7. Republic of Korea

Whon-Il Park

South Koreans are familiar with the words of a song, 'My RR Card'. In 1997, a Korean rock singer roused sympathy by the following lines:

> Korean citizens hold RR cards
> I'm bearing in mind 800216-1068312
> This number is more important than my name
> Engraved in my head
> The number will be alive until I die

Without the resident registration card, South Koreans have trouble getting inside government buildings, or applying for financial transactions and website membership. Sometimes they are asked by policemen to show the identity card on the street.

Transsexuals have more troubles with these cards. While the first group of the resident registration number means the birthday (yy/mm/dd), the following seven digits denote the sex and residential information of the holder. So it is troublesome to hold a card which shows a different sexual identity from his/her appearance. Some transsexuals filed a lawsuit with the court to change the sex digit, but only a few succeeded. Until June 2006, when the Supreme Court approved the change of sex in the family census registry, judges would not have allowed such change.

HISTORY OF PRIVACY PROTECTION

At first, holding the resident registration card was mandatory for the purpose of national security. But the situation has drastically changed in the past 40 years. With unparalleled economic development and democratization of the Korean society, the resident registration number is no longer indispensable to protect the country. On the contrary, it could be a Big Brother's weapon. The fate of this number illustrates the changing view of privacy in South Korea. Initially introduced for national security, the number is now regarded as a potential threat to privacy.

Conflict between Liberty and Security

With the end of the Japanese occupation (1910–45), South Korea adopted liberal democratic ideas. But the Korean War broke out in 1950 and divided the Korean peninsula. After a brief and tumultuous democratic interlude in the early 1960s, Korea's politics were dominated by a series of military strongmen (Ginsburg 2004, pp.2–3). This authoritarian period nevertheless had a silver lining of rapid economic development.

From the late 1960s until the 1980s, North Korea staged occasional terrorist attacks against South Korea. In January 1968, North Korean guerrillas infiltrated to the outskirts of the Blue House, the Presidential residence in Seoul. A few days later the Pueblo, an intelligence ship of the US Navy, and all its crew, were seized by North Korean patrol ships in international waters. The North Korean regime continued to terrorize their South Korean brethren by hijacking a private airplane in 1969, and directing a Japanese agent to assassinate President Park Chung-Hee and First Lady in 1975. In 1983, they attempted to kill President Chun Doo-Hwan on his state visit to Myanmar. In 1987, North Korean terrorists destroyed a Korean airplane with 115 passengers and crew flying over the Indian Ocean to stymie the Seoul Olympic Games.

Perhaps Korea's threatening geopolitical reality justified some restriction of fundamental rights for the sake of national security. However, the restriction of freedom went too far. Throughout the 1970s, President Park proclaimed a series of Emergency Presidential Decrees to restrict fundamental rights ostensibly to protect the state from the North Korean threat. But, in a real sense, President Park's political action was oriented to continue his dictatorship.

Struggle for Democratization

Mounting demand for privacy protection generated pressure on the Korean government to respect the constitutional rights. In 1987, the democratic movement, known as the 'June Struggle', changed the political landscape. It made the authoritarian regime comply with citizens' constitutional rights. Confronted with student protests against the iron fist rule of President Chun, the general-turned President allowed a broad liberalization. The international environment was a crucial factor in his decision to democratize the nation (Ginsburg 2004, p. 4).

Meanwhile, military tension between North and South eased in the midst of East-West rapprochement. The 1988 Seoul Olympiad focused the international spotlight on the daily life of ordinary Koreans. Rights of Korean dissidents attracted worldwide attention. In 1996, Korea was admitted to the

Organization for Economic Cooperation and Development (OECD). To secure admission, South Korea promised to observe human rights. At that time, its per capita income exceeded $10,000. In the wake of the rising prosperity of the late 1980s, human rights issues came to the foreground of public opinion.

The advent of the Information Age has opened a new dimension of privacy issues. The information highway has made it possible for the government to implement far-reaching e-Government projects. For example, the government planned to consolidate relevant information in the public sector, and to provide on-line administrative services to citizens. At the same time, popular curiosity has found all sort of new outlets, including celebrity scandals now detailed over the internet.

Full Bloom toward a Ubiquitous Society

Since the early 1990s, 'ubiquitous computing' has become one of the most frequently-used words. The government took an initiative to establish the nationwide computer and communications network in such areas as government administration, banking and finance, education, R&D and national defense.

According to a survey by the Communication Ministry, 31.6 million people over six years of age use the Internet. This means that virtually all Koreans have access to cyberspace. Korea boasts the highest distribution rate of internet broadband networks in the world (JoongAng 2005a). Over 70 per cent of Korean households subscribe to high-speed internet services. The Information Age has brought to Korea significant improvements in the efficiency and convenience of living. The 'nationwide internet breakdown' on 23 January 2003, when the Sapphire/SQL Slammer worm computer virus paralyzed nationwide administrative and banking operations through national key networks for half a day, illustrated how dependant Korea has become on the internet.

Information processing equipment and facilities are distributed and used everywhere including homes, work places, schools, transportation, communications, finance, sports and games, just like the nerve center of a body. Ordinary Koreans enjoy the benefits of high-speed internet services, but they also demand that the government be concerned about privacy issues involved in the use of this new technology. As for the ubiquitous computing, government officials and specialists are eager to develop some useful guidelines to prevent the abuse and misuse of such sophisticated technology.

Overview of Privacy Protection Laws

South Korea's privacy protection legislation has been established by sector.

The public sector, where the resident registration number was generally used, had urgent need of data protection law while privacy protection in the private sector was implemented on a case-by-case basis.

The Public Agency Data Protection Act of 1995 governs the government's collection of personal information in accordance with the OECD Guidelines on privacy protection. This Act applies to all public institutions, government departments and offices in the Administration, the Legislature and the Judiciary as well as local governments, various schools, government-owned companies, and public sector institutions. Accordingly, in the public sector, privacy protection provisions are found in the Act on Communication Secrets, the Telecommunications Business Act, the Medical Services Act, and the Public Agency Data Protection Act, among others. Because an OECD member state is required to observe OECD rules, the Korean government adopted the OECD Privacy Principles.

In the private sector, the Credit Information Act, the Framework Act on Electronic Commerce and the Electronic Signature Act contain data protection provisions. For example, the Framework Act on Electronic Commerce requires that electronic traders shall not use, nor provide to the third party, personal information collected through electronic commerce beyond the notified purpose for collection without prior consent of the data subject or except as specifically provided in any other law.

Among others, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the 'Data Protection Act' as amended in 2001) generally applies to entities or individuals that process personal data for profit through telecommunication networks and computers. Personal credit information and medical records are protected by other legislation.

Public Sector Privacy Legislation

The Public Agency Data Protection Act sets the norm for the management of computer-based personal information held by government agencies. Under this Act, government agencies are required to limit data collection, ensure the accuracy of data, keep public registers of data files, ensure the security of the information, and limit use of personal data to the purposes for which they are collected. Only computerized data fall within the scope of this Act. Manually collected information may be protected by the Criminal Code and other relevant laws, which require public servants to maintain confidentiality in administrative work.

Personal information maintained by public agencies, whether computerized or not, is also governed by the Act on Disclosure of Information by Public Agencies, South Korea's freedom of information act. But if the information

affects another individual's privacy, the public agency must decline to disclose it. The data subject is also entitled to request necessary modification of defective government-held data (Constitutional Court 1989).

The Public Agency Data Protection Act is enforced by the Ministry of Government Administration and Home Affairs (the 'Administration Ministry') responsible for government administration and police affairs. The Administration Ministry must be informed in advance of what kind of personal information files are maintained in each office by the head of competent agency, and it must publish the list of such personal information files more than once a year in the Official Gazette. The Administration Ministry may request the pertinent public agency to submit the personal information processing report, permit its employees to inspect the actual conditions, and give suggestions or advice on how to protect personal information effectively.

Critics of this Act say that there are few provisions to prevent excessive collection of information by public agencies. In addition, there are overall exceptions to the application of this Act with regard to agencies like the National Intelligence Service (NIS) and other law enforcement bodies. And there is no guarantee of independence of the oversight body in the Administration Ministry and the Personal Information Protection Deliberation Committee under the Prime Minister.

Surprisingly, it was disclosed in early 2005 that NIS, a Korean CIA, had collected personal information without court permission. According to news reports, NIS secretly eavesdropped on conversations of 1800 politicians, journalists, government officials and businessmen in a 24-hour-a-day operation during the period from 1998 to 2003. Public opinion demanded a special prosecutor to investigate the case. As a result, the former heads of the nation's intelligence agency were arrested in November 2005, and sentenced for illegal wiretapping (JoongAng 2005b).

INCREMENTAL INFLUENCE OF PUBLIC OPINION

Over the past two decades, public opinion has played a leading role in democratization of South Korea. Government disregard for citizens' privacy has been the target of criticism by the press as well as civic organizations. The internet and cellular phones play an effective role in mobilizing public opinion. The power of public opinion comes from the keyboards of netizens or the thumbs of mobile phone users based upon Constitutional rights. In the same way as they gathered to support the Korean football team in the 2002 FIFA World Cup, Korean people often gather in front of Seoul City Hall at night to declare or protest something important with candle lights.

Constitutional Ground for Privacy Disputes

The Korean Constitution provides for the general protection of privacy (Art. 17), and specifically for the protection of privacy of home (Art. 16) and in communications (Art. 18). The Constitution also affirms that freedoms and rights of citizens shall not be neglected on the grounds that they are not enumerated in the Constitution (Art. 37(1)). These protections can be abridged in exceptional circumstances: freedoms and rights of citizens may be restricted by the law only when necessary for national security, law and order, or public welfare. Even when such restriction is imposed, essential aspects of the freedom or right shall not be violated (Art. 37(2)). It means that the utmost need to enhance the administrative efficiency cannot justify the infringement upon the privacy of ordinary citizens.

In 2003, the Constitutional Court made a noteworthy interpretation of these provisions:

> The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private living. Concretely, the privacy protection is defined as protecting and maintaining the confidential secrecy of an individual; ensuring the inviolability of one's own private life; keeping from other's intervention of such sensitive areas as one's conscience or sexual life; holding in esteem one's own personality and emotional life; and preserving one's mental inner world. (Constitutional Court 2003)

The data protection rule is to protect the data subject from inappropriate access to, and abuse or misuse of, its personal information. Personal information is understood to mean the data of a living person comprising sign, character, voice, sound and image,and so on, which may be used solely, or together with other easily combined data, to identify the data subject by means of a name, resident registration number, and so on. With the advancement of information technology, the scope of such information increasingly expands to include email addresses, credit card numbers, log files, cookies, GPS location data, DNA data, etc. In this connection, individual belief, conscience, medical records, sexual orientation, race, trade union activities and criminal records are regarded as sensitive data.

NEIS Controversy Defeating e-Government Project

The biggest recent privacy struggle between the government and the public was regarding the National Education Information System (NEIS), a scheme proposed in 2003. This plan ostensibly aimed at enhancing the efficiency of educational administration and improving teachers' working conditions. The

Ministry of Education and Human Resources Development (the 'Education Ministry') asserted that NEIS would be an efficient, technologically advanced and transparent system.

NEIS sought to centralize personal data of about eight million students from 12,000 primary and secondary schools across the country in a national broadband network. Twenty-seven categories of personal information were to be consolidated in NEIS servers maintained by local education agencies. NEIS was supposed to include data on students' academic records, medical history, counseling notes, and family background. Even data on teachers' trade union activities were to be held by the Education Ministry.

The National Teachers' Union (NTU) opposed the system. It and other civic organizations conducted protest rallies and threatened a general strike. Disappointed by the lukewarm response of the government, they brought an action with the National Human Rights Commission. The enhanced efficiency in information sharing offered by NEIS was depicted as a potential risk to privacy. The Commission recommended that three of 27 categories of personal data be excluded from the NEIS databases.

Accordingly the Education Ministry excluded these three categories of data, keeping other 24 categories of school affairs intact. While NTU threatened to stage an all-out protest against the implementation of NEIS in November 2003, the Seoul District Court approved a motion to block the use of NEIS data-contained CDs of three high school students. As a result, the Education Ministry was prohibited from distributing useful student data from the NEIS necessary for the application for the college entrance exam. Because NEIS data-contained CDs regarding applicants were indispensable to the processing of the on-line college entrance applications, such a negative court order could paralyze the whole college entrance exam procedure. In December 2003, the government decided to separate the sensitive data from the NEIS databases and to operate them in different computer systems.

In July 2005, the Constitutional Court held that such personal information as the graduate's name, birthday and graduation date, contained in the NEIS databases, are necessary for the administrative purposes of the Education Ministry. Consequently, pertinent schools and institutions are able to issue certificates of graduation at any time by accessing the NEIS database. So the current NEIS databases were found to comply with the Constitution and the relevant laws on data protection, and could be maintained (Constitutional Court 2005).

Changing Concept of Privacy

In South Korea, the right to privacy is a developing and unfinished concept.

For one thing, the right to privacy and the freedom of expression are both

fundamental rights; and there is no priority between them. So we have to compare and analyze the competing legal interests when they are infringed upon. The Korean Supreme Court held:

> In a democratic state, it is common to form a majority opinion by means of free making and exchange of one's expression, thereby maintaining the democratic political order. So the freedom of expression on a public issue shall be protected as a constitutional right, but the right to privacy or the individual reputation and secrecy shall be ensured as much. The conflict between the right to privacy and the freedom of expression should be settled and adjusted in a concrete case after comparing the interests in a social environment protected by the respective right or freedom, and the extent and method of regulation should be determined accordingly (Supreme Court 1998).

Secondly, once privacy is violated, the damage can be difficult to repair. When celebrities' privacy is violated in a scandalous news story, their loss of privacy becomes a *fait accompli* regardless of the truth. Because a forced apology to cancel the former privacy invasion or the publication of the opposite opinion could exacerbate the infringement upon privacy, injunctive remedies are more generally granted than in the case of defamation (Sung 2003, p. 88).

NATIONAL CULTURE AND TRADITIONS

Traditionally Korean citizens have been accustomed to authoritarian rule. More recently, they have grown aware of their fundamental rights. Though they are required to use the resident registration number in daily life, they have come to understand the negative aspects of information society, that is, abuse or misuse of personal information. As South Korea has become more democratic, civic groups have been very active in demanding privacy protection from the government and IT businesses. In response to such demands, the Korean government has implemented a unique remedy system that provides pecuniary compensation to alleged privacy victims.

Pros and Cons of General Identifier

Although 'Asian Values' allegedly contributed to economic growth, they functioned as a stumbling block to democratic developments. Since the Korean War in the early 1950s, Korean rulers favored national security and economic growth over human rights. But democratization changed the situation dramatically. A good example is the ID system.

As mentioned before, in South Korea, every citizen is given an ID number at birth – the resident registration number. This number contains 13 digits

conveying information about the holder. This ID system was generally implemented just after the armed guerrilla attack in January 1968. Now the ID number is used for administrative purposes, from applying for various government services to proving that one is a real person with a real name. As a result, someone with access to administrative databases associated with use of the card can gain detailed information about where its holder is living, how much he earns and pays in tax, and what kind of business he is engaged in. It is because the residence, tax and other government databases are constructed based on this general identifier.

The resident registration number functions as a link to government-maintained databases. This number makes it possible for government officials to compile personal information and to do profiling and data matching of extensive information about Korean citizens. The 13-digit number is like 'Aladdin's sesame' to open government databases. Because it is easy to centralize and profile citizens' data, privacy-conscious South Koreans seek assurances that the ID number is not used for purposes of surveillance (Sung 2003, p. 94). Several civic groups have acted as watchdogs against government plans to establish and consolidate databases for administrative efficiency.

In the private sector, on-line information service providers usually demand users' resident registration numbers. To protest this practice, some users submit made-up numbers instead of real ones; others steal someone else's ID number. For example in 2005, 53.9 per cent of those who filed claims with the Personal Data Protection Center in Seoul reported their ID numbers had been illegally used or stolen (PIDMC Yearbook 2005, p. 50). Against this backdrop, some critics suggested that information service providers should not be allowed to collect individual users' ID number (Chung and Kim 2004).

Real Name Required for Financial Surveillance

Throughout the 1990s, the Korean government took the initiative in protecting citizens' privacy both by law and in practice. But civic organizations were not satisfied with these measures. They demanded reinforced security measures for individual privacy including credit information.

Take an example of the Real Name Financial Transaction System, which sought to ensure that financial transactions are conducted under real names. It meant that no one could open bank accounts without disclosing his or her name and resident registration number. Until the early 1990s financial transactions of large amounts between private parties had usually been conducted under false names or pseudonyms to protect the confidentiality of such transactions and to evade tax as well.

In 1993, President Kim Young-Sam suddenly proclaimed his Emergency Presidential Order on Real Name Financial Transactions and Protection of

Confidentiality. The newly-elected President Kim sought a clean image by enforcing the conduct of all financial transactions under real names. It was believed that former Presidents Chun Doo-Hwan and Roh Tae-Woo had concealed their slush funds under false names or pseudonyms. If concealed financial transactions could be exposed by means of the real name transaction system, a remarkable increase of tax revenues should result. This regulation aimed at keeping the underground economy under tight control by making all transactions subject to taxation. The Presidential Order was transformed into the Act of the same name in December 1997.

The real name financial transaction system required everyone to submit such certificates as the resident registration card, driver license or passport evidencing his or her real name before completing transactions with financial institutions. The subsequent surveillance effect was bigger than expected. In November 1995, ex-Presidents Chun and Roh were convicted and jailed for accumulating and concealing huge slush funds while in office and violating the Presidential Order.

The act prevented banks and other financial institutions from informing third parties (for example, creditors, tax collectors, investigators, and so on) of any financial transaction involving banks, savings, securities companies and insurance companies without a request or the consent of the data subject. There are some exceptions where personal information is required under subpoena or warrant, or required by law for a tax inquiry under tax laws, etc. In July 2001, three large credit card companies were fined under the law. The companies were found to have disclosed personal information on their customers (including bank account numbers, salary, credit card transaction records, customer names, addresses, phone numbers and resident registration numbers) to insurance companies without telling their customers or obtaining their consents in advance (Herald 2001). Those credit companies were affiliated with the insurance companies under the same business group.

Crimes Abusing and Misusing Personal Identity

The identity card or NEIS systems are loaded with personal information, opening the possibility of many crimes and abuses. After the financial crises in 1997, a wave of identity crimes broke out. Criminals found ways to use affluent people's personal data to commit fraud or burglary. The original NEIS was dangerous because it disclosed students' family wealth and other information which could be used illegally by criminals.

In the 2000s, some burglars were reportedly tracking foreign-made luxury cars with certain motor vehicle registration plates. Initially the plate number showed the registration place of the garage. Once, robbers threatened a female driver when she parked her car at an isolated parking lot at night. In 2004, the

government hurried to change the format of private car plates to omit information on the owner's place of residence.

Privacy Agency Providing Pecuniary Remedies

In Korea, financial penalties pay for the protection of privacy. The Korean Personal Information Dispute Mediation Committee (PIDMC) provides financial compensation to individuals whose statutory privacy rights are found to have been infringed upon by merchants. In 22 cases reported by PIDMC during 2003–04, the committee awarded compensatory damages in 17 cases where a breach of privacy rules was found. Damages ranged from US$100 to US$10,000 (see PIDMC 2005). A mere misuse of personal information case, for example, reckless disclosure of personal data, usually results in compensation of around US$100. The more serious the privacy invasion is, the more compensation is required. In only a few cases of breach did PIDMC recommend corrections or other remedies without any payment of compensation.

A woman specifically requested her mobile phone company not to disclose details of her telephone calls to anyone else. Then she found that a branch of the telephone company had nevertheless disclosed them to her ex-husband, who had produced a copy of her ID card when applying for the details. The mobile phone company was held responsible for professional negligence, and she was awarded 10 million won (equivalent to US$10,000) in compensation for the economic and mental damages.

In another case, a plastic surgeon displayed a movie of a patient's operation on his clinic's website. He was required to pay 4 million won (around US$4000). The award would have been increased if she had objected to it during the filming. A translation service company posted a woman's resume on its website without her consent, as if she was an interpreter employed by them; the company was required to pay 200 thousand won (around US$200) compensation. An insurance company that provided a person's personal information to another company so that they could solicit business from him was required to pay 200 thousand won (around US$200). Taking into consideration monetary compensation, Korea's privacy authorities regard privacy violations more seriously than any other data protection agency in the world. We will see later how this unusual privacy agency is doing its work.

Recently pecuniary remedies have seen a different dimension of incidents as Korean-made on-line games are getting popular cross the border. In April 2006, the Seoul Central District Court held that NC Soft of Lineage II should pay 500 thousand won (around US$500) each to the plaintiffs. The court said that game site operators obtaining commercial profits from many users have a duty of special care to protect the personal information of customers. Though actual damage could not be identified, the defendant should pay damages on

account of a gross negligence or fault that it did not preserve users' personal ID and password by encryption and caused the personal data to be stolen by other customers (Park 2006b, p. 12).

Lackluster Self-regulation of the Private Sector

Self-regulation does not work well in South Korea. Take the example of the Half Price Plaza, an on-line shopping mall. The internet shop owner ran aggressive on-line advertisements, promising its members half price on a number of items. In the end, the owner ran away with customers' deposits. This case rang an alarm bell that on-line shopping malls are not always safe and credible.

One semi-official form of self-regulation was established under the Data Protection Act. The Korea Association of Information and Telecommunication (KAIT, www.kait.or.kr), a private entity supported and supervised by the government, started its operation in 2000. KAIT regularly awards the Privacy Mark to internet sites and on-line businesses voluntarily engaged in data protection on an appropriate level. KAIT established an association composed of chief privacy officers (CPOs) in charge of personal information of customers. The organization is to enhance work ethics and awareness of privacy protection, to provide educational and training programs to member companies, and to formulate self-regulatory guidelines by industry.

Although the Data Protection Act does not otherwise stipulate industry-wide self-regulation, it is possible for any entity to implement self-regulatory measures (see Yi and Ok 2003). For example, the Association for the Improvement of E-Mail Environment was established in 2002 by direct marketing merchants as its members to cope with increasing citizens' dissatisfaction with spam and direct marketing mails, as well as improving the internet-based business culture and coordinating the interests of its member businesses.

WINNERS AND LOSERS

The privacy issue on the internet has produced apparent winners and losers. The Korean government has successfully implemented e-Government services via high-speed internet. Today ordinary citizens can process administrative applications at home by using their own home computers. However, the government had to admit some side effects of e-Government when the civic organizations successfully protested against the NEIS.

Privacy concerns have consistently helped swell the numbers of supporters of activist civic organizations. As a result of slush fund investigation, financial

information of the individual is more often than not disclosed because of bribery investigation, tax examination or health insurance fraud, while credit information is firmly protected by a special law.

Increasing Activism of NGOs

In the 1990s, politicians who had earlier been persecuted by military rulers gained power through democratic elections. Civic organizations friendly to such politicians as Kim Young-Sam and Kim Dae-Jung received handsome government support. Since the mid-1990s, these organizations have helped liberalize public policy making in South Korea by participating in various government committees and by shaping public opinion. The Korean political pendulum has made a full swing from the authoritarianism of past decades to today's free society. Civic groups have usually rated privacy issues very high – in contrast to the authoritarian rulers who deemed national security and economic growth as superior to human rights. They provide advice on privacy issues to individuals as well as businessmen, and conduct monitoring of market practices.

One of these groups is the Citizens' Action Network (CAN, action.or.kr) ? a non-profit NGO which encourages citizen action to reinforce the rights of ordinary taxpayers and consumers by the voluntary contributions of its members. CAN focuses on information-related rights maintaining an internet bulletin board regarding privacy invasion. Anybody can report to it such incidents as spam mails, unauthorized use of resident registration numbers and location information, closed circuit televisions (CCTVs) installation for monitoring, and so on. CAN advocates a comprehensive data protection law applying to both the public and private sectors.

People's Solidarity for Participatory Democracy (PSPD, www.peoplepower21.org) is also dedicated to justice and human rights and to legal and policy reforms. Since its establishment in 1994, PSPD, with 13,000 members as of 2005, has been serving as a watchdog against the abuse of power. It has staged public awareness campaigns, particularly in the area of privacy. PSPD has kept an eye on possible violations of privacy protection provisions by major industries. In 2003, PSPD claimed violations of the Data Protection Act by cellular phone companies, and filed suit for the deletion of such data and damages on behalf of over 4000 of their former customers.

The Korea Progressive Network Jinbonet (KPN, center.jinbo.net) is an activist network seeking enhanced human rights, anti-censorship and free use of copyright in cyberspace. Occasionally it staged a campaign 'e-Government hand-in-hand with Information Human Rights!' which addressed the problems of the resident registration number and NEIS. They demanded that installation of such systems as CCTV, software for monitoring emails or internet usage,

biometrics devices, smart cards and location detectors should be subject to the prior consent of the laborers or trade unions.

These civic organizations all support a campaign to replace the resident registration number with alternative IDs. They held various 'Be-Aware-of Big Brother' events around 25 June 2004 which marked the centennial anniversary of the birth of George Orwell. At one meeting of the centennial event, they debated on how to preserve human rights in a digital environment. In 2003, they succeeded in delaying the nationwide implementation of a real name check on the internet bulletin board, in which the government wanted to prevent users with a false name or non-existent resident registration numbers from posting any message or idea.

Protection of Credit Information and Slush Funds Scandal

In a privacy-friendly world, personal account information should be held confidential from others including the government. However, demand is growing for surveillance of transactions in the private sector as a means of reducing tax fraud and health insurance cheating. Government-maintained data matching is often called for to detect tax fraud.

Initially, individual credit information had no privacy protection. In the 1990s, the partially disclosed slush money of former Presidents changed the course of data flow. Investigators found the hidden transactions of ex-President Chun exploiting the underground economy. In order to avoid a run on the bank by ordinary people in fear of all-out tax examination, the government had to promise banking secrecy to individual depositors.

Consumer credit information has been protected separately by the Credit Information Act since 1995. Individual credit information, positive or negative, including bank accounts and transaction details may be used to decide to create or maintain financial transactions with the data subject. There are exceptions where credit information might be provided for other purposes with written consent of the data subject; under subpoena or warrant; for an inquiry under the tax law; or in accordance with other laws.

Consumers who feel their credit information has been misused by distrustful employers and landlords may claim damages against the credit information processor or users. In proceedings, credit information processors or users are required to prove the absence of intention or negligence. The Korean Financial Supervisory Service, a half governmental credit information watchdog, is empowered to supervise the operations of credit information companies. At present, credit information is protected separately from ordinary personal information, but in a manner consistent with core OECD privacy principles.

KISA's Activities as Privacy Guardian

Under the Data Protection Act, data subjects can demand access to their personal information, insist on correction of false information and challenge wrongful information. Collection of personal information should be minimized within the scope of purpose, and the collection and processing of data must be subject to privacy-related laws and regulations.

The Data Protection Act creates a guardian for privacy protection and security, the Korea Information Security Agency (KISA). KISA was established in 1996 to ensure information security and safety. It seeks to develop information security technology and policy research on information security. KISA has conducted surveys of compliance with privacy protection provisions in such areas as mobile communications, on-line shopping malls, banking and financing, department stores, accommodation, traveling, etc. It also monitors whether websites provide for the presence of a chief privacy officer, clarification to users of the purpose of collection and use of personal information, permission for access to the collected data and necessary modifications, the duration of maintenance of such information, and so on.

During 2005, KISA documented 3982 violations of privacy rules in a survey of 27 thousand businesses. Among these were unauthorized use of personal data and collection of children's data without parents' consent. Though the overall compliance ratio in 2005 was slightly over 80 per cent, KISA encouraged the information and communication businesses to implement technological and managerial safeguards of privacy including the adoption of Privacy Enhancing Technologies (PETs). It strongly recommended new guidelines on RFID privacy protection (Korean Briefing 2006), which came into effect in 2006.

Resolution of Privacy Complaints

South Korea has developed a unique method for resolving privacy complaints in the private sector, including a combination of government agency (KISA) investigation and alternative dispute resolution (ADR) with a possibility of litigation.

Under the Data Protection Act, anyone aggrieved in data protection matters may file his or her case with the Personal Data Protection Center (PDPC) within KISA. KISA has operated a secretariat of PDPC since April 2000. The purpose of the Center is to handle complaints regarding data protection, to monitor market practices, and to provide advice on various queries. The Center investigates complaints and provides advisory corrective measures in case of minor violations. It also assists complainants in more serious cases to petition the Personal Information Dispute Mediation Committee (PIDMC). In

more serious cases, the Center notifies the Communication Ministry, police and prosecutors' office of violations or incidents.

Many observers hold that the legal status of both the data protection oversight body (PDPC) and the dispute settlement body (PIDMC) should be more independent. Lawmakers and civic groups also demand that the Data Protection Act be modified so as to secure the extended applicability of the Act into the public sector, which has been regulated by the different law and governmental entity, and the institutional independence of the oversight body.

Functions of the Dispute Mediation Committee

Recently, an increasing number of plaintiffs in Korea have been resorting to alternative dispute resolution (ADR) – arbitration or mediation. Regarding the privacy issue, a separate dispute settlement body has been established under the 2001 amendment to the Data Protection Act, because disputes related with privacy could not be settled by the same procedures as e-commerce or consumer protection disputes.

If a privacy complaint cannot be readily resolved by the Personal Data Protection Center (PDPC), the injured party may file a petition with the Personal Information Dispute Mediation Committee (PIDMC). PIDMC is intended to facilitate the prompt, convenient and appropriate settlement of disputes arising out of personal data or privacy infringement. The Committee is composed of up to 15 members, appointed or commissioned by the Minister of Information and Communication from among well-qualified lawyers, IT engineers, professors, representatives of consumer organizations and IT businesses, whose term, integrity and professionalism are ensured by the Data Protection Act.

Dispute mediation proceedings may be initiated by either an injured subject or the on/off-line information service providers, and are settled free of charge. When a petition for mediation is filed with PIDMC, the Committee opens factual investigation in an informal way and proposes a settlement for agreement by the parties prior to formal mediation. If the parties fail to agree upon a settlement, PIDMC starts the mediation proceedings. After fact finding efforts through hearings, discoveries and experts' examinations, the Committee suggests a mediation proposal for an agreement by the parties within 60 days from the filing of petition. When both parties say 'yes' to the draft mediation with moderate compensation to the applicant within 15 days from the proposal, and execute the mediation record, the mediation becomes legally enforceable like an out-of-court settlement. Otherwise, each party may file a civil suit with a competent court, and the Committee may support the data subject to conduct the court proceedings with reliable evidence and its own findings. In other cases, the parties may go directly to court.

PIDMC is supported by the Secretariat within KISA, which receives petitions for dispute mediation, conducts the factual investigations, prepares the agenda for the Committee meetings and keeps its minutes. PIDMC plays an important role in protecting individual privacy in the cyberspace. As an alternative dispute settlement body, it is swift and efficient in rendering pecuniary compensation to privacy victims subject to the agreement of parties concerned.

INFORMATION FLOWS AND CONSTRAINTS

Recently celebrities have generated more than their share of privacy controversies. Ironically public appetites for sex scandals and gossip about entertainers has contributed to the popularization of high-speed internet services. The resulting incidents have contributed to the improvement of privacy legislation in the private sector.

Extreme Cases of Internet Exposures

In 1999 and 2000, the high-speed internet networks circulated pornographic videos of Ms Oh, an actress, and Ms Baik, a Korean pop singer, apparently without the entertainers' consent. Such incidents have sparked debates in South Korea. Which is the first and foremost between the individual right to privacy and the freedom of expression or citizens' right to know? Most journalists, NGO activists and academics preferred privacy to freedom of expression, and demanded effective countermeasures.

An unprecedented sensational case culminated when the so-called 'Entertainers' X-File' prepared by a research group was disseminated through an internet messenger program like MSN to the public in January 2005. The file, initially prepared for an advertisement agency, contained unconfirmed rumors and personal details of 99 entertainment celebrities. Some of these celebrities considered lawsuits against the agency, seeking damages over unauthorized release of such sensitive data.. At that time, a standing committee of the National Assembly held public hearings on how to ensure the effectiveness of a newly proposed amendment to the Data Protection Act. The participants agreed on the entertainers' right to privacy. They considered such issues as the need for consolidated data protection legislation of both the public sector and the private sector, the absence of an independent oversight body and the permissible extent of collection of personal information by private companies.

In another case, the tale of the 'Dog-Shit Girl' showed the extraordinary power of netizens. When a young lady refused to clean up after her dog in a

subway train, this scene was captured by another passenger with a digital phone camera. These photos were posted on internet bulletin boards. The homepages showing the 'Dog-Shit Girl' were bombarded with hits from netizens criticizing her action. It was like a kangaroo court, and nobody seemed disturbed about the violation of the young woman's privacy.

In January 2006, the Seoul Prosecutors' Office signaled its impatience against such netizens. This time their victim was not an entertainer. Ms Lim Su-Kyung, a former student activist who visited North Korea without government approval in 1989, lost her son in an accident. At that point, 20 or so netizens including college professors and bank officers attacked her, denouncing her as a 'red' and ridiculed her son's death. The prosecutor brought them to the court by summary indictment without formal proceedings with fine up to one million won (around US$1,000) each, on the count of defamation of Ms Lim.

Thanks to the explosive advancement of information technology, Korean citizens usually enjoy brand-new services like internet blogs, mini-homepages, on-line shopping, on-line games and chatting and so forth. But there is a dark side of abuse or misuse of personal information involved in these services, on-line defamation or personal assault among them. So far we failed to find effective remedies or deterrents.

Private Sector Privacy Laws under Total Reshaping

The division of data protection between the public and private sectors is not unique to Korea. The United States and Japan have similar set of rules (EPIC 2001, p. 4). In South Korea, the logic of these two sets of laws is quite different. State and local governments and public enterprises are seen as using personal information in the public interest, whereas the private sector is ruled by market forces and pursuit of private interest.

Since the mid-1980s, the Korean government has been building up information infrastructure in both the public and private sectors. The Act on the Expansion of Computer Networks and the Promotion of Its Utilization of 1986 was changed to incorporate the protection of privacy in a new chapter in 2001, and thus obtained the new name 'Data Protection Act'. This newly revised act sets out principles of data protection of notice and consent on the basis of informational self-determination (Schwartz and Reidenberg 1996, p. 36), the right of data subjects, the responsibility of information service providers, the possible remedies following the infringement on the personal data, etc. All these principles follow the OECD Privacy Guidelines (EPIC 2001, p. 202).

Initially these data protection provisions are applicable to on-line information service providers that use computer systems and communication networks. So this Act has yet to extend its scope of application to certain specific manual data processors that collect or use clients' data. These include

travel agencies and hotels, department stores, airlines, private schools or educational institutes; and other service providers which deal off-line with their customers' personal information.

In response to mounting pressure from civic groups, the Korean government made amendments to the substantive protections in the Data Protection Act in 2004 (Park 2006a, pp. 20–21). The data subject's consent is required for automatic data collection devices which extract email addresses from websites for the purpose of spamming, and data subjects have rights to know how their information was used or provided to third parties. The Communication Ministry may establish data security guidelines for information service providers. 'Spam breaker' software should be distributed by information service providers. The on-line information service providers are required to undergo an annual security diagnosis and audit by specified data protection consultants. The government can set standards for mandatory notices to affected data subjects, for example, in the event of security breaches. Information service providers are also required to obtain the consent of data subjects before they transfer personal information to foreign countries.

KISA and Other Authorities for Privacy Protection

KISA plays various roles under the law, including performing the Secretariat of PIDMC; devising and developing technology and countermeasures to hacking and virus-related problems; operating a peak digital signature authentication agency to safeguard electronic commerce; evaluating a diverse range of information security systems; promoting information security industry; conducting R&D on cryptographic technology; developing system and network security technology; standardizing information security technology; and staging public awareness campaigns on information security.

KISA formulates mandatory guidelines for private businesses requiring them to take precise measures for privacy and security protection. KISA is unusual among world data protection bodies, in that it combines a significant role in privacy complaint resolution with high-tech functions in relation to computer security. In 2004, KISA was admitted as a member of the International Conference of Data Protection and Privacy Commissioners.

In legal terms, the responsibility to protect personal information is taken by the Communication Ministry and the law enforcement agencies. The Ministry is in charge of formulating data protection policy and implementing the Data Protection Act. The Ministry may issue corrective orders or impose penalties on identified violators.

Police and prosecutors are also involved in privacy protection. If the violation of data protection provisions is subject to the criminal punishment, then the police investigate, and court hearings and decisions follow with appropriate

penalties. In the Supreme Public Prosecutors' Office, the Internet Crime Investigation Center devotes itself to hacking and other computer incidents, internet-based fraud, and personal data protection violations. The Cyber Terror Response Center in the National Police Agency attempts to prevent any wrongdoing or misuse of personal data and internet-based criminal activities. A victim of privacy violations may have on-line or off-line access to the above-mentioned institutions, that is, KISA, prosecutors' office or police station.

Effectiveness of Law Enforcement in the Private Sector

As the internet population surpassed 30 million in Korea in 2004 – over 70 per cent of the total population – conventional cyber-crimes including frauds in communications and on-line games decreased in numbers. But new types of cyber-crimes such as defamation on the internet or privacy invasion are on the increase.

For example, in March 2005, the lists of two million customers of CJ Home Shopping Co., a leading telemarketing company in Korea were leaked. According to police, a representative of a call center service company obtained the customer lists from a home shopping-related logistic company during several months of 2004. The lists contained customers' names, addresses, and telephone numbers.

KISA reported that internet users' complaints of privacy infringement in the private sector in 2005 amounted to 18,200, a 3.6 per cent increase over the previous year. Complaints against information service providers included failure to respond to users' withdrawal of consent; lack of any procedure for exit; unauthorized use of another's name, resident registration number or ID cards in cyberspace, and so on (PIDMC Yearbook 2005, p. 50).

How is it that these privacy protection violations continue to take place even though the Data Protection Act prohibits such activities? Is it because the sanction or punishment is so light? Is it because such privacy invasion is an everyday occurrence in this Information Society? Perhaps it is because cyberspace has become an important part of our daily life. In the Information Age, personal information is not only an intangible asset but also a valuable item to be protected from outside attacks.

CONCLUSIONS AND PROSPECTS

Though Koreans are using the high-speed internet, mobile phones and other digital devices every day, no one believes that users' ethics, usually called 'netiquette' in Korea, are satisfactory. Koreans have a long way to go to

improve their cyber-culture. As an information highway is completed, there must be appropriate traffic regulation.

Alternative ID System Wanted

Nowadays, Koreans are eager to set standard practices for newly adopted information technology. Korean practices and experiences are being closely watched by other countries because Korea is regarded as a testing ground for technological change. For example, an alternative ID system to the current resident registration number is being sought. Another suggestion is that users' real names should be used on the internet on a limited basis to prevent cyber-defamation or malicious replies on the internet bulletin board (Jeong 2005).

However, proponents of freedom of speech object to such an idea. While critics suggested several measures to prevent the unauthorized use of others' ID numbers, the government proposed an alternative ID for use in electronic commerce. In 2005, the government devised a new identification system for the internet. In a few years, on-line businesses will be required to adopt such new PIN systems instead of the controversial resident registration numbers (Chosun 2005).

Legislative Proposal of New Comprehensive Law

Notwithstanding the 2004 amendments to the existing Data Protection Act, there are campaigns to enact a comprehensive law on privacy protection from scratch. The government and legislators, in consultation with civic groups, made such proposals to the National Assembly in 2004 and 2005. The 2004 proposal was automatically repealed because of the closing of the plenary session of the National Assembly.

The three draft bills, proposed by the ruling party and two opposition parties, showed government policy and the intentions of interested groups. They are almost identical in such aspects as the classification and scope of personal information, but they differ in the nature of oversight body and applicable remedies.

All political camps agree the new act should be a comprehensive one governing both the public and private sectors. But they disagree on many points. At issue is the independence of the supervisory body. Until now two government departments conduct the overall supervision of data protection regulation: the Administration Ministry in the public sector and the Ministry of Information and Communication in the private sector. Civic groups are critical of this supervisory system because it cannot ensure the independence of the oversight body or the efficiency of privacy protection. They contend that government departments are unable to regulate themselves to protect citizens'

privacy while they are actively carrying out e-Government or digitalization projects. One of the draft bills made the supervisory body independent of all three branches of government, while others have proposed to organize it within the office of the Prime Minister. How this issue is resolved is bound to have a major influence on the future of privacy protection in Korea.

The government and the ruling party were against the reinforced punishment of privacy invasion, and the adoption of class actions other than the current ADR or litigation system. The government does not want to see an avalanche of law suits stimulated by such a new proposal, which might prevent efficient data flow. On the other hand, the civic groups are critical of the master plan of e-Government which facilitates unrestricted data flow in the public sector.

While lawmakers hesitated to deliberate the proposed data protection legislation, there took place the presidential election at the end of 2007 (Park 2007, p. 10). President-elect Lee Myung-Bak proposed a slimline government reorganization based upon the landslide victory, and the Communication Ministry will be dismantled into the Broadcasting and Communications Commission. Consequently data protection in both the public and private sector will be taken over by the Ministry of Administration and Security, and the data protection functions of KISA will be directed by the new ministry. Therefore, data protection legislation would certainly be reconsidered from the beginning on account of the reshaping of governmental functions. It remains to be seen whether the privacy protection in Korea will be reinforced or not in the near future.

Future Prospects

South Korea has achieved both economic growth and political democratization in a short period of time. Its digitization progress in technology and practices such as sophisticated home networking, e-Government projects and u-health practices well deserve worldwide attention. The Korean government and people agree on the idea that the law and practices regarding privacy protection should be in conformity with global standards.

South Korea has significant data protection legislation and, at least in the private sector, novel methods of enforcing privacy rights. Together with the Data Protection Act's coverage of information service providers, sensitive data including credit information and medical data are regulated under separate laws like the Credit Information Act and the Medical Services Act.

As Korea develops a society based upon ubiquitous sensor networks, the awareness and level of privacy protection among individuals and IT businesses are increasingly high. Take an example of RFID, an indispensable material in a ubiquitous sensor network. This burgeoning RFID industry is

being regulated by the RFID Privacy Guidelines 2005 (as amended in 2007), which requires RFID providers to notify users of the presence and functions of RFID tags attached to, or built into, goods. As a result, the concerted efforts of the government and businesses as a whole are necessary lest the new technology should invade privacy of consumers.

When regulatory measures are properly implemented, the existing data protection regime in Korea seems to reach the level of privacy protection in advanced countries. However, some practices remain below the global standards. There is a room for improvement in areas such as procedural transparency with respect to wiretapping; possible data conveyance to third parties without notice to data subjects; helpless individuals' position against spam mails, and unnoticed computer matching in the public sector.

On the other hand, different efforts on the internet real name system have been made to realize a more transparent society. For example, the Act on the Public Election and the Prevention of Election Corruption allows only the person with a real name with his/her resident registration number to list his/her opinion on the bulletin board of the internet press. Thus one cannot express one's political opinion under a pseudonym on the internet. Certainly Korea's privacy legislation will be upgraded in the midst of the tension between mounting privacy awareness and rapid technological advancement.