Republic of (South) Korea

Constitutional Privacy Framework

The Constitution of the Republic of Korea provides for the protection of secrecy and liberty of private life.[1] Article 16 states, "All citizens are free from intrusion into their place of residence. In case of search or seizure in a residence, a warrant issued by a judge upon request of a prosecutor has to be presented."[2] Article 17 states, "the privacy of no citizen shall be infringed."[3] Article 18 states, "The privacy of correspondence of no citizen shall be infringed."[4] In general, the government respects the integrity of the home and family.[5]

The protection of human rights in South Korea, including the right to a fair trial before an independent and impartial tribunal, is still in its infancy. It was only in November 2001 that the National Human Rights Commission of Korea was created to police the actions of the state in this context.[6] The Commission has been beset with problems in fulfilling its role due to a lack of autonomy and political independence, as well as other structural problems.[7]

Data Protection Framework

South Korea has adopted a data protection regime similar to the United States and Japan, with one act covering the public sector and sectoral legislation for the private sector.[8] The statute in the former category is the 1994 Act on the Protection of

---

[1] Constitution of The Republic of Korea, Chapter II (Rights and Duties of Citizens), § 16; Section 9 further stating that "it shall be the duty of the State to confirm and guarantee the fundamental and inviolable human rights of individuals."

[2] However, Korean courts are willing to "rubber stamp" practically all prosecutors' requests. "Courts are issuing warrants for search and seizure almost automatically upon request from Public Prosecutors and . . . the issue of search and seizure warrants is being abused." "Courts' Issue of Warrants for Search and Seizure at the Rate of 99.3%," Edaily, October 14, 2004 <http://news.naver.com/news/read.php?mode=LSD&office_id=018&article_id=0000212219&section_id=102&menu_id=102>.

[3] Korean Constitution, *supra* at § 17.

[4] *Id.* at § 18.

[5] US State Department Human Rights Report 2006 - South Korea, available at <http://www.state.gov/g/drl/rls/hrrpt/2006/78778.htm>.

[6] <http://www.humanrights.go.kr/eng/index.jsp>.

[7] Asia Pacific Human Rights Network, "National Human Rights Commission of Korea: Miles To Go," September 2004.

[8] C. Chung and I. Shin, "On-Line Data Protection and Cyberlaws in Korea" 27 Korean J. of Int'l and Comp. L. 21, 24 (1999).

Personal Information Maintained by Public Agencies,[9] which is generally applicable to the automated processing of personal data in the public sector, but not to manual records.[10] This statute has a provision recommending that private entities respect the data protection principles in the statute, but it has no appropriate administrative or enforcement mechanism to that effect.[11]

The Act on the Protection of Personal Information Maintained by Public Agencies imposes an obligation on public agencies to maintain records of personal information databases and to report these databases to the Ministry of Government Administration and Home Affairs (MOGAHA), the ministry responsible for the Act.[12] The MOGAHA publishes lists of these databases in an official journal, which is publicly available.[13] In addition, the MOGAHA can request relevant information from the data holding entities and issue opinions on their data processing practices.[14] A data subject has a right of access to, and correction of, personal information held by public agencies.[15] The Act establishes a Data Protection Review Commission, under the Premier's Office, headed by the Vice-Minister of the MOGAHA, to recommend and review proposals on improving data protection policy.[16]

The Act has been criticized for its ineffectiveness.[17] The MOGAHA has placed little emphasis on rigorous application of the legislation and reportedly has little will to uphold privacy versus administrative efficiency. In January 1999, the Act was amended to give even more power to the MOGAHA, streamline the procedure for access to personal information by data subjects, and limit exemptions to disclosure. However, there remains no independent oversight of government application of the Act.

Acts governing the collection, use and disclosure of personal information in the private sector include the Protection of Communications Secrets Act (1993) (*a.k.a.,* "Anti-Wiretap Law");[18] the Telecommunications Business Act (1991);[19] the Medical

---

[9] Act No. 4734, last amended by Act No. 8871, February 29, 2008

[10] *Id.* at §§ 1, 2(3).

[11] Chung and I. Shin, *supra* at 31.

[12] Act No. 4734 § 6.

[13] *Id.* at §§ 7-8.

[14] *Id.* at §§ 18-19.

[15] *Id.* at §§ 12, 16.

[16] Act No. 4734 § 20.

[17] Chung and I. Shin, *supra* at. 21, 33.

[18] Act No. 4650, last amended by Act No. 8867, February 29, 2008. Article 3 (Protection of Secrets of Communication and Conversation), paragraph 1 of this Act provides that "No person shall censor any mail, wiretap any telecommunications, provide the communication confirmation data, record or listen to conversations between others that are not made public, without recourse to this Act, the Criminal Procedure Act or the Military Court Act."

[19] Act No. 4394, last amended by Act No. 8867, February 29, 2008.

Service Act (1973);[20] the Real Name Financial Transactions and Secrecy Act (1997);[21] the Use and Protection of Credit Information Act (1995);[22] the Framework Act on Electronic Commerce (1999);[23] and the Digital Signatures Act (1999).[24]

The Act on Promotion of Information and Communications Network Utilization and Data Protection (the Act),[25] modeled after the German Online Service Data Protection Act of 1997,[26] came into effect in 2000. The Act adopts common "fair information principles"[27] and rules for the collection, use, and disclosure of personal data by "providers of information and communications services," such as common carriers, Internet service providers and other intermediaries, particularly content providers. The Act also covers specific off-line service providers such as travel agencies, airlines, hotels, and educational institutes.

The Act requires that "data users" seek consent from "data subjects" for the collection, use, and disclosure of data to a third party "beyond the notification as prescribed in the Act or the limit specified in a standardized contract for the utilization of the information and communication services."[28] Data users should collect as little personal data as is necessary[29] and are prohibited from collecting sensitive personal information, including ideology, faith and medical data without explicit consent of the data subject.[30] However, consent is not required when it is necessary to give effect to a contract, adjust fees, or when the personal information is provided after having been rendered unidentifiable to the individual, such as for the compilation of statistics, academic research or market surveys.[31] The Act allows the data subject to withdraw consent for the collection, use and disclosure of data at any time and requires the data user to comply, unless the preservation of such personal information is required by another Act. Further, every data subject has a right to access and correct his or her personal information.[32]

---

[20] Act No. 2533, last amended by Act No. 8852, February 29, 2008.

[21] Act No. 5493, last amended by Act No. 8863, February 29, 2008.

[22] Act No. 4866, last amended by Act No. 8863, February 29, 2008.

[23] Act No. 5834, last amended by Act No. 8979, March 21, 2008.

[24] Act No. 5792, last amended by Act No. 8852, February 29, 2008.

[25] Act No. 5835, last amended by Act No. 9119, June 13, 2008.

[26] Gesetz zur Regelung der Rahmenbedingungen für Informations und Kommunikationsdienste: IuKDG, Ch. 2.

[27] The fair information principles of the Act are derived from the eight principles found in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 23, 1980, OECD, available at <http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html>.

[28] Act No. 5835, § 16 (2).

[29] *Id.* at § 16(1).

[30] *Id.* at § 4.

[31] *Id.* at 3. But *see* L. Sweeney, The Identifiability of Data, (forthcoming), discussing the ease of re-identifying ostensibly de-identified data.

[32] Act No. 5835, § 18(2).

South Korea

A data user must obtain consent from an appropriate legal guardian when collecting, using or disclosing personal information from children under 14, and may request appropriate minimum information of the guardian in order to effect that consent. A legal guardian has a right to access and correct the child's personal information. Upon receiving a guardian's request for correction, the data user must cease to use or disclose erroneous information until they have made the correction.[33]

The Act prohibits one from sending unsolicited commercial e-mail contrary to an addressee's explicit refusal of such e-mail.[34] All unsolicited commercial e-mail must contain the word "Advertisement" in the subject line of every message and must contain opt-out instructions and contact information for the sender.[35] Additionally, several direct marketers established the Association for the Improvement of the E-Mail Environment in early 2002 to help cope with the increasing number of unsolicited commercial e-mails problem in Korea.[36]

The government imposes criminal and administrative penalties for breaches of data protection principles. The processing of personal information without consent or beyond the scope of the purpose for which the collection was made, attracts either penalties of up to one year in prison or a fine of KRW 10 million (USD 9,856).[37] Data subjects may file damage claims for breaches of the Act with the Personal Information Mediation Committee or with a court. The onus is on the data user to prove either good faith intentions to comply, or non-negligence.[38]

There is significant overlap between the aforementioned act, the Framework Act on Electronic Commerce (FAEC) and the Digital Signatures Act (DSA). For this reason and others, some legal commentators have called for comprehensive reform.[39] The FAEC requires data users to give data subjects sufficient information regarding the purpose of collection.[40] Under the FAEC, the data user must obtain explicit consent

---

[33] *Id.* at § 18(4).

[34] *Id.* at § 19(3).

[35] *Id* at 5. Due to the volume of unsolicited commercial e-mails, the government is contemplating an amendment that would curtail distribution and punish senders. Further, the amendment proposes the addition of "Adult" or "Consent" in the subject line of each and every unsolicited commercial e-mail and punitive measures for their senders who use false contact information or hinder technologically their tracing or deletion.

[36] Personal Information Dispute Mediation Committee of the Korea Information Security Agency, "Personal Data Protection in Korea," August 2002, at 12 (available at <http://www.cyberprivacy.or.kr/inter.htm>).

[37] Act No. 5835 at § 30. Additionally, § 32 imposes lesser administrative penalties of KRW 5 million for violations of other data protection principles.

[38] Personal Information Dispute Mediation Committee of the Korea Information Security Agency, "Personal Data Protection in Korea," August 2002 at 4.

[39] *See* C. Chung and I. Shin, *supra* at 42-43, citing the lack of an appropriate oversight authority as the major weakness of the Korean data protection regime; I. Kim, "A Study on the Data Protection Act" 26 Public Law 2 (June 1998) (in Korean); I. Lee, "Trends in the Korean Data Protection Legislation" Road to the Information Society (November 1999) (in Korean).

[40] Act No. 5834, §§ 30-31.

from the data subject before collecting personal information, and is prohibited from using the personal information collected for inconsistent purposes.[41] Additional requirements of the FAEC include appropriate security,[42] and a right of access, correction or deletion.[43] The DSA prohibits an individual from fraudulently using another person's private key or issuing a key.[44] It also has data protection provisions[45] similar to the Electronic Commerce Act and penalties equal to the Act on Promotion of Information and Communications Network Utilization and Data Protection.

Human rights groups in Korea had insisted on enacting the Basic Act on the Protection of Personal Information as a comprehensive privacy law, and establishing independent privacy supervisory authority for a long time from late nineties. Three different acts on the protection of personal information which include establishing independent privacy supervisory authority were proposed in the 17th National Assembly. The Democratic Labor Party proposed the act that was drafted in cooperation with human rights groups in November 2004. The act drafted by government and the ruling party, Uri Party, was proposed in July 2005, and the act drafted by Grand National Party was proposed in October 2005. In November 2006, members of the Futures Forum for Korea in the Korean National Assembly attempted to arrive at an agreement on a proposal for a comprehensive privacy law.[46] However, these acts were not passed even in the Standing Committee in National Assembly. Finally, the acts were repealed automatically when the 17th National Assembly was closed in may 2008.

After that, there was a public hearing on June 27, 2008, on the Basic Act on the Protection of Personal Information drafted by the Ministry of Public Administration and Security (MOPAS), to which the name of MOGAHA was changed in the new government in 2008, to propose in the 18th National Assembly. However MOPAS plans not to establish an independent privacy supervisory authority, but take charge of supervisory role by itself. Human rights groups criticize that MOPAS itself is main object to be supervised as a ministry directly managing huge personal information such as resident registration databases, and that it's illogical to supervise itself.

---

41 *Id.* at § 13(2).
42 *Id.* at § 13(3).
43 *Id.* at § 13(4).
44 Act No. 5792, §§ 19-23.
45 *Id.* at § 24.
46 Email from Jongin Chang, *supra*.

South Korea

The protection of personal information has become a critical issue in Korea, which now has the largest population of broadband Internet users in the world.[47] In May 2005, the People's Solidarity for Participatory Democracy reported, based on a survey of 15 Internet portals, that most Korean Internet portals still require customers to provide a large amount of personal information, even their resident registration numbers (a 13-digit system whereby an individual's age, gender, place of birth and other private data, are stored and tracked by the government), without clarifying how the personal data will be used and without obtaining their individual consent.[48]

The MIC introduced 'i-PIN' (Internet Personal Identification Number) to replace the use of the RRN (the Resident Registration Number) online. Unlike the RRN, the 'i-PIN' does not include personal information: the date of birth, birthplace, or sex. It is easily replaceable if individuals want to acquire a new number. However, few Internet websites and companies have accepted this alternative to date because of the added cost and burden of changing their systems' databases.[49]

In 2007, MOGAHA launched a month-long online that Internet users to find and delete their resident registration numbers, Korea's version of social security numbers, if they are found circulating on the Web. Search programs operated by the Korea Information Service, the National Information and Credit Evaluation, and the Seoul Credit Rating and Information compiled lists of Web sites using an individual's identification number.[50] Last year, law enforcement authorities found the resident registration numbers of more than 1.2 million people intercepted by hackers who sought to create fake accounts for online games.[51]

In December 2001, the MIC established the Personal Information Dispute Mediation Committee, as an alternative to civil litigation, to facilitate a prompt, convenient and appropriate settlement of data protection disputes.[52] Members of the Committee, which includes lawyers, IT engineers, professors, consumer advocates and industry representatives, are appointed for three-year terms. Both data subjects or data users can initiate mediation, free of charge. The Committee first engages in informal fact-finding and makes non-binding recommendations for settlement. If parties cannot

---

47 Leo Lewis, "Chat room bullies face end to their internet anonymity," Times Online, June 29, 2007, available at <http://www.timesonline.co.uk/tol/news/world/asia/article2005592.ece>.

48 "Portals Criticized over Privacy Standards," Korea Herald, May 31, 2005, available at <http://www.koreaherald.co.kr/archives/result_contents.asp?id=200505310041&query=internet>.

49 Email from Jongin Chang, University of Seoul, Korea, to Allison Knight, Research Director, Electronic Privacy Information Center, August 1, 2007 (on file with EPIC).

50 Kim Tong-hyung, "Internet users can clean up personal information," Korea Times, March 12, 2007, available at <http://www.asiamedia.ucla.edu/article.asp?parentid=65654>.

51 *Id.*

52 Personal Information Dispute Mediation Committee of the Korea Information Security Agency, "Personal Data Protection in Korea," August 2002, at 8-9.

reach a settlement, they can begin formal mediation. If parties fail to reach a mediated settlement, they can pursue matters in a competent civil court. They can also bypass the Committee process altogether and go directly to court.[53]

The Korea Association of Information and Telecommunication (KAIT) has instituted a privacy trust mark for websites and other online businesses that satisfy appropriate data processing standards. Regarding personal information, qualified trust mark applicants provide notice and purpose of collection, use and disclosure. In addition, the applicants provide special treatment for children under 14, and offer remedies for data subjects.

In June 2004, the Korea Information Security Agency (KISA) found that many Korean Internet websites pose a threat to personal information privacy. The agency reported that thousands of websites that collect personal information about subscribers, including resident registration numbers, remain vulnerable to security breaches.[54] To address this problem, KISA planned to conduct more investigations, levy administrative penalties on offending websites, and solicit feedback on privacy problems from users.

The Auction site, which was one of the biggest on-line market in Korea, was hacked causing personal information of more than ten million people to be exposed in February 2008. Soon after, the fact that one of the major ISPs, Hanaro-Telecom, intentionally abused its more than six million clients' personal information (the number of leaked records were more than eighty five millions) became known in April 2008. These accidents were a great shock to the public. The victims of these accidents raised class suits against the Auction and Hanaro-Telecom.

Human rights groups claimed that the reason why leakage of personal information had occurred on a large-scale in these accidents was because large-scale personal information was collected unnecessarily by the companies in one hand, and public authority did not perform its jobs in monitoring and overseeing these companies' behaviors in collecting and using personal information in the other hand, and urged the government to enact the Basic Act on the Protection of Personal Information and establish an independent privacy supervisory authority.[55]

Among the personal information leaked in these accidents, the exposure of the Resident Registration Numbers poses tremendous problems. The Korean government allowed private entities to collect such sensitive information without proper

---

53 *Id.*

54 "Agency Says the Web is Quite a Leaky Place," JoongAng Daily, June 15, 2004

55 Korean Progressive Network Jinbonet, "Four Comments on the Leakage of Personal Information", April 24, 2008, available at <http://act.jinbo.net/webbs/view.php?board=policy&id=1396&page=9>

regulations, and abandoned its responsibility by not providing effective corrective measures even though massive numbers of Resident Registration Numbers have been traded and used for fraudulent IDs. To minimize the damage of victims, human rights groups requested the MOPAS to reassign their Resident Registration Numbers in May 2008. However, MOPAS denied that request saying it is impossible.

Beginning June 2007, Internet users are required to provide their real names and their Resident Registration Numbers before posting comments or uploading video or audio clips on bulletin boards.[56] The proposed law is a response to the increasing number of libelous and fraudulent accusations made by Koreans about public figures, as well as cyber-bullying between schoolchildren. Researchers have suggested a link between the online comments and suicide levels, as well as increased physical confrontations. The Department for Education and Skills would issue guidelines to help parents and children understand the proper steps to take if they find themselves victims of cyber-bullying. At least 34 sites with more than 300,000 users are affected by the law.[57]

Since the MIC expressed the necessity of introducing the 'Internet real name policy', which obligates every user of major Internet portal sites and government sites to confirming his/her real identity, in the early 2003, human rights groups had been against the policy. They criticized that the policy would violate freedom of expression and right to anonymity of all users. In addition, they worried about identity theft in the process of authentication using name and Resident Registration Number.

As the public opinion criticizing beef import negotiation between Korea and U.S. spread fast over the Internet in 2008, the Korean government and the governing party, GNP, planned to expand the sites which were forced to adopt Internet real name policy up to over 200 sites including Google.

Meanwhile, the revision of Public Election Act was passed in the National Assembly in May 2004, which requires Internet newspaper sites to adopt technical management of confirming user's real identity in their bulletin boards or chat rooms during the election period. Human rights groups and Internet newspapers criticized that 'Internet real name policy during the election period' would restrict political participation of citizens, and announced disobedience to the policy. The National Human Rights Commission(NHRC) expressed objection to 'Internet real name policy' in the "Opinions to the National Assembly about Politics related Law and its revision" in

---

[56] Leo Lewis, *supra*.
[57] *Id.*

February 2004.[58] In the opinion, the NHRC pointed out that Internet real name policy was clearly censorship presuming that all people who would post in the bulletin board during the election period would circulate false information and/or libel, and violated freedom of expression under the article 19 of the World Human Rights Declaration and the article 21 of the Constitution by restricting freedom of expression and right to form opinions based on anonymity in the Internet, and would possibly violate right to control his/her own information under the article 17 of the Constitution in that individual information would be subject to misuse for the purpose other than original purpose presented when information was collected, by allowing the minister of MOGAHA and credit information companies to confirm users' identity using name and Resident Registration Number when requested by Internet newspapers.

Since 'Internet real name policy during election period' was first enforced in May 31st local elections in 2006, some of progressive Internet newspapers practiced disobedience. An Internet newspaper, 'People's Media Chamsesang', which was imposed a fine of KRW 10 million at the price of disobedience during the presidential election in 2007, raised a unconstitutionality suit on April 4, 2008.[59] In addition, A netizen raised a unconstitutionality suit claiming that Internet real name policy violated basic rights under the Constitution at the last date of enforcement of Internet real name policy during general election, on April 8, 2008.

Wiretapping and Surveillance

State security services have a history of conducting surveillance of political dissidents. The Korean Government designed the Protection of Communications Secrets Act of 1993 and the reform of the NIS to curb government surveillance of civilians.

The Protection of Communications Secrets Act lays out broad conditions under which the monitoring of telephone calls, mail, and other forms of communication is legal.[60] This Act requires government officials to secure a judge's permission before placing wiretaps, or, in the event of an emergency, soon after placing them. The Act also provides jail terms for persons who violate this law. Some human rights groups argue that a considerable amount of illegal wiretapping, shadowing, and surveillance photography still occurs, and they assert that the lack of an independent body to

---

[58] National Human Rights Commission, "Opinions to the National Assembly about Politics related Law and its revision", Febrary 17, 2004, available at <http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=554728&page=1>

[59] "People's Media Chamsesang, 'Internet Real Name Policy is Unconstitutional'", People's Media Chamsesang , April 4, 2008, <http://www.newscham.net/news/view.php?board=news&nid=47126>

[60] Act No. 4650.

investigate whether police have employed illegal wiretaps hinders the effectiveness of the Anti-Wiretap Law.[61]

In June 2007, revisions to the Protection of Communications Secrets Act passed the National Assembly's Legal and Judiciary Committee. The revisions would require mobile phone service providers, credit card firms and mass transit operators to store clients' records for up to a year and provide the information at the request of state investigators. This means a citizen's cellular phone calls, e-mails, financial transactions and even where he or she goes on buses and subways over the past year must be kept and disclosed upon a warrant request.[62]

The Protection of Communications Secrets Act has articles on retainment of communication log data such as phone records, location log data, Internet log data, etc., but has not penal clauses. The revision forces communication service providers to retain communication log data by imposing fines not exceeding KRW 30 million on who don't retain communication log data. Moreover, the revision requires mobile phone service providers to redesign their networks to permit wiretapping.

Human rights groups criticized that the amendment would severely jeopardizes people's right to privacy and freedom of expression by regarding all people as potential criminals and making people under surveillance. Considering that users of major Internet portal sites and government sites are obligated to confirm his/her real identity in Korea, retaining communication log data enables investigators to monitor one's every action, which has critical impact on citizen's privacy.[63]

The NHRC expressed its opinion on the revision of the Protection of Communications Secrets Act under National Assembly on January 16, 2008.[64] In the written opinion, the NHRC said that the revision could threaten citizen's privacy by forming recognition that interception could be routinized, and had the possibility to be abused by communication service providers. And the NHRC criticized that forcing service providers to retain communication log data for some period would be against the principles of the protection of personal information and violate the intent of the act. At the end of the written opinion, the NHRC emphasized that the revision could cause the leak or misuse of personal information lasting for a long period of

---

61 US State Department Human Rights Report 2004 – South Korea, available at <http://www.state.gov/g/drl/rls/hrrpt/2004/41647.htm>.

62 "New Bill Turns Korea Into Orwellian State," The Korea Times, June 25, 2007, available at <http://www.koreatimes.co.kr/www/news/opinon/opi_view.asp?newsIdx=5375&categoryCode=202>.

63 6 Human Rights Groups, "We censure the revision of The Protection of Communications Secrets Act that would make people under surveillance", June 22, 2007, available at <http://act.jinbo.net/webbs/view.php?board=policy&id=1280&page=1>

64 National Human Rights Commission, "Opinion to the chairman of the National Assembly on the Revision of the Protection of Communications Secrets Act ", January 16, 2008, available at <http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=555406&page=1>

time considering that 'the Basic Act on the Protection of Personal Information' and independent privacy supervisory authority didn't exist.

The revision to the Protection of Communications Secrets Act did not pass in the National Assembly until the 17th National Assembly was closed in may 2008, and were repealed automatically. However, the revision is expected to be proposed again in the 18th National Assembly.

The Anti-Wiretap Law sets out "broad conditions under which the government may monitor telephone calls, mail, and other forms of communication, for up to two months in criminal investigations and four months in national security cases."[65] Some human rights groups raised concerns about possible government wiretapping abuse. The Ministry of Information and Communication said that between January and June of 2006, the government conducted 528 cases of wiretapping, down 11 percent from the 550 cases during the same time period in 2005. Telecommunications companies also reported providing more than 35 percent fewer phone records to law enforcement agencies when compared with last year.[66]

South Koreans have long had to live with widespread surveillance and wiretapping abuses by intelligence and police officials under successive regimes. In October 1998, President Kim Dae-Jung ordered a full-scale probe into illegal wiretapping. Rep. Hyong-Oh Kim of the opposition GNP stated that he believed that over 10,000 taps were actually placed in 1998.[67] The government proposed amendments to the Protection of Communications Secrets Act in November 1999 that would allow victims of illegal wiretapping to sue in court, limit the number of crimes for which wiretapping is allowed, and provide for notice to targets of wiretapping. The government set up a wiretapping complaint center under the MIC in October 1999.[68] The UNHRC heard testimony on Korean wiretapping at its meeting in October 1999.[69]

According to the opposition GNP, public prosecutors, police and many governmental bodies, such as the SPPO, the National Police Agency (NPA), the National Tax Administration (NTA), the Financial Supervisory Service (FSS), the Financial Intelligence Unit (FIU), the Fair Trade Commission (FTC) and the Central Election Management Committee (CEMC), are not only indiscriminately monitoring bank accounts, but there has also been a sharp rise of wiretapping incidents by

---

65 US State Department Human Rights Report 2006 – South Korea, *supra*.

66 *Id.*

67 "Kim Hyong-o Says more than 10,000 May Be Exposed to Gov't Taps," Korea Times, February 13, 1999.

68 "Government to Operate Eavesdropping Complaint Center," Korea Herald, October 30, 1999.

69 United Nations Human Rights Committee, Summary record of the 1,792nd meeting: Republic of Korea. 22/11/99. CCPR/C/SR.1792, (November 22, 1999).

investigating authorities, with a high risks to infringement of human rights.[70] Furthermore "a considerable number of these surveillances have been carried out without proper legal procedures such as obtaining a warrant or the consent of the individual concerned, but simply at the convenience of the investigating authorities."[71]

According to an MIC report, the number of location-tracking services furnished by mobile phone service providers to state investigation agencies in 2004 has significantly increased over those in 2003.[72] Government authorities such as the NPA and the NIS tracked mobile phone users in 16,497 instances just during the first half of 2004.[73] The total number of cases was 20,773 in 2003, a 62.3 percent increase over the 12,184 cases in 2002.[74]

Through material submitted by the Ministry of Finance and Economy (MOFE) and other agencies to the National Assembly, it was also discovered that even in non-emergency cases, which only require the senior prosecutor's consent – rather than a court approval – public prosecutors obtained telecommunications records by breaking the rule in 40 percent of the cases.[75] There were 124,893 cases of disclosures of telecommunications data, an increase of 24.3 percent compared to the same period in 2003.[76]

South Korean courts routinely accept recordings, or transcripts of recordings, as admissible evidence in both civil and criminal proceedings. The Supreme Court ruled in October 2002 that it is not illegal for a party to a phone call to record the phone conversation secretly without the other party's knowledge, although the recording of a phone conversation by a third party without the consent of both parties to the phone call is illegal.[77] In August 2004, the Seoul Central District Court ruled that it was not

---

[70] "Government's Intrusion into Privacy Is Excessive" Maeil Gyungjae [The Economic Daily], October 19, 2004, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=009&article_id=0000400141&section_id=101&menu_id=101>.

[71] *Id.*

[72] "Location-Tracing Sparks Privacy Concerns", Korea Times, November 16, 2004, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=040&article_id=0000016873&section_id=108&menu_id=108>.

[73] *Id.*

[74] *Id.*

[75] "Sharp Rise in Tappings of Mobile Phone Text Messages and Voice Mailboxes by Government Investigative Agencies," JoongAng Daily, November 24, 2004.

[76] "Government's Intrusion into Privacy Is Excessive," Maeil Gyungjae [The Economic Daily], October 19, 2004, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=009&article_id=0000400141&section_id=101&menu_id=101>.

[77] "Third party's Recording of Phone Conversation without Consent of Both Parties to the Phone Call Is Illegal," Kookmin Ilbo, October 14, 2002, available at

illegal for a journalist to publish a recording that he made of a phone conversation without the other person's consent.[78]

Unauthorized phone taps – through the illegal use of interception equipment and radio frequency devices – have also been increasing at an alarming rate.[79] Despite rising public awareness over violations of privacy, in 2005, the Ministry of Justice (MOJ) has been pushing a controversial new law that grants government authorities greater freedom to gather evidence through phone taps by requiring landline and wireless telephone companies to implement new surveillance technologies.[80] The MOJ is in discussions with the MIC and expects to complete the law by August 2005.[81]

South Korea has one of the world's highest concentrations of mobile-phone users. As the quality of photos taken by phone cameras improves, there is rising concern about possible privacy abuses. In November 2003, the MIC introduced regulations to protect against the surreptitious taking of photos in public areas such as locker rooms and swimming pools. Starting in 2004, mobile phone manufacturers are required to design camera-enabled mobile phones to make "camera shutter" sounds, of at least 64 decibels, when a picture is taken.[82] The *Korea Times* reported that the MIC was drafting a new bill to prohibit individuals from taking photographs of others using camera phones without prior consent.[83]

According to the US State Department, it was "difficult to estimate the number of political prisoners because it was not clear whether particular persons were arrested for exercising the right of free speech or association, or were detained for committing acts of violence or espionage."[84] Amnesty International reports that the Korean

---

<http://news.naver.com/news/read.php?mode=LSD&office_id=005&article_id=0000122348&section_id=102&menu_id=102>.

78 "Not Illegal to Write Article Based on Secret Tape Recording," Edaily, August 3, 2004, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=018&article_id=0000188418&section_id=102&menu_id=102>; *see also* "Publishing Article Based on Secret Tape Recording of Conversation Is not Unlawful," OhMyNews, August 3, 2004, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=047&article_id=0000048896&section_id=102&menu_id=102>.

79 "Illegal phone taps increasing sharply," Korea Herald, June 15, 2005, available at <http://www.koreaherald.co.kr/archives/result_contents.asp?id=200506150043&query=illegal%20phone%20taps>

80 "Illegal Phone Taps Increasing Sharply," Korea Herald, June 15, 2005, available at <http://www.koreaherald.co.kr/archives/result_contents.asp?id=200506150043&query=illegal%20phone%20taps>.

81 *Id.*

82 "Phone Camera Makers Are Told to Use 'Click' to Protect Privacy," JoongAng Daily, November 12, 2003.

83 "Camera Phone to Require Shutter Sound from Next Year," Korea Times, November 11, 2003.

84 US State Department Human Rights Report 2004 - South Korea, available at <http://www.state.gov/g/drl/rls/hrrpt/2004/41647.htm>.

government continued to require released political prisoners to report regularly to the police under the Social Surveillance Law.[85]

Under the National Security Law, it is forbidden for South Koreans to listen to North Korean radio in their homes or read books published in North Korea if the government determines that they are doing so to help North Korea. However, in 1999 the government made it legal for South Koreans to view North Korean satellite telecasts in their private homes. The government also allows the personal perusal of North Korean books, music, television programs, and movies as a means to promote understanding and reconciliation with North Korea. Student groups make credible claims that government informants are posted on university campuses.[86]

The Use and Protection of Credit Information Act of 1995 protects credit reports.[87] In July 2001, three large credit card companies were fined under this law. The companies were found to have disclosed personal information on their customers (including bank account numbers, pay levels and credit card transaction records, and customer identifiers such as names, addresses, phone numbers and resident-registration numbers) to insurance companies without giving notice to their customers or obtaining their consent in advance.[88] The Postal Services Act protects postal privacy.[89]

Since January 2002, Korea has maintained a DNA database of missing children.[90] Registry in the database is voluntary, and it is available to parents and children in orphanages.[91] The Supreme Public Prosecutor's Office (SPPO) analyzes the samples, and the information is stored in a database maintained by Biogrand, a private company.[92] Privacy advocates are concerned that the SPPO, an office engaged in criminal prosecutions, collects the DNA samples.[93] The SPPO maintains that they do not have access to personally identifiable information aside from age and sex when they receive a DNA sample, and that the database's use is strictly for family relationships.[94] Privacy advocates are nevertheless wary because there are no specific

---

85 *See* Amnesty International, Republic of Korea (South Korea), available at <http://www.web.amnesty.org/ai.nsf/index/ASA250181998>.

86 US Department of State, Country Report on Human Rights Practices – South Korea 2003.

87 No. 4866, Enforcement Decree for the Act Relating to Use and Protection of Credit Information.

88 "Stricter Privacy Protection," Korea Herald, July 19, 2001.

89 Act No. 542, last amended by Act No. 8852, February 29, 2008.

90 E-mail from Kim Nak ho, Department of Communications, Soul National University to Waseem Karim, Law Clerk, Electronic Privacy Information Center (EPIC), July 5, 2002 (on file with EPIC).

91 *Id.*

92 *Id.*

93 *Id.*

94 *Id.*

laws that address DNA information.[95] As such, there is the potential for abuse and extending the database's function.

On April 19, 2005, it was asserted during a National Assembly session that the MIC "had purchased private information of fingerprints and facial skeletal features without a clear-cut legal basis."[96] Rep. Hae-Suk Suh of the Uri Party argued: "Over two years since 2002, the MIC has spent [KRW] 2.8 billion to establish a database on vital information of 5,620 people including minors. . . . The government continues to amass personal identification data on the grounds that it is useful for the commercialization of biometrics."[97] The MIC admitted that its affiliate, the Korea Information Security Agency (KISA), has "carried out the collection of 3,600 fingerprints and 2,020 facial skeletal features," but denied any wrongdoing, pointing out that the Act on Promotion of Information and Communications Network Utilization and Data Protection (DPA) stipulates that "the MIC can ferret out measures for protection of individual information together with the KISA."[98]

Biometric Passports

The Ministry of Foreign Affairs and Trade proposed a revision of the Passport Act which would introduce electronic passports(or biometric passports) in may 2007. It's only one year since the new passport in which picture is digitally printed was introduced in September 2005, to tighten security of passports. Before this change, the picture in the passport was printed and then glued to the passport. An electronic passport has IC chip embedded on the back cover and the personal information is retrieved by RFID technologies. According to the guideline of International Civil Aviation Organization (ICAO), the IC chip should contain the passport holder's personal information and a face shot and optionally fingerprints. Korean electronic passports was designed to include fingerprints as a requisite information on the ground of improving accuracy. The reason why the Korean government introduce electronic passports is to be eligible for the U.S. Visa Waiver Program (VWP). Human rights groups criticized that electronic passport system would violate citizen's privacy due to gathering of biometric information and indefinite collection of personal information, and that introduction of electronic passport system just after introduction of digital passport system is wasting budget.[99] Moreover, they criticized

---

95 *Id.*

96 "Ministry Buys Individual Information for Research", Korea Times, April 20, 2005, available at <http://news.naver.com/news/read.php?mode=LSD&office_id=040&article_id=0000021481&section_id=108&menu_id=108>.

97 *Id.*

98 *Id.*

99 38 Human Rights Groups including Korean Progressive Network, "Stop Electronic(Biometric) Passports", October 8, 2007, available at <http://act.jinbo.net/webbs/view.php?board=policy&id=1322&page=1>

that Electronic Travel Authorization(ETA), that one of the requirements of VWP, is just a different name of Visa system, and that personal information can be easily transferred across national borders due to the measures such as the passenger information exchange agreement.

The revision of the Passport Act, which postponed the collection of fingerprints for two years, was passed in the National Assembly in February 2008. Electronic passports will be issued to the public from August 2008. Human rights groups including Korean Progressive Network Jinbonet built up 'Reissue for Freedom' campaign that encourage people to apply for reissue of their passports before electronic passports will be introduced.[100]

CCTV

Public institutions have been introducing CCTVs rapidly since the Kangnam-gu ward office and the Kangnam police office installed five CCTVs by a way of showing an example in 2002. According to "White Paper of MOGAHA(2003-2007)", the number of CCTVs installed by public institutions is estimated about 126 thousands in June 2007.[101] They are used for crime prevention, control over illegal parking or fly-tipping, etc. Human rights groups had criticized that CCTVs installed by public institutions had no legal ground and would infringe citizen's privacy. In may 2004, the NHRC announced "The Policy Recommendation on the Installation and Management of Unmanned Regulation Equipments such as CCTVs Installed by Public Institutions", which pointed out that at present the police or the local government entities judged necessity, installation locations, ways of management and installation processes of unmanned regulation equipments such as CCTV at their discretion, which could infringe citizen's right by taking pictures and recording the portrait and motion of passersby, or private life depending on the way of installation and management. And the NHRC recommended the chairman of the National Assembly and the minister of the MOGAHA to make a legal guideline on unmanned regulation equipments such as CCTV by enacting a new law to guide the installation and management of unmanned regulation equipment such as CCTV installed by the police or the local government entities for crime prevention and investigation, or modifying the Act on the Protection of Personal Information Maintained by Public Agencies.[102] Since then, articles on CCTV were included in the Act on the Protection

---

[100] People Who Advocate on ‘Reissue for Freedom’ against Electronic Passports, "Statement on 'Reissue for Freedom'", April 22, 2008, <http://biopass.jinbo.net/>

[101] Ministry of Public Administration and Security, "White paper of MOGAHA(2003-2007) ", available at <http://www.mopas.go.kr/gpms/ns/mogaha/user/userlayout/bulletin/userBtView.action?userBtBean.ctxCd=1010&userBtBean.ctxType=21010005&userBtBean.bbsSeq=1034660>

[102] National Human Rights Commission, " The Policy Recommendation on the Installation and Management of Unmanned Regulation Equipments such as CCTVs Installed by Public Institutions", May 10, 2004, available at <http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=554769&page=2>

of Personal Information Maintained by Public Agencies in May 2007, and were enforced since November 2007.

However, according to 'the survey on management of CCTV installed by public institutions' conducted by the Data Protection Review Commission under the Premier's Office in February 2008, most of CCTVs were capable of zooming and rotating. In addition to that, some CCTVs had recorded voices even without the recognition of the person concerned. Only 64 % of CCTVs noticed their existence. This survey investigated only 12,778 CCTVs installed by 14 public institutions. Human rights groups has insisted on removing illegally managed CCTVs and strengthening the regulations on CCTV.[103]

There is not legal ground to regulate CCTVs in the private sector yet. There is only "Guideline for Protection of Personal Image Information by CCTV" proposed by the MIC in October 2006.[104]

Workplace Surveillance

On November 27, 2007, the NHRC made a decision that electronic surveillance using various technologies such as CCTV, IC chip embedded card, GPS etc. was conducted in the workplace in the private and the public sector, which could violate human rights of workers who were kept under surveillance, and recommended the minister of the Ministry of Labor to enact a special act to regulate strictly all kinds of electronic surveillance in the workplace and a concrete guideline for the protection of human rights, which should be included in the act. In addition, recognizing that generalized electronic surveillance was an important factor which would change worker's circumstances, it recommended the minister to revise 'the Labor Standard Act' reflecting the factor, and to strengthen its supervision of individual workplace.[105]

The Youngnam University Medical Center, which was under conflicts between labor and management since August 2006, installed CCTVs around the sit-in place of the labor union in Octorber 2006. Labor unions and human rights groups in the region criticized that it was intended to supervise and control the labor union.

---

[103] Human Rights Network, "CCTVs Installed by Public Institutions are a Concealed Camera?", May 19, 2008, available at <http://act.jinbo.net/webbs/view.php?board=policy&id=1422&page=1>

[104] Korea Information Security Agency, "Guideline for Protection of Personal Image Information by CCTV", available at, <http://www.kisa.or.kr/kisa/privacy/jsp/privacy_notice_view.jsp?g_id=privacy&cgubun=&keyField=title&gid=privacy&b_gubun=01&cpage=1&page=1&dno=29&d_no=29&r_no=0&keyWord=>

[105] National Human Rights Commission, "The Act for the Protection of Workers under Electronic Surveillance is Needed", November 27, 2007, available at <http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=555369&page=1>

The fact that the location information of workers and laid-off workers of Samsung had been traced for several months through illegally-copied mobile phones became known to public in 2004. Though labor unions and human rights groups in the region claimed that it was the surveillance conducted by Samsung, the prosecution announced that it was true that someone traced the location of workers, but they couldn't find who traced the location, and stopped indictment. However, the prosecution resumed investigation in March 2008, because a new testimony and evidences that location tracing had been conducted by Samsung were presented.

Open Government

The Official Information Disclosure Act is a "freedom of information act" that allows Koreans to demand access to government records. It was enacted in 1996 and went into effect in 1998.[106] The Supreme Court ruled in 1989 that there is a constitutional right to information "as an aspect of the right of freedom of expression, and specific implementing legislation to define the contours of the right was not a prerequisite to its enforcement."[107] In 2007, an Information Disclosure Task Force comprised of government, media and academics was formed to create proactive disclosure policies and to suggest revisions to the Information Disclosure Act.[108]

In March 2003, the Korean Ministry of Education and Human Resources launched the National Education Information System (NEIS), a nationwide database that links the information of over 10,000 school and education agencies.[109] The purpose of the NEIS is to enable schools to share education information with each other.[110] Various organizations opposed the implementation of the NEIS due to the threat that the system poses on the privacy of students and teachers, including the National Teacher's Union, which organized a strike.[111] Furthermore, the NHRCK recommended that the Ministry of Education abandon maintaining three categories of information (school management information, student academic records, and health and enrollment records) within the NEIS, determining that the Ministry lacked the

---

106 Wholly amended by Act No. 7127, January 29, 2004, last amended by Act No. 8871, February 29, 2008

107 Right to Information (1 KCCR 176, 88 HunMa 22, Sep. 4, 1989).

108 "Forming Information Disclosure Enhancement Task Force to ensure the people's rights to know," Ministry of Government Administration and Home Affairs, August 2, 2007 <http://www.mogaha.go.kr/gpms/ns/mogaha/user/userlayout/english/bulletin/userBtView.action?userBtBean.ctxCd=1030&userBtBean.ctxType=21010009&userBtBean.bbsSeq=1011596>.

109 "Privacy or Convenience," Korea Herald, May 22, 2003.

110 Among the stated goals "are setting up the national standardization of educational content, evenly distributing educational information among different regions, and establishing more rational educational policies," Launching the National Education Information System (NEIS)

111 Participants in the strike were also opposed to pressure from the World Trade Organization to open Korea's educational sector to foreign competitors. "Teachers Union to Launch Strike Against NEIS," Yonhap English News, March 26, 2003.

legal foundation to implement NEIS in this manner, and the threat that the system posed to privacy was significant.[112] As a result of the opposition, the government decided that they would rethink the NEIS after gathering more information.[113]

International Obligations

South Korea is a member of the Organization for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[114]

---

[112] Among the risks cited by the NHRCK was the potential for hackers to steal information from the system. *Id.* The Commission stated that the kind of information that the system contained about a student was so intimate that it demanded constitutional protection. "Privacy or Convenience," Korea Herald, May 22, 2003.

[113] Hyung-Jin Kim, "Controversial Education Database under Review," Korea Herald, May 20, 2003.

[114] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at <http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.