIC OF SLOVENIA

Articles 35, 37 and 38 of the 1991 Constitution recognizes the rights of privacy, secrecy of communications and data protection.[562] The Law on Personal Data Protection was enacted in 1990.[563] It broadly adopts the basic principles of the OECD Guidelines on the Protection of Privacy and the Council of Europe's Convention. Specifically, the law regulates the security of personal data in data files; restricts third-party access and use only upon the written consent of the data subject; provides for data subject access to his or her files; and permits the transfer of personal data to other countries only if the recipient country guaranteed "full protection of personal data" to include that held on "foreign citizens." However, the Slovenian law merely provides for a somewhat nebulous "republican organ" oversight of personal data protection practices, and therefore is not compliant with the pan-European instruments on data protection, including the E.U.'s Privacy Directive.

Slovenia is in the process of amending its data protection law to be fully compliant with E.U. and COE requirements. This includes establishing a separate data protection office. Since Slovenia is one of the first of central and eastern European nations likely to join the E.U., it was told by European Internal Market Commissioner Mario Monti during his visit to Slovenia in May 1998, that "legislative adjustments" to its data protection law were required before the country could accede to E.U. membership.[564] Slovenia hopes to conclude its negotiations and enter the E.U. as a full member by the year 2002.

A judge's warrant must be issued prior to a house search or telephone tapping. A new Law on the Police was adopted in 1998 allows for surveillance to be authorized under special circumstances by a General Police Director.[565] In 1994, Parliament fired the country's defense minister, Janez Jansa, following claims that he tapped journalists' phones.[566] Defense Minister Tit Turnsek resigned in February 1998 after two military intelligence officers were arrested by Croatian authorities while

561. *Court Rules Law on Public Prosecutors Unconstitutional*, CTK NATIONAL NEWS WIRE, Mar. 4, 1998.

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

563. Law on Personal Data Protection, Mar. 7, 1990, THE OFFICIAL JOURNAL OF THE REPUBLIC OF SLOVENIA, No. 8/90, 38/90 and 19/91.

564. *E.U. / Slovenia: Monti Stands Firm on Need for Follow-through of New Legislation*, EUROPEAN REPORT, May 16, 1998.

565. Law on the Police, July 18, 1998.

566. United Press International, Mar. 28, 1994.

driving a vehicle filled with electronic surveillance equipment.[567] The Law on National Statistics regulates the privacy of information collected for statistical purposes.[568]

REPUBLIC OF SOUTH AFRICA

Section 14 of the South African Constitution of 1996 recognizes the rights of privacy, freedom of information and data protection.[569] The South African Constitutional Court delivered a number of judgments on the right to privacy relating to the possession of indecent or obscene photographs,[570] scope of privacy in society,[571] and searches.[572] All the judgments were delivered under the provisions of the Interim Constitution as the causes of action arose prior to the enactment of the Final Constitution. However, as there is no substantive difference between the privacy provisions in the Interim and Final Constitutions, the principles remain authoritative for future application.

South Africa is currently in the process of adopting a comprehensive privacy and freedom of information law. The Open Democracy Bill was introduced in July 1998.[573] The bill covers both public and private sector entities and allows for access, rights of correction and limitations on disclosure of information. The bill would be enforced by the Human Rights Commission. This Bill is now before the Portfolio Committee on Justice, which promised to hold public hearings on the final draft before sending the Bill to Parliament for tabling. Human Rights Commissioner Pansy Tlakula criticized the draft in July 1999 for not providing access to information held by private institutions or individuals. Parliament has a deadline of February 2000 to enact the bill.

South Africa does not have a privacy commission, but has a Human Rights Commission which was established under Chapter 9 of the Constitution and whose mandate is to investigate infringements on and protect the fundamental rights guaranteed in the Bill of Rights, and to take steps to secure appropriate redress where human rights were violated.

---

567. Deutsche Presse-Agentur, Feb. 25, 1998.

568. Law on National Statistics (July 25, 1995) <http://www.sigov.si/zrs/eng/szakoni.html>.

569. The Constitution of the Republic of South Africa, Act 108 of 1996, *available at* <http://www.parliament.gov.za/legislation/1996/saconst.html>.

570. Case and Another v. Minister of Safety and Security and Curtis and Another v. Minister of Safety and Security 1996, (3) SA 617 (CC).

571. Bernstein and others v. Von Weilligh Bester NO and others, 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (SA) - delivered Mar. 27, 1996.

572. Mistry v. The Interim National Medical and Dental Council of South Africa and others as yet unreported, CCT 13/97, decided on May 29, 1998.

573. Open Democracy Bill No. 67 (1998) <http://www.parliament.gov.za/bills/1998/b67-98.pdf>.

The Interception and Monitoring Act of 1992 regulates the interception of communications.[574] This Act prohibits the intercepting of certain communications and monitoring of certain conversations, and also provides for intercepting of postal articles and communications and monitoring of conversations in the case of a serious offense, or if the security of the country is threatened. In 1996, it was revealed that the South African Police Service was monitoring thousands of international and domestic phone calls without a warrant.[575] In November 1998, the South African Law Commission recommended changes to the Interception and Monitoring Act to facilitate monitoring of cellular phones and Internet Service Providers.[576]

There are no other specific pieces of legislation on general data protection law. Other than the Constitutional right to privacy, the South African common law protects rights of personality under the broad umbrella of the *actio injuriarum.* The elements of liability for an invasion of privacy action are the same as any other injury to the personality, namely an unlawful and intentional interference with another's right to seclusion and private life.

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. This is part of the information technology strategy formulated by the Department of Communications to provide kiosks for access to government services.[577] In the long term, the smart card is intended to function as passport, driver's license, identity document and bank card. The driver's license will include fingerprints.

KINGDOM OF SPAIN

Article 18 of the Constitution recognizes the right to privacy, secrecy of communications and data protection.[578] The Spanish Data Protection Act (LORTAD) was enacted in 1992 and based on an early draft of the E.U. Directive.[579] It covers automated files held by the public and private sector. The law establishes the right of citizens to know what per-

574. Interception and Monitoring Prohibition Act, No. 77 of 1992 (amended by the Intelligence Services Act, No. 38 of 1994).

575. *Newspaper Uncovers 'Unlawful' Tapping by Intelligence Units*, THE STAR, Feb. 21, 1996.

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

577. David Shapshak, *SA Services Get 'Smart'*, MAIL & GUARDIAN, Apr. 24, 1998.

578. Constitucion [Constitution of Spain, Amendment Aug. 27, 1992] [C.E.], *available at* <http://www.uni-wuerzburg.de/law/sp00t___.html>.

579. Ley Organica 5/1992 de 29 de Octubre de Regulación del Tratamiento Automatizado de los Datos de Caracter Personal (LORTAD). <http://www.ag-protecciondatos.es/datd1.htm>.

sonal data is contained in computer files and the right to correct or delete incorrect or false data. Personal information in an automated system may only be used or disclosed to a third party with the consent of the individual and only for the purpose which it was collected. The government approved a bill revising the act to make it consistent with the E.U. Directive in July 1998. It is waiting to be approved by the Parliament.

The Agencia de Protección de Datos is charged with enforcing the LORTAD.[580] The Agency maintains the registry and can investigate violations of the law. The agency issued a number of decrees setting out in more detail the legal requirements for different types of information.[581] It can also impose penalties. In June 1997, it fined Telefonica, the Spanish telephone company, 110 million pesetas for providing information from their subscriber database to banks, direct marketing companies and Reader's Digest.[582] The agency in 1997 registered 3,312 new databases, received 682 complaints, conducted over 10,000 telephone consultations, and issued 20 reports.[583] As of December 1997, 229,000 databases were listed in the Register.

Interception of communications requires a court order.[584] The 1997 Telecommunications Act amended the law and restricted the use of cryptography.[585] There were a number of scandals in Spain over illegal wiretapping by the intelligence services. In 1995, Deputy Prime Minister Narcis Serra, Defense Minister Julian Garcia Vargas and military intelligence chief Gen. Emilio Alonso Manglano were forced to quit following revelations that they had monitored the conversations of hundreds of people, including King Juan Carlos.[586] In May 1999, Gen. Manglano, the former director of the CESID, and Col. Juan Alberto Perote, a former operations chief were convicted and sentenced to six months jail time for their role in the wiretappings. Five other ex-agents who did the actual surveillance were given four-month terms.[587]

---

580. Agencia de Protección de Datos [Data Protection Agency] <http://www.agprotecciondatos.es>.

581. *See* Agencia de Protecction de Datos, *Legislaccion* (visited Jan. 2, 2000) <http://www.ag-protecciondatos.es/datd.htm>.

582. *Telefonica De Espana Appeals Fine For Sharing Database*, DOW JONES, June 19, 1997.

583. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Second Annual Report* (Nov. 30, 1998).

584. Ley Organica 11/1980 de 1 de Dec 1980. Penal Code, Sections 196-199.

585. *See* Global Internet Liberty Campaign Member Statement, *New Spanish Telecommunications Law Opens a Door to Mandatory Key Recovery Systems* (July 1998) <http://www.gilc.org/crypto/spain/ gilc-crypto-spain-798.html>.

586. *Spain Socialists Seek Opposition Apology on Bugging*, REUTERS, Feb. 6, 1996.

587. *Ex-Spy Chief Sentenced in Spain*, AP ONLINE, May 26, 1999.

There are also additional laws in the penal code,[588] and relating to credit information[589] video surveillance,[590] and automatic tellers.[591] The Spanish Supreme Court ruled in March 1999 that a Spanish reporter who disclosed the initials of two AIDS-infected inmates working in a prison kitchen would be given a one-year suspended sentence, fined $26,000 and be barred from journalism for a year.[592]

KINGDOM OF SWEDEN

Sweden's Constitution, which consists of several different legal documents, contains several provisions that are relevant to data protection. Section 2 of the Instrument of Government Act of 1974[593] provides, *inter alia*, for protecting individual privacy. Section 13 of Chapter 2 of the same instrument states also that freedom of expression and information – which are constitutionally protected pursuant to the Freedom of the Press Act of 1949[594] – can be limited with respect to the "sanctity of private life." Moreover, Section 3 of the same chapter provides for a right to protection of personal integrity relating to automatic data processing. The same article also prohibits non-consensual registration of persons purely on the basis of their political opinion. It is also important to note that the European Convention on Human Rights (ECHR) was incorporated into Swedish law as of 1994. The ECHR is not formally part of the Swedish Constitution, but has, in effect, similar status.

Sweden enacted the Personal Data Act of 1998 to bring Swedish law into conformity with the requirements of the EC Directive on data protection.[595] The new Act basically repeats what is set out in the EC Directive. This Act regulates the establishment and use, in both public and private sectors, of automated data files on physical/natural persons. The Act replaced the Data Act of 1973, which was the first comprehensive national act on privacy in the world.[596] The 1973 Act shall continue to

588. *See* Nuevo Codigo Penal, *Delitos Relacionados con la Technologias de la Informacion* (visited Jan. 2, 2000) <http://www.onnet.es/ley0009.htm>.

589. INSTRUCCION 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito <http://www.onnet.es/ley0029.htm>.

590. LEY ORGÁNICA 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos <http://www.onnet.es/ley0064.htm>.

591. Seguridad en cajeros automáticos y otros servicios. ORDEN de 23 de abril de 1997 <http://www.onnet.es/ley0060.htm>.

592. *Spanish Court Convicts Reporter,* AP ONLINE, Mar. 4, 1999.

593. Regeringsformen, SFS 1974:152.

594. Tryckfrihetsförordningen, SFS 1949:105.

595. Personuppgiftslagen, SFS 1998:204, to be in force Oct. 24, 1998, *available at* <http://www.din.se/RTF-filer/pul-eng.rtf>.

596. Datalagen, SFS 1973:289.

apply until October 2001 with respect to processing of personal data which is initiated prior to October 24, 1998. Following some controversy over applying the act to the Internet, the Data Inspection Board proposed revising the act to cover "harmless data" "if it is obvious that there is no risk of infringement of the privacy of the data subject." This proposal will be introduced in the fall.

The Data Inspection Board (Datainspektionen) is an independent board overseeing the enforcement of the Data Act.[597] As of June 1999, under the new Act, the board received 102 complaints and made 28 investigations. In 1998, the board received 269 complaints and conducted 199 investigations. In 1997, it received 250 complaints and made 302 investigations. There are 47,921 registered databases.[598] The Board was active in trying to limit the use of the personal identity number.[599] They are also pursuing a case against SABRE, the airline reservation system, for transferring medical information of passengers without adequate controls. The case is currently pending before the Supreme Administrative Court. Several lower courts upheld the Board's ruling.

Numerous other statutes also contain provisions relating to data protection. These include the Secrecy Act of 1980,[600] Credit Reporting Act of 1973,[601] Debt Recovery Act of 1974,[602] and Administrative Procedure Act of 1986.[603] A court order is required to obtain a wiretap.[604] The law was amended in 1996 to facilitate surveillance of new technologies.[605]

Over the past year, there was increasing publicity and discussion about the fact that Sweden's police/security services have carried out, over a long period, covert surveillance of a large number of Swedish citizens, mostly political leftists, often on highly tenuous or trivial grounds. Pressure is mounting for an official Commission of Inquiry to be set up, similar to the Commission set up in Norway (see above), in order to investigate these surveillance practices, which were demanded by the United States as a condition to receiving military technology. Previously, it was also discovered that the Swedish statistical agency, Statistika, was monitoring 15,000 Stockholm residents born in 1953 in intimate de-

597. Data Inspection Board <http://www.din.se/>.

598. Email Communications from The Data Inspection Board, June 23, 1999.

599. Anitha Bondestam, "Identity Numbers," Presentation at the XVth International Conference of Data Protection and Privacy Commissioners, Sept. 1993.

600. Sekretesslagen, SFS 1980:100. For information on the background to the new Act, see Integritet—Offentlighet—Informationsteknik [Integrity—Publicity—Information Technology], SOU 1997:39.

601. Kreditupplysningslag, SFS 1973:1173.

602. Inkassolag, SFS 1974:182.

603. Förvaltningslagen, SFS 1986:223.

604. Law 1974/203 amended by Law 1989/529.

605. Law of May 8, 1996.

tail. The information included statistics on drinking habits, religious beliefs, and sexual orientation. The DIB was not even aware of this program and subsequently ordered the destruction of the master tape containing the data.[606]

SWISS CONFEDERATION (SWITZERLAND)

Article 36(4) of the Constitution protects the secrecy of communications.[607] The Federal Act of Data Protection of 1992 regulates personal information held by government and private bodies.[608] The Act requires that information be legally and fairly collected and places limits on its use and disclosure to third parties. Private companies must register if they regularly process sensitive data or transfer the data to third parties. Transfers to other nations must be registered and the recipient nation must have equivalent laws. Individuals have a right of access to correct inaccurate information. Federal agencies must register their databases. There are criminal penalties for violations. There are also separate data protection acts for the Cantons (states). In June 1999, the E.U. Data Protection Working Party determined that Swiss law was adequate under the E.U. Directive.[609]

The Act creates a Federal Data Protection Commission.[610] The commission maintains and publishes the Register for Data Files, supervises federal bodies and private bodies, provides advice, issues recommendations and reports, and conducts investigations. The commissioner also consults with the private sector. Its most recent report, the Commission recommended that ISPs and Website hosts institute clear data protection policies.[611]

Telephone tapping is governed by the Penal Code and Penal Procedure Code amended by the 1997 Telecommunication Act.[612] A court order is required for every wiretap. A proposal to modify wiretapping and

606. WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 64 (New York: Stockton Press, 1992).

607. Bundesverfassung, Constitution federale, Costituzione federale [Constitution of Switzerland] [BV, CST., COST. FED.], *available at* <http://www.uni-wuerzburg.de/law/sz00t___.html>.

608. Loi fédérale sur la protection des données ("LPD") (19 juin 1992) <http://www.admin.ch/ch/f/rs/235_1/index.html>.

609. Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 5/99 on the level of protection of personal data in Switzerland* (June 7, 1999) <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp22fr.pdf>.

610. Swiss Federal Data Protection Commissioner (visited Jan. 2, 2000) <http://www.edsb.ch/>.

611. Préposé fédéral de la protection des données, *Rapport d'activités* 1998/99. p. 241.

612. Art 66-73, Procédure pénal fédérale. Loi de 23 Mars 1979 sue la protection de la vie priveé. Telecommunications Law 30.04.97/BAKOM/TC/frm ("LTC") (Apr. 30, 1997) <http://www.admin.ch/ bakom/tc/fmg2/e/fmg2_30.4.97.htm>. O du 1er décembre 1997 sur le ser-

mail interception was introduced in July 1998.[613] There were 1,020 wiretaps authorized in 1996.[614] There have been numerous public revelations of illegal wiretapping. A 1993 inquiry found that phones used by journalists and ministers in the Swiss Parliament were tapped.[615] The Data Protection Commissioner also accused PTT, the state telephone company, of illegally wiretapping telephones. There were considerable protests in 1996 when it was revealed that the federal government was wiretapping journalists to discover their sources. Swiss President Arnold Koller described the taps as "excessive."[616] In December 1997, the newspaper Sonntags Zeitung reported that Swisscom, the Swiss telephone company, was tracking the location of cellular phone users and maintaining those records for an extended period.[617] The Data Protection Commissioner issued a report in July 1998.[618] A Department of Justice working group has been developing revisions for the legislation for several years and in 1999, the Privacy Commission withdrew its support after the working group expanded the number of offenses to include many minor offenses.[619]

Besides the Data Protection Act, there are also legal protections for privacy in the Civil Code[620] and Penal Code,[621] and special rules relating to workers' privacy from surveillance,[622] telecommunications information,[623] banking privacy,[624] health care statistics,[625] professional

---

vice de surveillance de la correspondance postale et des télécommunications <http://www.admin.ch/ch/f/rs/c780_11.html>.

613. Deparyement Federal de Justice et Police, Ecoutes téléphoniques: Communiqué de presse (1er juillet 1998) <http://www.admin.ch/cp/f/359B36DB.3BB3@mbox.gsejpd.admin.ch.html>.

614. Conseil national: Session d'automne 1997, Surveillance téléphonique, 10 octobre 1997.

615. Statewatch Bulletin, vol. 3 no 1, Jan.-Feb. 1993.

616. *Phone Taps Raise Ire Of Swiss Public*, CHRISTIAN SCIENCE MONITOR, Mar. 14, 1997.

617. DIGITAL CELLULAR REPORT (Jan. 15, 1998).

618. *See* (visited Jan. 2000) <http://jya.com/swisscom-nix.htm>.

619. Préposé fédéral de la protection des données, Rapport d'activités 1998/99.

620. § 28 of the Civil Code, Dec. 10, 1907.

621. Code pénal, Titre troisiéme: Infractions contre l'honneur et contre le domaine secret ou le domaine privé, Art 173-179.

622. Section 328 of the Code of Obligations. *See* International Labour Organization, Conditions of Work Digest, Vol. 12, 1/1993.

623. Telecommunications Law ("LTC") (Apr. 30, 1997) <http://www.admin.ch/bakom/tc/fmg2/ e/fmg2_30.4.97.htm>.

624. 1934 Federal Banking Law on Privacy. *See* Paolo S. Grassi & Daniele Calvarese, *The Duty of Confidentiality of Banks in Switzerland: Where it Stands and Where it Goes. Recent Developments and Experience. The Swiss Assistance to, and Cooperation with the Italian Authorities in the Investigation of Corruption Among Civil Serviants in Italy (The "Clean Hands" Investigation): How Much is Too Much?*, 7 PACE INT'L L. REV. 329 (discussing effects of money laundering legislation on limiting banking privacy).

confidentiality including medical and legal information,[626] medical research,[627] police files,[628] and identity cards.[629] In 1989, a Parliamentary inquiry revealed that the Federal Police had collected files on about 900,000 people, most of whom were not suspected of committing any offense.

REPUBLIC OF CHINA (TAIWAN)

Article 12 of the 1994 Taiwanese Constitution protects the privacy of correspondence.[630] The Computer-Processed Personal Data Protection Law was enacted in August 1995.[631] The Act governs the collection and use of personally identifiable information by government agencies and many areas of the private sector. The Act requires that "[t]he collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose." Individuals have a right of access and correction, the ability to request cessation of computerized processing and use, and the ability to request deletion of data. Data flows to countries without privacy laws can be prohibited.[632] Damages can be assessed for violations. The Act also establishes separate principles for eight categories of private institutions: credit information organizations, hospitals, schools, telecommunication businesses, financial businesses, securities businesses, insurance businesses, mass media, and "other enterprises, orga-

625. Office fédéral de la statistique, *La protection des données dans la statistique médicale* (1997) <http://www.admin.ch/bfs/stat_ch/ber14/statsant/ff1403c.htm>.

626. Code pénal, Art 320-322.

627. O du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale ("OALSP") (14 juin 1993) <http://www.admin.ch/ch/f/rs/c235_154.html>.

628. O du 31 août 1992 sur le système provisoire de traitement des données relatives à la protection de l'Etat ("Ordonnance ISIS") (31 août 1992) <http://www.admin.ch/ch/f/rs/c172_213_60.html>. O du 14 juin 1993 concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat (14 juin 1993) <http://www.admin.ch/ch/f/rs/c235_14.html>. O du 19 juin 1995 sur le système de recherches informatisées de police ("RIPOL") <http://www.admin.ch/ch/f/rs/c172_213_61.html>.

629. O du 18 mai 1994 relative à la carte d'identité suisse <http://www.admin.ch/ch/f/rs/c143_3.html>.

630. Zhonghua Renmin Gongheguo Xianfa [Constitution of the Republic of China, Adopted by the National Assembly on Dec. 25, 1946, promulgated by the National Government on Jan. 1, 1947, and effective from Dec. 25, 1947] [XIANFA], *available at* <http://www.oop.gov.tw/roc/charter/echarter.htm>.

631. Computer-Processed Personal Data Protection Law of Aug. 11, 1995.

632. Graham Greenleaf, A Proposed Privacy Code for Asia-Pacific Cyberlaw (visited Jan. 2, 2000) <http://jcmc.huji.ac.il/vol2/issue1/asiapac.html>.

nizations, or individuals designated by the Ministry of Justice and the central government authorities in charge of concerned end enterprises."

There is no single privacy oversight body to enforce the Act. The Ministry of Justice enforces the Act for government agencies. For the private sector, the relevant government agency for that sector enforces compliance. The Criminal Investigation Bureau (CIB) arrested several people in November 1998 for selling lists of more than 15 million voters and personal data of up to 40 million individuals in violation of the Act.[633]

Under the martial law-era Telecommunications Surveillance Act, permission for telephone tapping and other similar interferences with privacy of communications must be granted according to law. According to the Taiwan Association for Human Rights, "prosecutors appeared to have abused their eavesdropping power by authorizing law enforcement units to monitor more than 16,000 telephone calls in less than a year. Such behavior has constituted a serious infringement of people's privacy."[634] On July 26, 1997, the Independence Morning Post accused intelligence director Yin Tsung-wen of ordering the phone-tapping of National Assembly deputies who opposed a proposal to modify the Constitution to eliminate the provincial government. The report said Yin passed on the phone-tapping order to a number of police and other intelligence agencies.[635] Article 315 of Taiwan's Criminal Code states that a person who, without reason, opens or conceals a sealed letter or other sealed document belonging to another will be punished under the law. The TSA was amended in June 1999 to impose stricter guidelines on when and how wiretaps can be used.

Responding to public concern following repeated incidents of the filming and selling of videotapes of couples making love in motels, the Taiwanese Ministry of Justice decided to revise the Criminal Code to impose stiffer penalties on those convicted of eavesdropping or making secret videos. A person found guilty of eavesdropping or making secret films without any business motives would be punished with a prison term of up to three years.[636]

In 1997, the Taiwanese government proposed a new national ID card called the "National Integrated Circuit (IC) Card." The plan called for a smartcard based system with over 100 uses for the card including ID, health insurance, driver's license, taxation and possibly small-value payments. The card would be issued and operated by Rebar Corporation, a private company which would have set up and paid for the system on

633. *Police Arrest Data Thieves*, CHINA NEWS, Nov. 10, 1998.

634. *Taiwan Takes Stick on Human Rights*, CHINA NEWS, Dec. 8, 1997.

635. INDEPENDENCE MORNING POST, July 26, 1997.

636. *Motel Sex Tapes Prompt Revised Law*, CHINA NEWS, Feb. 27, 1998.

its own, but would have kept any profits from its creation. The entire system was estimated to cost NTD 10 billion (USD 357 million). There were hearings to evaluate privacy concerns after protests about the plan arose.[637] Rebar withdrew from the project in November 1998 over costs and amid public protests. The government has now considered creating its own paper-based card, and may later transfer it to a private company for operation.[638] It is also now considering a smartcard-based system just for health information.[639]

KINGDOM OF THAILAND

Article 37 of the 1997 Constitution protects the privacy of communications.[640] The National Information Technology Committee (NITC) approved plans in February 1998 for a series of information technology (IT) laws. Six sub-committees under the National Electronics and Computer Technology Centre (Nectec) are currently drafting laws on E-Commerce Law, EDI Law, Privacy Data Protection Law, Computer Crime Law, Electronics Digital Signature Law, Electronics Fund Transfer Law and Universal Access Law. The first three, the electronic commerce law, a digital signature law and the electronic fund transfer law are expected to be completed in 1999 and submitted to the Parliament.[641] The second group of laws is expected to be complete in 2000. A proposed Internet Promotion Act, put forward by the Internet Society of Thailand in late 1997 that included censorship provisions, generated intense opposition.

The Official Information Act was approved in 1997.[642] The Act sets a code of information practices on personal information system run by state agencies. The agency must ensure that the system is relevant to and necessary for achieving the objectives of operating the State agency, make efforts to collect information directly from the person who is the subject, public material about its use in the Government Gazette, provide for an appropriate security system; notify such person if information is collected about them from a third party, not disclose personal information in its control to other State agencies or other persons without prior

637. Terho Uimonen, *When Smart Cards Get Too Smart*, THE INDUSTRY STANDARD, Sept. 7, 1998.

638. *New Format of National ID Expected in 2001; IC-based Citizen Card Put Off*, CHINA TIMES, July 9, 1999.

639. Chuang et al, To Trade or Not to Trade: Thoughts on the Falied Smart Card Based National ID Card Initiative in Taiwan, May 1999.

640. Constitution of the Kingdom of Thailand (1997), *available at* <http://www.parliament.go.th/library/con16.htm>.

641. Electronic Commerce Laws Expected In Thailand Next Year, THE NATION, May 11, 1999.

642. Official Information Act, B.E. 2540 (1997) <http://www.krisdika.go.th/law/text/lawpub/ e02092540/text.htm>.

or immediate consent given in writing by the person except in limited circumstances, and provide rights of access, correction and deletion. A high level Official Information Board oversees the Act.

Phone tapping is a criminal offense under the 1934 Telegraph and Telephone Act.[643] In 1996, Prime Minister Banharn introduced a bill that would give the Supreme Commander and the three armed forces chiefs the power to approve wire-tapping for national security reasons. It drew strong opposition from the chairman of the House justice and human rights committee, Witthaya Kaewparadai, who described the proposal as "irrational". The Bangkok Post described it as an "unsavory move."[644] Illegal wiretapping is common in Thailand. In April 1997, tapes and transcripts from wiretaps of Sanan Kachornprasart, the opposition party Democrat secretary-general, were found in the compound of Government House.[645] The Armed Forces Security Centre was accused of being behind the tapping.[646]

In June 1998, the Royal Thai Police Department asked Thai Internet service providers to adopt Caller-ID in order to keep a record of the telephone numbers and login information of people accessing the network. Under the proposal, ISPs will be asked to record this information on their servers, and allow the police to access this information during investigations of Internet-related crime.[647]

In 1997, Thailand began issuing a new national ID card with a magnetic strip. The computer system will be linked with other government departments including the Revenue Department, the Ministry of Foreign Affairs, the Ministry of Defense and the Office of the Narcotics Control Board. The government also plans to link the system with other governments to allow holders to travel in Asian countries without the need for a passport, using only the new card. Bank customers carrying the new ID card can use it as an ATM card as well.[648] In 1995, Control Data Systems was awarded a $11.5 million contract by the Bangkok Metropolitan Administration (BMA) project to install the Computerized National Census and Services Project. The system includes names, addresses, national ID card numbers, and census information such as birth and death

643. Telegraph and Telephone Act, B.E. 2476 <http://www.krisdika.go.th/law/text/lawpub/ei004/text.htm>.

644. *Thailand: Editorial-Democracy in Danger if Spying Sanctioned*, BANGKOK POST, July 5, 1996.

645. Yuwadee Tunyasiri, *Thailand: Politics - PM Denies Chuan's Wire-tapping Claim*, BANGKOK POST, Apr. 8, 1997.

646. *Inside Politics Infuriated by Tap Rap, FT Asia Intelligence Wire*, July 3, 1997.

647. Prangtip Daorueng, *Thailand: Critics Fret Over Gov't Access to Internet Records*, INTER PRESS SERVICE, Sept. 23, 1998.

648. *Thailand: Issuing Computerized National Identity Cards*, NEWSBYTES, Sept. 8, 1997.

records and address changes. It will be used for checking individual tax returns and compiling census statistics.[649] It is expected to be complete by next year for elections.

REPUBLIC OF TURKEY

Section Five of the 1982 Turkish Constitution on "Privacy and Protection of Private Life" protects privacy and secrecy of communications.[650] There is a state of emergency in some areas of Turkey and Constitutional rights have been limited.

The Turkish Ministry of Justice is currently working on draft legislation on the Protection of Personal Data. The new proposals follow the Council of Europe's 1981 Convention and the European Union Directive. The new proposals will cover collecting and processing of data by both public and private bodies. However, in this special draft legislation, the tendency is to put in penalties of administrative nature. Criminal penalties will appear under articles 193-196 of the draft Criminal Law. The new proposals would make it a criminal offense to collect and process data unlawfully or without consent with a maximum prison sentence of three years. In the draft law, it is considered a criminal offense to cause the data to be seized by others, to be deteriorated, or to be damaged as a result of failure to take the necessary security measures. A prison sentence of one to four years is contemplated for these offenses. The draft Criminal Law also regulates collecting and processing of ethical characteristics, political, philosophical and religious opinions, races, union relationships, sexual lives and health conditions of individuals as criminal offenses unless permitted by laws. The prison sentence for violating the regulation is one to two years. The draft Criminal Law also considers disclosure and delivery of personal data to unauthorized persons. Furthermore, failure to destroy the data required to be destroyed within a specific time period is a criminal offense with a prison sentence of 6 months to one year. The draft states that the above mentioned criminal offenses are applicable for all systems in which data is held and emphasizes the liability of legal entities. The new proposals discussed within the May 1998 E-Commerce Laws Working Party Report[651] emphasize both the importance of facilitating the collection and processing of personal data and protecting personal data of individuals in the information age.

649. *Control Data Wins Thai Census Project,* NEWSBYTES, Oct. 3, 1995.

650. Constitution Republic of Turkey, *available at* <http://www.mfa.gov.tr/GRUPC/ca/cag11142.htm>.

651. TURKISH REPUBLIC FOREIGN TRADE OFFICE, E-COMMERCE LAWS WORKING PARTY REPORT (May 8, 1998) *available at* <http://kurul.ubak.gov.tr/e-ticaret.html> (providing a summary of the report in Turkish).

Within the Turkish national legislation, protecting personal rights is regulated in the Civil Code. Pursuant to Article 24 of the Civil Code, an individual whose personal rights are violated unjustly may request from the judge protection against the violation. Individuals can bring action on violation of their private rights. However, there is no criminal liability for such violations of personal rights and currently there is no protection of personal data laws (through data protection laws or any other laws) under the current Turkish Criminal Code.

Articles 195-200 of the Turkish Criminal Code on the freedom of communications govern communication through letters, parcels, telegram and telephone. Despite the existing laws and regulations, the right to privacy and private communications seem to be rather problematic in Turkey. According to Civaoglu, a columnist for the Turkish daily Milliyet: "Apart from the right of privacy of individuals being violated in Turkey, it would be correct to say that these rights are practically "raped" in Turkey."[652] According to acting Security Director Kemal Celik, all telephones in Turkey are bugged. The Turkish parliament's telephone bugging committee, set up to investigate allegations of government phone taps, confirmed allegations that the Security Directorate listens in on all telephone communications, including cellular calls, according to a secret 50-page report documenting and confirming the bugging of telephones.[653] According to Celik's report, selective secret bugging of phones in Turkey enabled the Security Directorate to solve 33 assassination attempts since 1995. Numerous other incidents, including bombings and murders, were also solved since indiscriminate and unregulated bugging of phones began in Turkey.

In 1990, a parliamentary commission on human rights was established with the power to monitor the human rights situation in Turkey and abroad. Currently, the commission consists of 25 parliamentarians, three consultants and four secretaries. Since its inception, the commission took up some 20 cases on its own initiative. Most of these cases relate to alleged violations of physical integrity[654] and it is unknown whether the Commission has dealt with any cases of individual privacy.

652. Güneri Civaoglu, *Demokrasi'nin irzi* [Rape of Democracy], MILLIYET, Dec. 1, 1996, *available at* <http://www.milliyet.com.tr/1996/12/01/yazar/civaoglu.html>.

653. *No Privacy on the Phone Lines*, ASIA TIMES, Apr. 16, 1997, at 8.

654. *See* Commission On Human Rights, *Question of the Human Rights of All Persons Subjected to any Form of Detention or Imprisonment: Promotion and protection of the right to freedom of opinion and expression*, Report of the Special Rapporteur, Mr. Abid Hussain, submitted pursuant to Commission on Human Rights resolution 1996/53 Addendum Mission to Turkey at <http://www.unhchr.ch/html/menu4/chrrep/3197a1.htm>, Distr. General E/CN.4/1997/31/Add.1 Feb. 11, 1997.

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

The United Kingdom (UK) does not have a written constitution. In 1998, the Parliament approved the Human Rights Act that will incorporate the European Convention of Human Rights into domestic law, a process that will establish an enforceable right of privacy.[655] The Act will go into force in October 2000.

The Parliament approved the Data Protection Act (1998) in July 1998.[656] The legislation updates the 1984 Data Protection Act in accordance with the requirements of the European Union's Data Protection Directive.[657] The Act covers records held by government agencies and private entities. It provides for limits on the use of personal information, access to records and requires that entities that maintain records register with the Data Protection Commissioner.

The Office of the Data Protection Commissioner is an independent agency that enforces the Act.[658] Under the previous Act, a total of 225,000 organizations and businesses registered,[659] although this figure is believed to fall well short of the total number of entities that qualify to register. The Commission also received over 4,000 complaints in 1997-1998 and issued Guidance notes on homeworkers, financial service intermediaries and debt tracing.

There are also a number of other laws containing privacy components, most notably those governing medical records[660] and consumer credit information.[661] Other laws with privacy components include the Rehabilitation of Offenders Act, 1974, the Telecommunications Act 1984, the Police Act 1997, the Broadcasting Act 1996, Part VI and the Protection from Harassment Act 1997. Some of these Acts are amended and may be repealed in part by the 1998 Data Protection Act. The Police and Criminal Evidence Act (1984) allows police to enter and search homes without a warrant following an arrest for any offense. And while police may not demand identification before arrest, they have the right to stop and search any person on the street on grounds of suspicion. Following arrest, a body sample will be taken for inclusion in the national DNA

655. Human Rights Bill, CM 3782, Oct. 1997 <http://www.official-documents.co.uk/document/hoffice/rights/rights.htm>.

656. Data Protection Act 1998 [c. 29] <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>.

657. Data Protection Act 1984 c. 35 <http://www.hmso.gov.uk/acts/acts1984/1984035.htm>.

658. Data Protection Registrar, *Homepage* (visited Jan. 2, 2000) <http://www.open.gov.uk/dpr/dprhome.htm>.

659. ANNUAL REPORT OF THE DATA PROTECTION REGISTRAR (July 1998).

660. Access to Medical Reports Act of 1988 and the Access to Health Records Act of 1990.

661. Consumer Credit Act of 1974.

database.[662]

The privacy picture in the UK is mixed.[663] There is, at some levels, a strong public recognition and defense of privacy. Proposals to establish a national identity card, for example, have routinely failed. On the other hand, crime and public order laws passed in recent years placed substantial limitations on numerous rights, including freedom of assembly, privacy, freedom of movement, right of silence and freedom of speech.[664] There has been a proliferation of Closed Circuit Television (CCTV) cameras in hundreds of towns and cities in Britain. The camera networks can be operated by police, local authorities or private companies, and are partly funded by a Home Office grant. Their original purpose was crime prevention and detection, though in recent years the cameras became important tools for city center management and the control of "anti social behavior." Between 150 million and 300 million pounds a year is spent expanding the web of 200,000 cameras covering public spaces in Britain,[665] but despite the ubiquity of the technology, successive governments were reluctant to pass specific laws governing their use. Their use came under greater criticism recently and recent research by the Scottish Centre for Criminology found that the cameras did not reduce crime, nor improved public perception of crime problems.[666]

The Interception of Communications Act of 1985 limits surveillance of telecommunications. Police can obtain telephone taps by obtaining a warrant signed by the Home Secretary. In 1998, 1,913 orders for intercepting telephone communications were approved, an increase of 25 percent from the previous year and nearly 400 percent over ten years. Telephone taps for national security purposes are authorized by the Foreign Minister. The law was amended in 1997 to allow bugging of homes with only the permission of a chief constable or police commissioner. A Special Commissioner will review these activities.[667] There were also 118 orders for interception of mail communications. The National Criminal Intelligence Service published a series of codes of practice on interception, surveillance, use of informants, undercover operations and use of intelligence materials in May 1999 to ensure adherence with the Euro-

662. Criminal Justice and Public Order Act of 1994, *available at* <http://www.hmso.gov.uk/acts/summary/01994033.htm>.

663. *See* SIMON DAVIES, BIG BROTHER (Pan Books, 1996), *available at* Privacy International, *United Kingdom* <http://www.privacy.org/pi/countries/uk/>.

664. *See* Criminal Justice and Public Order Act of 1994.

665. House of Lords, Science and Technology Comm., Inquiry: "Use of Digital Images as Evidence," Feb. 3, 1998, § 4.3.

666. The Scottish Centre for Criminology, *Crime Prevention Publications* (visited Jan. 2, 2000) <http://www.scotcrim.u-net.com/researchc.htm>.

667. Police Act of 1997 <http://www.hmso.gov.uk/acts/acts1997/1997050.htm>.

pean Convention on Human Rights incorporation into UK law.[668] In June 1999, the Home Office issued a Consultation Paper on wiretapping proposing many changes to the existing law, including requiring Internet Service Providers to facilitate wiretappings, lengthening the times for taps to three months and authorizing the use of roving wiretaps.[669] However, the report was silent on key areas such as judicial review of taps and public oversight.

There is a long history of illegal wiretapping of political opponents, labor unions and others in the UK.[670] In 1985, the European Court of Human Rights ruled that police interception of individuals' communications was a violation of Article 8 of the European Convention on Human Rights.[671] The decision resulted in the adoption of the Interception of Communications Act 1985. Most recently, the European Court of Human Rights ruled in 1997 that police eavesdropping of a policewoman violated Article 8.[672] In the late 1970's, M15, Britain's security service, tapped the phones of many left-leaning activists including the future Secretary of State for Trade and Industry Peter Mandelson, and kept files on Jack Straw, now Home Secretary, and Harriet Harman, former Social Security Secretary, as well as Guardian journalist Victoria Brittain. The High Court issued an injunction against the Mail on Sunday preventing the publication of further revelations. In September 1998, it was revealed that there were secret talks between the Association of Chief Police Officers (ACPO) and representatives for Internet Service Providers (ISPs) with the aim of reaching a "memorandum of understanding" to give the police access to private data held by ISPs.[673]

In late 1997, a report commissioned by the European Parliament and prepared by the UK based research group Omega Foundation, confirmed that Britain was a key player in a vast global signals intelligence operation controlled by the U.S. National Security Agency (NSA).[674] According to the report, the U.S. and its UK partner, GCHQ, "routinely and indiscriminately" intercepted large amounts of sensitive data which had

668. National Criminal Intelligence Center (May 13, 1999), *available at* <http://www.ncis.co.uk/ncis/web/Press%20Releases/codes%20practice.htm>.

669. Secretary of State for the Home Department, *Interception of Communications in the United Kingdom: A Consultation Paper* (June 1999) <http://www.homeoffice.gov.uk/oicd/ioc.htm>.

670. *See, e.g.*, PATRICK FITZGERALD & MARK LEOPOLD, STRANGER ON THE LINE 1987.

671. Malone v. United Kingdom (A/95): (1991) 13 EHRR 448, Apr. 26, 1985.

672. Halford v. United Kingdom (Application No 20605/92), 24 EHRR 523, June 25, 1997.

673. *Police Tighten the Net*, THE GUARDIAN ONLINE (Sept. 17, 1998) <http://online.guardian.co.uk/theweb/905960359-privacy.html>.

674. European Commission, Science and Technology Options Assessment Office ("STOA"), *Assessing the Technologies of Political Control* (Brussels, 1997) <http://www.jya.com/>.

been identified through keyword searching. The eavesdropping was carried out from a number of spy bases in the UK, most notably the Menwith Hill base in the north of England. The report led to some concern in various European States, and on September 14, 1998, the European Parliament, in plenary session in Strasbourg, took the unprecedented step of openly debating the operation. A "compromise resolution" framed in the wake of the debate by the four leading parties called for greater accountability and "protective measures" over such intelligence gathering.[675]

Territories

The dependent territories of the Isle of Man,[676] Isle of Guernsey, and Isle of Jersey each have a data protection act and data protection commission.

UNITED STATES OF AMERICA

There is no explicit right to privacy in the U.S. Constitution. The Supreme Court has ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights. This includes a right to privacy from government surveillance into an area where a person has a "reasonable expectation of privacy"[677] and also in matters relating to marriage, procreation, contraception, family relationships, child rearing and education.[678] However, records held by third parties such as financial records or telephone calling records are generally not protected unless a legislature enacted a specific law. The court also recognized a right of anonymity[679] and the right of political groups to prevent disclosure of their members' names to government agencies.[680]

The U.S. has no comprehensive privacy protection law for the private sector. The Privacy Act of 1974 protects records held by U.S. Government agencies and requires agencies to apply basic fair information practices.[681] Its effectiveness is significantly weakened by administra-

675. Minutes of the plenary sessions, European Parliament, Sept. 14, 1998: 17. Transatlantic relations (ECHELON) B4-0803, 0805, 0806 and 0809/98.

676. Isle of Man Data Protection Register <http://www.odpr.org/>.

677. Katz v. U.S., 386 U.S. 954 (1967), *available at* <http://laws.findlaw.com/US/386/954.html>.

678. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965); Whalen v. Roe, 429 U.S. 589 (1977); Paul v. Davis, 424 U.S. 714 (1976).

679. McIntire v. Ohio Elections Comm., 514 U.S. 334 (1995).

680. NAACP v. Alabama, 357 U.S. 449 (1958), *available at* <http://laws.findlaw.com/US/357/449.html>.

681. Privacy Act of 1974, 5 U.S.C. § 552a (1974), Pub. L. No. 93-579, *available at* <http://www.epic.org/ privacy/laws/privacy_act.html>.

tive interpretations of a provision allowing for disclosure of personal information for a "routine use" compatible with the purpose for which the information was originally collected. Limits on the use of the Social Security Number were also undercut in recent years for a number of purposes.

There is no privacy oversight agency in the U.S. The Office of Management and Budget plays a limited role in setting policy for federal agencies and has not been particularly active or effective. The Federal Trade Commission (FTC) has oversight and enforcement powers for laws protecting consumer credit information and fair trading practices, but has no authority to enforce privacy rights, other than those arising from fraudulent or deceptive trade practices.[682] In the last several years, the FTC has received thousands of complaints but issued opinions in only three cases. It also organized a series of workshops and surveys, which typically show that industry protection of privacy on the Internet is poor, but the FTC said that the industry should have more time to make self-regulation work.

A patchwork of federal laws covers some specific categories of personal information.[683] These include financial records,[684] credit reports,[685] video rentals,[686] cable television,[687] educational records,[688] motor vehicle registrations,[689] and telephone records.[690] However, such activities as the selling of medical records and bank records, monitoring of workers, and video surveillance of individuals are currently not prohibited under federal law. There is also a variety of sectoral legislation on the state level that may give additional protections to citizens of individual states.[691] The tort of privacy was first adopted in 1905 and all but two of the 50 states recognize a civil right of action for invasion of privacy in their laws.

---

682. *See* Federal Trade Commission, *Privacy Initiatives* (visited Jan. 2, 2000) <http://www.ftc.gov/privacy/index.html>.

683. *See* MARC ROTENBERG, THE PRIVACY LAW SOURCEBOOK (EPIC 1999), *available at* <http://www.epic.org/bookstore/>.

684. Right to Financial Privacy Act, Pub. L. No. 95-630.

685. Fair Credit Reporting Act, Pub. L. No. 91-508, amended by Pub. L. No. 104-208 (Sept. 30, 1996), *available at* <http://www.ftc.gov/os/statutes/fcra.htm>.

686. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 1988.

687. Cable Privacy Protection Act of 1984, Pub. L. No. 98-549, (Oct. 30, 1984), *available at* <http://www.epic.org/privacy/cable_tv/ctpa.html>.

688. Family Educational Rights and Privacy Act, Pub. L. No. 93-380, (1974), *available at* <http://www.epic.org/privacy/education/ferpa.html>.

689. Drivers Privacy Protection Act, Pub. L. No. 103-322, 1994. <http://www.epic.org/privacy/laws/drivers_privacy_bill.html>.

690. Telephone Consumer Protection Act, Pub. L. No. 102-243, 1991.

691. Robert Ellis Smith, *Compilation of State and Federal Privacy Laws,* PRIV. J. (1997 ed.) <http://www.epic.org/privacy/consumer/states.html>.

Surveillance of telephone, oral and electronic communications for criminal investigations is governed by the Omnibus Safe Streets and Crime Control Act of 1968 and the Electronic Communications Privacy Act of 1986.[692] Police are required to obtain a court order based on a number of legal requirements. Surveillance for national security purposes is governed by the Foreign Intelligence Surveillance Act that has less rigorous requirements.[693] The federal wiretap laws were amended by a controversial bill in 1994 that required telephone companies to redesign their equipment to facilitate electronic surveillance.[694]

There were 1,329 orders to intercept for criminal purposes and 796 for national security purposes in 1998.[695] The use of electronic surveillance has more than tripled in the last ten years. The intelligence agencies also pushed for more authority and funding to conduct surveillance of Internet communications, arguing that this is necessary to protect the nation's infrastructure from "information warfare." In July 1999, it was revealed that the FBI was pressing for the creation of a Federal Intrusion Detection Network (FIDNet) that would permit widespread monitoring of Internet traffic.[696]

There has been significant debate in the United States in recent years about the development of privacy laws covering the private sector. Over 100 bills on privacy protection were introduced in the previous Congress, including laws on genetic and medical records, Internet privacy, children's privacy and other issues. Only a provision on collecting personal information from children on the Internet was approved.[697] The current position of the White House and private sector is that self-regulation is sufficient and that no new laws should be enacted except for a limited measure on medical information. There are currently efforts in Congress to improve financial privacy by prohibiting banks from selling personal information of customers without permission, but the proposal is strongly opposed by the banking industry. There is substantial activity in the states, particularly California, New York, Massachusetts, Minnesota, and Hawaii where comprehensive privacy bills for the private sector are now under consideration.

---

692. 18 U.S.C. § 2500, *available at* <http://www.law.cornell.edu:80/uscode/18/ch119.html>.

693. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801.

694. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-411. <http://www.epic.org/privacy/wiretap/calea/calea_law.html>.

695. *See* Electronic Privacy Information Center, *Wiretapping* (visited Jan. 2, 2000) <http://www.epic.org/privacy/wiretap/>.

696. John Markoff, *U.S. Drawing Plan That Will Monitor Computer System*, NY TIMES, July 28, 1999.

697. *See* EPIC Online Guide to 105th Congress Privacy and Cyber-Liberties Bills, *available at* <http://www.epic.org/privacy/bill-track.html>.

There were a series of high-profile revelations about privacy invasions in the past year. The Michigan Attorney General sued several banks for revealing that they were selling information about their customers to marketers. Other banks across the country subsequently admitted that there were also selling customer records, but many continue to do so. Intel and Microsoft developed products to secretly track the activities of Internet users and in the Microsoft case, TRUSTe, an industry-sponsored self-regulation watchdog ruled that the Microsoft practices did not violate their privacy seal program.[698] Thousands of pharmacies were discovered to be selling their patients' records to Elenysis, a company that then sold the records to pharmaceutical companies.[699] The Federal Depository Insurance Company proposed new "Know Your Customer" rules that would have required banks to track their customers' activities and inform the federal government of "unusual" transactions. The rules were withdrawn after over 250,000 people wrote the government, opposing the rules.

698. *See* Big Brother Inside, *Protect Your PC's Privacy* (visited Jan. 2, 2000) <http://www.bigbrotherinside.org>.

699. Robert O'Harrow, Jr., *Prescription Sales, Privacy Fears; CVS, Giant Share Customer Records With Drug Marketing Firm*, THE WASH. POST, Feb. 15, 1998.