

Privacy Issues and Public Opinion in Korea^{*}

한국에서의 개인정보보호와 여론의 역할

Park, Whon-II^{**}
(박 환 일)

〈 Table of Contents 〉

- I. Introduction
- II. Conflict between Liberty and Security
- III. Incremental Influence of Public Opinion
- IV. National Culture and Traditions
- V. Winners and Losers
- VI. Conclusion

Keyword : privacy protection, national security, OECD Principles, resident registration number, NEIS, abuse and misuse of personal information, dispute mediation, 프라이버시 보호, 국가안보, OECD 원칙, 주민등록 번호, 교육행정정보시스템, 개인정보의 오·남용, 분쟁조정

I. Introduction

In Korea, though individual privacy is protected by the Constitution,¹⁾ this kind of fundamental right had to give way to national security under the authoritarian government until the mid-1980s. This situation is quite similar to that in the

* This article was originally prepared for the international workshop held at Belagio, Italy from January 31 - February 4, 2006 under auspices of the U.S. National Science Foundation and the Rockefeller Foundation. Its extended version will be published as one chapter of the Privacy at Forty: Eight National Histories co-edited by Professors James Rule and Graham Greenleaf.

** Associate Professor, College of Law, Kyung Hee University.

1) See Articles 16, 17 and 18 of the Constitution.

United States after the 9.11 terror attack, where the national security has gained the top priority in every sector of life.

In the 1980s, Korea saw the democratization of society, and the Seoul Olympic Games accelerated the implementation of privacy protection in line with the global standards. This became an irreversible trend since Korea was admitted to the Organization for Economic Cooperation and Development (OECD). Actually, privacy protection began as propaganda toward foreign countries, but later has been an epicenter of civic movements over the social issues keeping abreast with the democratization of the Korean society. Accordingly ordinary citizens become more aware of the importance of privacy.

Part II of this article reviews the historical conflict between liberty and security, and overall privacy protection regime of Korea. Part III looks into the specific occasion and incident which ignited the privacy issue in Korea, and describes the role of public opinion in the national controversies. Part IV examines how the public opinion interacts with data protection in the context of the Korea's culture and traditions, while Part V discovers who became winners and losers during that process. Part VI concludes which role the public opinion is supposed to take in the future.

II. Conflict between Liberty and Security

Korean society has seen the privacy issues drastically change during the past 40 years. For example, the resident registration number is no longer regarded as indispensable to national security. Initially it was considered mandatory for the purpose of national security to hold the resident registration card. Now it is often treated as Big Brother's weapon. The fate of this ID number illustrates the changing view of privacy in Korea.

1. Supremacy of National Security

With the end of the Japanese occupation (1910-45), 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 number of military strongmen.²⁾ 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 Korea. In January 1968, North Korean guerrillas infiltrated to the outskirts of the Blue House, Presidential Residence in Seoul. A few days later the *Pueblo*, a U.S. Navy intelligence ship and all its crew were seized by North Korean patrol ships in international waters. The North Korean regime continued to terrorize their 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 commercial 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 prolong his dictatorship.

2. Struggle for Democratization

Mounting demand for privacy protection enhanced people power calling for the Korean government to respect 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

2) Tom Ginsburg, "The politics of legal reform in Korea" in Ginsburg (ed) *Legal Reform in Korea*, (Routledge Curzon, 2004), pp.2-3.

President allowed a broad range liberalization. The international environment was also a crucial factor in his decision to democratize.³⁾

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, and the rights of Korean dissidents attracted worldwide attention. A turnaround took place when Korea became a member state of the OECD in 1996. To secure admission to the OECD, the Korea government promised to observe the human rights. Also, in the wake of the rising prosperity of the late 1980s, as Korea's per capita income exceeded 10 thousand dollars, human rights issues came to the foreground of public opinion.

The advent of the Information Age brought in a new dimension of privacy issues. The information highway has made it possible for the government to implement far-reaching e-Government projects. At the same time, the curiosity of ordinary people started to search and gather various information from encyclopedic knowledge to the entertainers' scandal from the Internet.

3. Overview of Privacy Protection Laws

Privacy protection legislation of Korea 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.

Accordingly, in the public sector, data protection provisions are found in several pieces of legislation, including the Act on the Communication Secrets, the Telecommunications Business Act, the Medical Services Act, and the Public Agency Data Protection Act, among others. In particular, Korea's admittance to OECD in 1996 paved the way to the full-fledged data protection laws in the public sector. Because an OECD member state is required to observe OECD rules, the Korean government adopted the OECD Privacy Principles. 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

3) *Id.*, p.4.

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.

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.

Specifically, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Data Protection Act" as amended in 2001) is generally applicable to entities or individuals that process personal data for profit through telecommunication networks and computers. Personal credit information and medical records are protected by a different specialty laws. In the first place, it is advisable to delve into data protection in the public sector.

III. Incremental Influence of Public Opinion

For the past two decades since the mid-1980s, public opinion played a leading role in democratization of Korea. And there was no exception in privacy protection. Government practices ignoring citizens' privacy have been the target of criticism of the press as well as civic organizations. Nowadays, 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.

1. 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 of communications (Art. 18). For good measure, it also provides that freedoms and rights of citizens shall not be neglected on the grounds that they are not enumerated in the Constitution (Art. 37(1)). The right of government to control these freedoms is limited 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)).

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. To put it in a concrete manner, the privacy protection is defined to maintain the confidential secrecy of an individual; to be ensured the inviolability of one's own private life; to be protected from other's intervention of such sensitive areas as one's conscience or sexual life; to be held in esteem of one's own personality and emotional life; and to preserve one's mental inner world."⁴⁾

In this regard, public opinion demanded personal information to be defined in a concrete manner in line with universal standard. The data protection rule has to protect the data subject from inappropriate access to, and abuse or misuse of, its personal information. Personal information means the data of a living person comprising sign, character, voice, sound and image, etc., 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.⁵⁾ With the advancement of information technology, the scope of such information increasingly expands to include e-mail addresses, credit card numbers, log files, cookies, GPS location

4) Constitutional Court, 2002 *Heon-Ma* 518 (*en banc*) on October 30, 2003.

5) This is a typical definition of "personal information" as provided for in Item 6 Paragraph 1 Article 2 of the Data Protection Act.

data, DNA data, etc. In this connection, individual belief, conscience, medical records, sexual orientation, race, trade union activities, criminal records are regarded as sensitive data.

2. NEIS Controversy defeating e-Government Projects

The most controversial privacy issue between the government and the public was regarding the National Education Information System (NEIS), which was proposed in 2003 to enhance the efficiency of educational administration and to improve the working condition of teachers. The Ministry of Education and Human Resources Development (the "Education Ministry") asserted that NEIS would be an efficient, technologically advanced and transparent system.

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

The National Teachers' Union (NTU) feared that their members would be put under surveillance through NEIS. Some databases were believed to contain sensitive data without any appropriate safeguards like data subject's consent or legal grounds. The NTU and other civic organizations conducted protest rallies and threatened a general strike. Disappointed by the lukewarm response of the government, the opponents 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 — teachers work, medical information and the higher-level school entrance results — be excluded from the NEIS databases.

Accordingly the Education Ministry excluded these three categories of data, keeping other 24 categories of school affairs intact. As the NTU threatened to stage all-out protests against the implementation of NEIS in November 2003, the

Seoul District Court approved the injunctive 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 examinations. A negative court order could paralyze the whole college entrance exam procedures. 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 the graduation date, contained in the NEIS databases, are necessary for the Education Ministry. Consequently, pertinent schools and institutions are entitled anytime to issue certificates of graduation. So the current NEIS databases were determined to comply with the Constitution and the relevant laws on data protection, and could be maintained.⁶⁾

3. Changing Concept of Privacy

In Korea, the right to privacy is not a firmly established legal concept in this quickly changing Information Age. Rather it is a developing, unfinished concept.

Firstly, 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."⁷⁾

6) Constitutional Court, 2003 *Heon-Ma* 282 (*en banc*) · 425 (consolidated) on July 21, 2005.

Secondly, once the right to privacy is violated, the damage can be difficult to repair. When celebrities' privacy was exposed to the public by a yellow paper, its unfound report became *fait accompli* regardless of the truth. Because a forced apology to negate the former privacy invasion or the publication of the opposite opinion could exacerbate the infringement upon the privacy, injunctive remedies are more generally granted than in the case of defamation.⁸⁾

Therefore, public opinion used to resort to the Constitutional principles to prevent the centralized management of personal information. The essential aspects of the right to privacy should be protected by every possible safeguard from laws and guidelines to contracts between the parties.

IV. National Culture and Traditions

Traditionally Korean citizens have been accustomed to authoritarian rule, but they are increasingly aware of their own fundamental rights. Though they are required to use the resident registration number in a daily life, they get to know the negative aspects of information society, i.e., abuse or misuse of personal information. During the course of democratization of the Korean society, civic groups have been very active in demanding privacy protection to the government and IT businesses. In response to such demand, the Korean government is implementing a unique remedy system that provides pecuniary compensation to alleged privacy victims.

1. 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 preferred national security and economic

7) Supreme Court, 96 *Da* 17257 on July 14, 1998.

8) Sung, S.J. et al, *CyberLaw*, Seoul: Gilbert, 2003, p.88.

growth to human rights. But democratization changed the situation dramatically. A good example is the ID system.

In Korea, every citizen is given an ID number at birth - resident registration number. This number contains 13 digits conveying information of the holder. This ID system was 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 he/she is a real person with a real name. Therefore anyone with access to the administrative databases can obtain detailed information about each holder including holder's residence, earnings and tax payments, and what kind of business he is engaged in, because the residence, tax and other government databases are constructed based upon 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 databases and to do profiling and data matching of extensive information about Korean citizens. The 13-digit number is the "master key" which opens the government databases. Because it is easy to centralize and conduct profiling citizens' data, privacy-conscious Koreans seek assurances that the ID number not be used for purposes of surveillance.⁹⁾ Several civic groups behave like a watchdog 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 percent of those who filed claims for with the Personal Data Protection Center in Seoul reported their ID numbers had been illegally used or stolen.¹⁰⁾ Against this backdrop, some critics suggested that information service providers should not be allowed to collect individual user's ID number.¹¹⁾

9) *Id.*, p.94.

10) PIDMC, *Korean Personal Information Dispute Mediation Committee Yearbook 2005*, p.50.

11) Chung, Y.S. and Kim, H.E., "Unauthorized Use of Resident Registration Numbers and Privacy Protection," *Internet Law Journal*, Vol.3 No.2, 2004, p.227.

2. Crimes abusing and misusing Personal Identity

As the identity card or NEIS is loaded with personal information, various identity crimes embarrassed the Korean society. After the financial crises in 1997, a wave of identity crimes broke out in the shadow of rapid developments of the IT industries and the enlarged gap between the rich and poor. Criminals found ways to use affluent people's personal data for their fraudulent activities or burglary. The original NEIS was dangerous because it contained students' family wealth and other information which could be used illegally by criminals. Eventually, these kinds of information disclosing students family background were deleted from the NEIS databases.

In the 2000's, burglars were reportedly chasing foreign-made luxury cars by noticing certain motor vehicle registration plates. Since the vehicle registration plate numbers identified where the car was registered, the robbers used that information in their heists. For instance, robbers threatened a female driver when she parked her car at an isolated parking lot at night. In response, the government hurried to change the format of private car plates in 2004 to remove the information of the owners' residence.

3. Privacy Agency providing Pecuniary Remedies

In Korea, pecuniary remedies pays 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, they awarded compensatory damages in 17 cases where a breach of privacy rules was found, ranging from US\$100 to US\$10,000.¹²⁾ A mere misuse of personal information case usually results in the compensation of around US\$100. The more serious the privacy invasion is, the more compensation is required as explained below. In only a few cases of breach did PIDMC recommend corrections or other

12) See PIDMC, Korean Personal Information Dispute Mediation Committee cases in WorldLII database available at <<http://www.worldlii.org/kr/cases/KRPIDMC>>.

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. She then 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 found liable for professional negligence and she was awarded 10 million won (equivalent to US\$10,750) 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 Web site. He was required to pay 4 million won (around US\$4,300). The award would have been increased if she had objected to being filmed. A translation service company posted a woman's resume on its Web site without her consent, as if she was an interpreter employed by them; the company was required to pay 200 thousand won (around US\$215) 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\$215). Taking into consideration of monetary compensation, Korea's privacy authorities regard privacy violations more seriously than any other data protection agencies in the world.

4. Self-Regulation of the Private Sector

Self-regulation does not work well in Korea. Take the example of the Half Price Plaza, an on-line vendor. The Internet shop owner carried out aggressive on-line advertisement, ensuring its members half price purchase of a number of items. In the end, the owner ran away with handsome pre-paid money. This case rang an alarm bell that on-line vendors are not always safe and credible.

There is a semi-official form of self-regulation, 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 the Internet sites and on-line businesses which are 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.¹³⁾ For example, the Association for the Improvement of E-Mail Environment, established in 2002 by direct marketing merchants, aims at coping 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.

V. Winners and Losers

The privacy issue on the Internet has produced apparent winners and losers. The Korean government has successfully implemented the e-Government projects carrying out government services through the high-speed Internet. But it had to admit some side effects of e-Government when the civic organizations successfully staged protest rallies against NEIS. Civic organizations have continuously enlarged their support bases on the privacy issue in the Information Age. As a result of slush fund investigation of former Presidents, individual's financial information is more often than not disclosed because of bribery investigation, tax examination or health insurance fraud, while individual's credit information is firmly protected by a special law. In any event, ordinary privacy victims could have a variety of remedies from the civic groups and the formal institution.

13) See Yi, C.B. and Ok, K.J., "Korea's personal information protection laws," *Privacy Law & Policy Reporter*, Vol.9 No.9, 2003.

1. 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, civic organizations have exerted considerable influence to enhance freedom in the public policy making process in Korea by participating in the various government committees or leading public opinion through mass media. The Korean political pendulum has made a full swing from the authoritarianism of past decades to today's free society. In the area of data protection, civic groups usually rated privacy issues very high in contrast to the authoritarian rulers who deemed national security and economic growth superior to human rights. Since the New Millennium, civic groups have worked to enhance public awareness of privacy protection. They provide advice on privacy issues to individuals as well as businessmen, and monitor market practices.

One of these civic organizations is the Citizens' Action Network (CAN, action.or.kr) — a non-profit NGO which encouraged citizens concerted action on the Internet to reinforce the rights of ordinary taxpayers and consumers with voluntary contribution of its members. As CAN puts its focus on the information-related rights, it operates 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, etc. 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 promoting justice and human rights in Korean society through the participation of the people, and to bringing about legal and policy reforms. Since its establishment in 1994, PSPD, along with 13 thousand members as of 2005, has been serving as a watchdog against the abuse of power and staging 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 a representative suit for the deletion of such data and damages on behalf of over 41 hundred of their former customers.

The Korea Progressive Network Jinbonet (KPN, center.jinbo.net) is an activist network for progressive ideology, i.e., enhanced human rights in the information society, anti-censorship and copyleft in the cyberspace. Occasionally it staged a campaign "e-Government hand-in-hand with Information Human Rights!" which addressed the problems of resident registration number and NEIS. Now that the electronic monitoring and surveillance of work places also raised privacy issues, they demand that installation of such systems as CCTVs, software for monitoring e-mails or the Internet usage, biometrics devices, smart cards, 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 June 25, 2004 which marked the centennial anniversary of the birth of George Orwell, the author of the novel, "1984." 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 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 number from posting any message or idea.

2. Losing Ground of Data Processors/Collectors

Personal credit information should be held confidential to others including the government. However, the demand for surveillance of transactions in the private sector is getting stronger to reduce tax and health insurance fraud. Government-maintained data matching is often called for to combine and reconcile the National Tax Database and the Public Health Insurance System and to detect fraudulent tax report by using the general identifier, resident registration number. It is an irony that surveillance is required for fiscal and security purposes while privacy protection in the private sector is stressed at the same time.

Initially, individual credit information was not the object of data protection. In the 1990s, the partially disclosed slush money of former Presidents changed the course of data flow, as investigators found the hidden transactions of ex-President Chun exploiting the underground economy. In order to avoid bank run by ordinary people for fear of all-out tax examination, the Korean government had to promise the protection of banking secrecy of individual depositors.

In Korea, individual credit information has been protected separately by the Credit Information Act since 1995 in line with the global standards that credit information should be protected like other personal information. So the individual credit information 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 court proceedings, credit information processors or users are required prove the absence of intention or negligence. The Korean Financial Supervisory Service, credit information watchdog, is empowered to supervise the operations of credit information companies. At present, credit information is fully protected separately from ordinary personal information, but in a manner in accordance with core OECD privacy principles.

VI. Conclusion

Korea's information society has developed on the basis of privacy protection rather than the national security and administrative efficiency. During the course of democratization, public opinion and the civic groups which led and organized the opinion have played an important role. At the same time, unregulated activities in the private sector gave rise to a number of ill-side effects and social problems. Though Koreans are enjoying the high-speed Internet, mobile phones and other

digital devices every day, no one agrees that users' ethical level¹⁴⁾ is satisfactory.

So the public opinion is required to function as an effective self-regulator like a compass and set in the right track of the information society. The frequently raised question is how to replace the controversial resident registration number, and establish and practice the proper privacy rules.

1. Alternative ID System Wanted

As Korea is regarded as a test bed in adopting new technologies, Korean practices and experiences are being closely watched by other countries. For example, an alternative ID system other than the current resident registration number is being sought while it is suggested that the real name should be used in the Internet on a limited basis to prevent cyber-defamation or malicious replies on the Internet bulletin board.¹⁵⁾

However, proponents of freedom of speech object to such an idea. While critics suggested several measures to prevent the unauthorized use of other's ID number, the government has proposed that an alternative ID should be used in electronic commerce. In 2005, the government devised a new identification system for the Internet access — personal ID numbers such as vertical resident registration numbers, personal identification key or certified authentication certificates issued by credit-rating agencies or certified digital signature authentication agencies, among others. Since 2007, on-line businesses would be required to adopt such new PIN system instead of the controversial resident registration numbers.¹⁶⁾

At present, it is an offense in Korea to use other person's resident registration number without the holder's permission. The newly revised Resident Registration Law, which became effective on September 25, 2006, has forced the police to decide whether a juvenile violator playing on-line games with other's ID should be punished or not.¹⁷⁾

14) It is usually called "netiquette" in Korea.

15) Jeong, J.H., "Legal Issues on the Internet Real Name System," Paper presented at a seminar hosted by the Korean Internet Law Association on December 10, 2005.

16) Chosun-Ilbo [English edition], "New Internet Identification to Protect Privacy," November 1, 2005.

17) Chosun-Ilbo, "Juvenile gamers are on the brink of becoming criminals," September 15,

2. Legislative Proposal of New Comprehensive Law

Notwithstanding the 2004 amendments to the existing Data Protection Act, there were campaigns to enact a new comprehensive law on privacy protection from scratch. The government and legislators, in consultation with civic groups, made proposals to the National Assembly consecutively in 2004 and 2005.¹⁸⁾

The three draft bills, proposed by the ruling party and two opposition parties respectively, showed the government policy and the intention of interested groups. They are almost identical in such aspects as the classification and scope of personal information, but split up 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 with respect to the proposed act is the independence of the supervisory body. Until now two government departments conduct the overall supervision of data protection regulation: the Ministry of Government Administration and Home Affairs in the public sector and the Ministry of Information and Communication in the private sector. The civic groups are critical of this supervisory system because it cannot ensure the independence of the oversight body or the efficiency of privacy protection. 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 proposal intends to strike a balance by allowing personal information to be collected to a limited extent only with consent of a data subject. And the government proposal includes the mandatory notification to data subjects of the presence of automated data collectors such as CCTVs, e-mail address extractors, etc. For the time being, these proposals are not expected to attract the attention of the majority of lawmakers owing to other impending political issues.

2006.

18) The 2004 proposal was automatically repealed because of the closing of the plenary session of the National Assembly.

3. Future Prospects

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 the worldwide attention. The Korean government and people agree on the idea that Korean law and practices regarding privacy protection should conform with the global standards.

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 the separate laws like the Credit Information Act and the Medical Services Act.

As Korea develops a society based upon ubiquitous sensor networks, the public awareness and level of data protection among the individuals and IT businesses are increasingly high. For example, industries using RFID (radio frequency identification), an indispensable material in ubiquitous sensor network, are being regulated by the RFID Privacy Guidelines 2005, which requires RFID providers to notify the users of the presence and functions of RFID tags attached to, or built in, goods. As a result, concerted efforts of the government and businesses as a whole are taken lest the new technology should invade privacy of consumers.

On the other hand, different efforts based 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. Regardless, Korea's privacy legislation appears to be headed for an upgrade in the midst of the growing tension between the mounting privacy awareness and rapid technological advancement.

References

- Chosun-Ilbo [English edition], "New Internet Identification to Protect Privacy," November 1, 2005.
- _____, "Juvenile gamers are on the brink of becoming criminals," September 15, 2006.
- Chung, Y.S. and Kim, H.E., "Unauthorized Use of Resident Registration Numbers and Privacy Protection," *Internet Law Journal*, Vol.3 No.2, 2004.
- Ginsburg, T., "The politics of legal reform in Korea" in Tom Ginsburg (ed) *Legal Reform in Korea*, Routledge Curzon, 2004.
- Jeong, J.H., "Legal Issues on the Internet Real Name System," Paper presented at a seminar hosted by the Korean Internet Law Association on December 10, 2005.
- PIDMC, Korean Personal Information Dispute Mediation Committee cases in 2005, WorldLII database available at <<http://www.worldlii.org/kr/cases/KRPIDMC>> (accessed on June 10, 2007).
- _____, *Korean Personal Information Dispute Mediation Committee Yearbook 2005*.
- Sung, S.J. et al, *CyberLaw*, Seoul: Gilbert, 2003.
- Yi, C.B. and Ok, K.J., "Korea's personal information protection laws," *Privacy Law & Policy Reporter*, Vol.9 No.9, 2003.

<Related Websites - last visited June 10, 2007>

Citizens' Action Network <<http://action.or.kr>>

Cyber Terror Response Center, National Police Agency <<http://www.police.go.kr>>

Internet Crime Investigation Center, Supreme Prosecutors' Office <<http://dci.spo.go.kr>>

Korea Association of Information and Telecommunication <<http://www.kait.or.kr>>

Korea Information Security Agency <<http://www.kisa.or.kr>>

Korean Constitutional Court <<http://www.ccourt.go.kr>>

Korean Personal Information Dispute Mediation Committee <<http://www.1336.or.kr/privacy.html>>

Korean Supreme Court <<http://www.scourt.go.kr>>

한국에서의 개인정보보호와 여론의 역할

박 환 일*

한국에서의 개인정보보호는, 헌법상으로는 사생활의 자유가 보장되고 있었음에도 국가안보와 행정편의를 위하여 유보되다가, 1980년대 중반 민주화가 진행된 다음에야 중시되기 시작하였다. 1968년 무장공비 침투사건을 계기로 주민등록제가 전면 실시되고 모든 국민의 주민등록증 소지가 의무화되면서 국가적으로 개인정보나 프라이버시 보호는 뒷전이었고, 이는 남북 긴장관계가 지속되는 동안 큰 변화가 없었다.

그러나 '6월 항쟁'의 결과 정치적·사회적 민주화가 진척되고 1988년의 서울 올림픽, 1996년의 OECD 가입으로 프라이버시 보호는 돌이킬 수 없는 대세가 되었다. 이에 따라 일반국민의 개인정보에 대한 인식이 높아져 정부가 의욕적으로 추진하던 전자정부 사업에도 제동이 걸렸다. 대표적인 사례가 교육행정정보시스템(NEIS)이다. 정부는 교육행정의 효율화를 위해 많은 예산을 들여 이를 의욕적으로 추진하였으나, 전국교원노조의 반발시위와 시민단체의 반대에 부딪혔다. 급기야는 국가인권위원회와 법원의 일부 항목 삭제 권고 및 사용 금지 가처분명령에 따라 문제의 항목을 제외한 채 별도 시스템으로 운용하기로 하고 가까스로 NEIS를 시행할 수 있었다.

이와 같이 개인정보보호에 있어서 여론은 매우 중요한 기능을 수행하고 있다. 국민들의 고양된 의식을 결집시켜 국가정책을 좌우할 수 있는 영향력을 발휘하기 시작했다. 여기에는 언론매체 못지않게 일반 네티즌들의 인터넷 통신과 휴대폰 연락이 사람들의 행동을 통일시키고 있다. 이와 함께 여론형성에 있어 시민단체(NGO)의 역할이 날로 커지고 있다. 이들은 여론의 형성을 주도하고 조직화하는 일을 한다. 시민단체는 정부기관은 물론 온라인기업, 개인들의 개인정보 침해활동을 감시하고, 피해자의 구제에도 힘쓰고 있다. 우리나라에서의 개인정보침해구제는 분쟁조정절차를 통하여 대부분 해결되고 있는데, 피해

* 경희대학교 법과대학 부교수, 법학박사.

액을 알 수 없더라도 정신적 고통에 대하여 금전적 피해보상을 하도록 하고 있다. 일반 국민들의 프라이버시에 대한 의식이 높아질수록 개인(신용)정보를 수집하고 이를 처리하는 온라인 업체들은 법의 감시를 받고 여차하면 손해배상을 하지 않을 수 없게 되었다. 개인신용정보는 신용정보법에 의하여 따로 보호를 받고 있다.

한국에서 현재 논란이 되고 있는 문제는 보편적 식별자로서의 주민등록번호를 어떻게 할 것이냐 이다. 당초의 행정목적과 관계없는 ID확인을 위해서는 그 대체수단을 사용하도록 정부기관과 시민단체들이 노력하고 있다. 앞으로 전개될 유비쿼터스 환경에서도 개인정보가 침해되지 않도록 정책적으로 유의할 필요가 있다. 특히 급속도로 보급되고 있는 CCTV나 GPS 위치정보, 휴대폰 정보는 그 편리함 못지않게 프라이버시를 위협할 수 있는 수단이 되기 때문이다. 이와 같이 개인정보보호가 중요시되고 있음에도 다른 정치적 이슈에 밀려 개인정보보호 감독기구의 독립성 확보 등을 골자로 하는 개인정보보호법의 제정이 차질을 빚고 있는 것은 안타까운 일이 아닐 수 없다.