New Legislative Proposals of Comprehensive Data Protection in Korea

Park, Whon-Il*

〈 CONTENTS 〉

Ⅰ. Was Pandora's Box open?

Where are Korea's data protection laws located compared with those of foreign countries? The writer became to understand the status in quo when he participated in an international workshop held in Bellagio, Italy in the early 2006.[1] Other participants were quite impressed by the fact that, during the past forty years, Korean people's privacy had been restricted by the authoritarian regimes in the name of national security, and came to the spotlight as human rights with the democratization of the Korean society taking place since the 1980s. Korea's

* Assistant Professor of Law at Kyung Hee University

1) Internationally well-known scholars and specialists from eight countries, e.g., Professor James Rule of the United States, Professor Graham Greenleaf of Australia and Professor Wolfgang Kilian of Germany among others, gathered in the Rockefeller Study and Conference Center in Bellagio, Italy during the period from January 31 to February 4, 2006. They discussed the current issues and prospects of data protection from the perspective of each country, and collaborated to publish a book *Privacy@40: A Comparative Study of Eight Jurisdictions* in 2006.

admittance to the Organization for Economic Cooperation and Development (OECD) in 1996 paved the way to the data protection legislation in both public and private sectors. Also NGOs' activities contributed to the fundamental changes of "e-Government projects" including the controversial National Education Information System (NEIS).

Really there have been a series of dramatic events regarding data protection in Korea. The most conspicuous thing, however, is that South Korea is an almost unique country that implements an ID number as a general identifier. In fact, the residence registration number is a kingpin in establishing and managing the government databases from social security to banking and taxation. But the Australian government failed in adopting the so-called "Australia card" in the late 1980s. The efforts of some other states to implement the ID card were also aborted by the opposition groups. Then was "Pandora's box" open exclusively in Korea? Did South Koreans cross the bridge of no return?

As observed by each participant in the workshop, the history of privacy protection, its cultural background and tradition and data protection laws and regulations vary from state to state. It resulted from the different situation of each country including government policy, political landscape, public opinion and civic group activities regarding the privacy issues. For example, in European countries which experienced the two world wars and fascism, data protection is meant to fundamental rights, as envisaged in the Universal Declaration of Human Rights (1948) and the Council of Europe Convention on Privacy (1981). Across the Atlantic, the United States used to leave the privacy issue to the market with no oversight body in existence even though the notion of "right to privacy" was first acknowledged in America. Since 9/11 terror attack, federal government's surveillance has been stepped up in a war against terrorism in the United States.

So the eye of storm of data protection laws in Korea seems to be how to treat the residence registration number. If this ID number is used by the government databases to a large extent as a universal indentifier, the government becomes to know too much about its citizens like an Orwellian "Big Brother." As a matter of

fact, the smart card proposed by the government in the late 1990s fizzled out, and the NEIS system has been drastically modified.

On the other hand, personal information is increasingly traded cross the border. So far international standards have been established to promote and facilitate the trans-border data flow by the OECD, the European Union, the United Nations, etc.

In this context, this article will discuss the legal framework of data protection in Korea and major contents of the newly-proposed draft Data Protection Act, and its prospects.

Ⅱ. Current Legal Framework of Data Protection

Constitutional basis

The Korea's Constitution provides for the protection of secrecy and liberty of private life, or privacy. Article 17 of the Constitution states that all citizens shall be entitled to the inviolable right to privacy. It purports to ensure every citizen the right to control and determine his or her own personal information.

〈Table〉 Data Protection Legislation in Korea

Area	Current Statutes
General	· Residence Registration Act (1962) · Postal Services Act (1972) · Act on the Protection of Personal Information Maintained by Public Agencies (1994) · Framework Act on Electronic Commerce (1999) · Digital Signature Act (1999) · Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.(2001) · Act for the Promotion of Digitalizing Administrative Works to Realize e-Government (2001) · Act on the Consumer Protection in Electronic Commerce (2002)

Electricity & Communications	· Telecommunications Business Act (1991) · Act on the Protection of Communications Secrets (1993)
Banking & Finance	· Act on Real Name Financial Transaction and Protection of Confidentiality (1997) · Act Relating to Use and Protection of Credit Information (1995)
Industries	· Act on the Prevention of Unfair Competition and the Protection of Trade Secrets (1991) · Act for the Automation of Trading Operations (1991)
Medicine	· Medical Services Act (1973) · Act for the Prevention of AIDS (1987) · Act on Emergency Medical Cares (1994) · Act Concerning Medical Engineers, etc.(1995) · Citizens Health Insurance Act (1999) · Epidemic Prevention Act (2000)

Note: Figures in parenthesis represent the year when the privacy protection clause was codified for the first time in the act.

In line with the Constitutional provisions, there are specific sectoral laws regulating data protection or confidentiality of the subject. For example, the Act on the Communications Secrets, the Telecommunications Business Act, the Medical Services Act, the Act on the Protection of Personal Information Maintained by Public Agencies (the "Public Agency Data Protection Act"), provide for the protection of personal data in general. In addition, the Act Relating to Use and Protection of Credit Information (the "Credit Information Act"), the Framework Act on Electronic Commerce, the Electronic Signature Act, etc. have contained the data protection provisions for the respective purposes. For example, the Framework Act on Electronic Commerce requires that electronic traders shall not use, or provide to any third party, the personal information collected through electronic commerce beyond the alleged purpose for collection thereof without prior consent of the data subject or except as specifically provided in any other law.

Specifically in the private sector, the existing Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the

“Data Protection Act”) is applicable in general. This Act protects only the living natural person, not the dead nor the corporation. The target of the Act deems to be the person who is doing business of collection, processing, storage, retrieval, transmission and receiving of personal information (the "information service provider") for commercial use. And credit reports are protected separately by the Credit Information Act.

Despite the far-fetched legal framework on privacy, it is argued that Korean legislation is somewhat several steps off the global standards. Someone points out that data protection laws should regulate both public and private sectors, and empower an independent supervisory body for privacy protection.

Against these backdrops, the newly-proposed draft bills on data protection are supposed to be a comprehensive one regulating both public and private sectors, and to put an independent oversight body in place, though its nature differs a little bit by proposals.

Latest amendments to the data protection laws

As the information technology and new security systems are widely used, ordinary people are increasingly concerned about privacy issues. Some districts of large cities are closely watched by closed circuit televisions (CCTVs) to prevent crimes. So civic organizations claim that pedestrians should be notified as "CCTV Installed Area." Likewise it is illegal that a hidden camera is operated without a consent of the subject.

Public opinion goes further in terms of privacy-sensitive issues. A data subject is entitled to demand access to its personal information, correction of false information and cancellation of wrongful information. The scope to collect personal information should be minimized and the collection procedure must be strictly observed.

Since public opinion thwarted the unlimited implementation of NEIS, the privacy impact assessment (PIA) system should set in with respect to the privacy

issue before state-of-the-art technologies or systems are introduced. So any collector of personal information is required to submit the PIA result to the oversight body.

Without doubt, it is a national goal to achieve the privacy protection while pursuing the advancement of information technologies in the "Information Age." We can expect the completion of e-Government projects within a few years to come. So the data protection should be kept abreast with such developments.

In the private sector, there have been some significant achievements. In particular, mounting pressures from the civic organizations as well as academic circles drove the Korean government to amend the Data Protection Act in 2004 as follows:

a. Data subject's consent is required for the automatic data collection devices.

When the information service providers want to obtain the consent of a user, they shall notify the user of the installation, operation or denial of the automatic data collection devices including the Internet log-in data files, or stipulate such matters in the general terms of their services.

b. User's right is confirmed with respect to the provision of his personal information.

Any user may demand the specification from information service providers in which the providers describe how they have used the personal information of the user or which personal information they have provided to the third party. And information service providers are required to take the necessary steps to meet such demand promptly.

c. A petit panel for the dispute mediation is newly established.

In order to facilitate the dispute settlement, the Personal Information Dispute Mediation Committee will put some personal information disputes to a petit panel which is composed of five or less Committee members.

d. A protection guideline is to be implemented.

The Minister of Information and Communication (MIC) may establish protection guidelines for the security measures of the information communications network to enhance the security of the networks, and advise information service providers to observe the guidelines. It is mandatory for the nation-wide information service providers.

e. A security diagnosis of data protection is mandatory.

Information service providers and Accumulated Information Facilities Operators are required to undergo a security diagnosis by specified data protection consultants with respect to their own information networks or facilities in accordance with the data protection guidelines every year.

f. Data protection measures may be advised for data subjects.

MIC may establish some standards necessary for the data protection and advise them to data subjects. In case of a possible incident or breakdown of information communications network, major information service providers may give an advice on data protection measures to users in accordance with the general terms and conditions of their services.

g. Spam breaker software may be distributed for free.

MIC may develop and distribute for free the software or program to stop or report to the authorities the unsolicited commercial e-mails for profit.

h. Trans-border data flow shall be protected.

Information service providers shall not make an agreement in violation of data protection provisions under the Data Protection Act. They are required to obtain the consent of data subjects before they transfer personal information to foreign

countries, and take data protection measures according to the Enforcement Decree of the Data Protection Act.

i. Data protection provisions are applicable to entrusted data processors.

Data protection provisions of the Data Protection Act have been applicable to such off-line data collectors as department stores, travel agencies, hotels, airlines, educational institutes, etc.[2] These provisions are to be applied extensively to the data processors entrusted by the information service providers.

j. Attempted invasion upon information communications network is to be punished.

An attempted invader without authorization or over-authorized capacity upon other's information communications network with illegal purposes is to be punished by imprisonment of less than three years or fines of less than 30 million won (equivalent to US$30 thousand).

Characteristics of the existing Act

Under the Data Protection Act, information service provider's collection, out-of-purpose use and onward transfer of personal data to a third party shall be subject to the consent of data subjects. So data subjects have got a controlling authority over their own personal data when those information service providers are going to utilize the data beyond their prior notification or the purposes specified in the general conditions for use, or convey them to a third party.[3]

---

2) EU Directive (95/46/EC) on data protection also covers manual filing systems the content of which is structured according to specific criteria relating to individuals allowing easy access to the personal data.

3) There are several exceptions to this principle. In case data collection is necessary to perform the contractual obligations regarding information and communication services, to calculate the charges for such services, or to conduct statistical works, academic research or market survey without exposing any individual particulars, and where other laws demand the

Also data subjects are entitled to withdraw their consent. When receiving the data subjects' withdrawal notice, the information service provider shall immediately take necessary measures to destroy such obtained data or to suspend the out-of-purpose use.

Data subjects may request access to their own personal data maintained by information service providers, and correction of any error or false information included therein.

When the information service provider intends to gather the personal data from children under the age of 14, it shall obtain the consent from a relevant legal representative, i.e., parents, or to utilize and convey such information to the third party. In this case, the information service provider may ask for the necessary minimum information, including the name, etc. of the legal representative without his/her prior consent, for an agreement with the legal representative.

The legal representative of children may request access or correction of children's data. When receiving legal representative's request for correction, the information service provider shall cease to utilize or convey such false information until the necessary correction is made. Also the legal representative may withdraw his/her consent to the collection, out-of-purpose use or onward transfer of children's information to a third party.

The flood of such spam mails made the government to amend the Data Protection Act in which such spam mails for profit could be denied. No one is allowed to send direct marketing (DM) e-mails for profit contrary to addressee's explicit refusal of such DM mails. Anyone who sent spam mails for profit against the explicit denial shall be fined up to 30 million won. The new amendment calls for the title of mail shall be "AD" or "DM." The content should include an explanation on how to deny the unsolicited mail, the source where the e-mail address is collected, and some useful information on the sender's name, telephone number or e-mail address. Also it is subject to fine to take technological measures

---

disclosure of personal information, there is no need of data subjects' consent.

to avoid the denial or withdrawal, to generate automatically receiver's e-mail addresses or to register automatically e-mail addresses for DM. It is at the cost of DM senders to process a refusal notice.

In the event that a data subject suffers any damage by the information service provider violating the data protection provisions, such data subject may claim the compensation for damages against the information service provider. In this case, the information service provider shall be responsible if it fails to prove non-existence of its intention or negligence of such violations. Claims for damages may be filed with the Personal Information Dispute Mediation Committee or the court.

An information service provider is required to collect personal data to the minimum within the purposes indicated. In this case, the information service provider shall not refuse to provide services to the user who declined to give other information than the minimum requirement. No sensitive data regarding political opinions, religious or philosophical beliefs or past history of health problems shall be gathered for any purpose, except when the data subject agree or other laws demand such information.

The information service provider is required to notify or inform explicitly its users of how users' personal data are processed by the Act to ensure the controlling authority of such users. In so doing, such users are capable of controlling their own personal data.[4)]

At the time of business transfers or mergers and acquisitions (M&As) which

4) At the time of collecting personal data, the information service provider shall notify the followings to users or explicitly in the general conditions for use (art.22 and art.10 of Enforcement Decree):
- the name of personal data manager, department, title and telephone number or other contact means of the information service provider;
- particular personal data items to be collected by the information service provider;
- the purposes of collection and utilization of personal data;
- the period of maintenance and utilization of personal data;
- the name of beneficiaries, purposes and contents when the personal data are conveyed to the third party;
- necessary information on how to request access to and correction of personal data; and
- the ways and means how to withdraw the consent or membership.

include personal databases between the parties, the transferor or transferee shall notify data subjects of the details.[5)]

In case that the information service provider entrusts the third party to process the collection, handling and maintenance of personal data, the information service provider shall notify the data subject of such fact. In this case, the information service provider is responsible for any damages which the authorized third party caused in violation of data protection provisions, as the third party is deemed to be the information service provider's employee. The information service provider may utilize or convey to the third party personal data beyond the purposes indicated at the time of collection only if the data subject consented thereto.[6)]

An information service provider shall promptly take necessary measures when data subjects' request access to or correction, if there is false information, of their own personal data. In this case, information service provider shall cease to utilize or convey such false information until the necessary correction is made. The information service provider shall, in no case, make it more difficult for data subjects to request withdrawal of consent, access to, or correction of, personal data than to collect such data.

The information service provider shall take necessary technological and managerial safeguards to secure safety lest personal data should be lost, stolen, leaked out, altered or damaged. The information service provider shall nominate the personal data manager or chief privacy officer (CPO) who safeguards personal data and deals with complaints from data subjects. The CPO may be elected among the officers or heads of departments handling personal data or dealing with complaints

5) Notification shall include:
- For the transferor, the ground (ex. business transfer or M&A) for such transfer of database, and the name, address and telephone number of the transferee; and
- For the transferee, the fact of transfer of database, the name of the new information service provider; the name of personal data manager, department, title and telephone number or other contact means of the new information service provider; the purpose for utilization; particular personal data to be received; necessary information on access to or correction of personal data; the period of maintenance and utilization of personal data.

6) There are some other exceptions. *See supra* note 3).

from the data subjects.

Ⅲ. New Legislative Proposals

Notwithstanding the above amendments to the existing Data Protection Act, there were movements for the enactment of a comprehensive law on privacy protection from scratch. The government and lawmakers made proposals to the National Assembly in 2004 and 2005. Three draft bills are almost identical in such aspects as the classification and scope of personal information, but significantly different in the nature of supervisory body and applicable remedies. In the course of political ups and downs in 2005, two draft bills were withdrawn.

Comprehensive Law on Data Protection

Until now privacy protection in the public sector has been conducted in a systematic way, the situation is somewhat different in the private sector. It's because the privacy protected by the Data Protection Act is in principle limited to the personal information as collected and used through the information communications network. And further to this limitation, other act, for example, the Medical Service Act which provides for only "confidentiality," is insufficient for the privacy protection.

As for the secured remedies to privacy infringement, an oversight body with full power and authority to investigate facts and to do corrective orders would be required. And the privacy impact assessment (PIA) might be necessary so as to analyze and eliminate the risk factors. The process of evaluation and certification of businesses could be introduced. These improvements seemed to be identical with the global standards including the EU Directive (95/46/EC).

As a result, the government is committed to establish a new provisions of the act as follows by separating and integrating the data protection provisions of the

existing Data Protection Act:[7]

- The scope of application is expanded to cover the person or entity that collects data for profit and processes and uses the data by means of the information communications network, computer systems, CCTVs and other electronic devices;
- To formulate a comprehensive policy for data protection in the private sector and to run the Personal Information Protection Committee;
- To protect personal information collected from others than the data subject;
- The cases of emergency rescue, required payment of over due tariffs, etc. are further exceptional to the prohibition of onward transfer of personal information;
- To establish and run the Data Protection Committee;
- To adopt the privacy impact assessment (PIA) system; and
- To clarify the nature of a comprehensive law; provided, however, that the Act is not applicable to such institutions as banks, securities companies, insurance companies, etc. subject to the Credit Information Act and the Act on the Establishment of Financial Supervisory Body.

Different Views and the Latest Developments

Against the government efforts to formulate a new comprehensive act, civic organizations as well as opposition lawmaker Roh Hoe-Chan made another framework law and submitted the draft bill to the National Assembly in 2004. In this connection, the Presidential Committee made a different proposal integrating the initial government bill separating the public and private sectors, while the Ministry of Government Administration and Home Affairs (MOGAHA) prepared a

7) Inside the Administration, originally two different bills were proposed by MOGAHA and MIC. But they were consolidated in a single draft bill of the Presidential Committee which called for a comprehensive law on data protection. Government officials saw the sectoral laws are not sufficiently strong in privacy protection to survive the opposition to such attempted but frustrated government proposals as smart ID cards, NEIS, the mandatory real name uploading on the Internet bulletin board, etc.

draft amendment to the existing Public Agency Data Protection Act, which would modify the responsibilities of public agencies to destroy the personal data files, the appointment of chief privacy officers, etc.[8)]

As a result, in autumn 2004, four draft bills on data protection were filed with the National Assembly and gave rise to fiercely competitive debates.

First, the proposal of civic groups suggested the followings:

- An independent oversight body shall be established;
- A class action shall be available to the individuals affected by privacy invasion;
- An injunctive motion against information service providers which use personal information shall be provided to the data subject;
- The adoption of the PIA system and the appointment of CPOs shall be necessary for the prevention of abuse or misuse of personal information; and
- The level of sanction against privacy protection violations shall be upgraded from negligence fine to penal punishment.

IT business circles and government officials were critical of such proposal because the independent oversight body is granted so much authority to hinder the IT industries, and the suggested registration of personal data files, class action, privacy impact assessment need further discussions among citizens and national consensus.

As a result, all the camps agreed the new act is of a comprehensive nature governing both the public and private sectors. But they contended in the following details:

- The Presidential Committee asserted that the supervisory body should be established inside the Administration preferably under the National Human Rights Commission (NHRC), because the wholly independent body proposed by civic groups costs too much in terms of budget and personnel;[9)]

8) Further information of the Presidential Committee on Government Innovation and Decentralization is available at http://www.innovation.go.kr.

9) The initial draft bill of the Presidential Committee was supposed to establish the Data

- The government proposal allows personal information to be collected to a limited extent only with consent of a data subject, in accordance with the provisions of relevant law, or for the achievement of the purpose of legal transactions;
- The government proposal includes the mandatory notification to data subjects of the presence of automated data collector such as CCTV, e-mail address extractor, etc.;
- The government and the ruling Uri Party were against the reinforced punishment and the adoption of class action; and
- The civic groups are critical of the master plan of e-Government which facilitates data flow in the public sector, but might cause personal information exposed to the public.

In April 2005, the draft bills except the civic group's proposal were withdrawn from the agenda of the Legislature on account of insufficient discussions. Later the government and the ruling Uri Party modified the initial bill by establishing an independent oversight body under the Prime Minister, which will control personal data including finger prints and DNA information. The Committee members would be composed of nine persons in total, of whom three are recommended respectively by the President, the Chairman of the National Assembly and the Chief Justice. The Committee is to improve and implement law and regulations on data protection, to afford appropriate remedies and to carry out international cooperation and support of civic organizations. Under the draft bill, idea, belief, physical information, medical records, etc., classified as sensitive data, are restricted in collection, and deserve specific technological and managerial safety measures. Their contents are required to be notified to data subjects.[10)]

Protection Committee under NHRC for the purpose of systematic and consistent execution of data protection. Then NHRC could render appropriate corrective advice, indictment or disciplinary recommendation to the violators of data protection provisions. However, NHRC declined to take up such responsibility as a data protection watchdog, so the initial bill had to be modified.

Form and Nature of Data Protection Supervisory Body

At present, the overall supervision of data protection is staged by two government departments: MOGAHA in the public sector and MIC in the private sector. The civic groups are critical of the supervisory system because it could not ensure the independence of the oversight body and the efficiency of privacy protection. They contend that government departments cannot regulate themselves to protect citizens' privacy while they are actively carrying out the e-Government or digitalization projects.

The newly proposed draft bills on data protection have clarified this: One bill put the supervisory body independent of three branches of the government, while others have proposed to organize it at the Office of the Prime Minister or NHRC.

Here at issue is the purpose of data protection. If it is to secure technological ways and means to prevent privacy invasion, the function may be successfully performed by a government body with technological advantage. If any threat to privacy amounts to the infringement upon the human rights, the function has to be carried out by NHRC. If one believes that privacy protection is in nature independent of the government function, it must be a wholly independent body. Looking at several precedents of foreign countries, we can find the name and powers of the privacy protection body vary widely country by country. Some countries call it a Commissioner, others an Ombudsman or Registrar. A number of countries including Germany and Canada also have offices on a state or provincial level.[11] It depends on the social and historical background concerning the importance of data protection rather than the government organization.

In Korea, privacy or data protection is concerned about the nature of human rights insomuch as it was usually placed next to national security and public order under the authoritarian regime. Therefore, at issue is the position of privacy oversight body in the context of government organization.

---

10) Digital Times, May 31, 2005.

11) Electronic Privacy Information Center, *Privacy & Human Rights, An International Survey of Privacy Laws and Developments,* 2001, p.12.

The government prefers the supervisory body under the Prime Minister, saying that independent body calls for additional over one hundred officials and considerable budget to take over the job. But civic groups represented by the Democratic Labor Party lawmaker Roh Hoe-Chan contend that the oversight body should be an independent one apart from the government because the supervisory function over the activities in the private sector could not be well performed under the Prime Minister's umbrella.

Of course, there are pros and cons of these two proposals which will be decided by the National Assembly in the near future. Critics of the independent body worry over the possibility of the unconstitutionality and weakened authority in privacy protection.

In Korea, the unique situation where the free society equipped with sophisticated IT devices is confronted with the warlike regime in the North would limit the scope of discussions. While the government wants to know everything of citizens on account of national security and public welfare, civic groups and opposition parties tried to prevent the misuse of citizens' private information by the government, and warned of the advent of a Big Brother society. Therefore, it is more meaningful whether the proposed oversight body is ready to protect the privacy of ordinary people in an information society and to make available to them appropriate remedies and redress in case of privacy infringement. Its organizational position and budget are the next question.

Compliance with Global Standards

As Korean citizens and enterprises are getting more and more internationalized, trans-border data flow is explosively increasing. In particular, EU member states are prohibiting data transfer to the third country which fails to ensure an adequate level of data protection in accordance with EU Directive on data protection (95/46/EC).[12] At present, with the consent of data subjects data flows are not so much obstructed,

12) Available at http://europa.eu.int/comm/justice_home/fsj/privacy.

but the Korean government is preparing necessary measures to meet the EU standards. On the other hand, the government has kept a close eye on any possible outflow of national's personal information maintained by multinational companies and foreign banking institutions to a third country with less satisfactory level of data protection.

At the same time, the government takes an initiative to lead discussions on privacy protection at the international conventions and to form a privacy steering group in the APEC Tel. Also it should be noted that, in September 2004, the Korea Information Security Agency (KISA) was admitted as a member to the International Conference of Data Protection and Privacy Commissioners. Another applicant, the Homeland Security Department of the United States, failed to become an official member of the Conference. Its membership committee rated KISA's efforts very high because KISA:

- has energetically conducted research into privacy protection in Korea;
- has received reports and given advice on incidents of privacy invasion through an emergency call of 1336;
- has published white papers on personal information protection every other year; and
- has provided actively customers with technological assistance on data protection.

KISA is also arranging international cooperation with other countries to prevent unsolicited commercial e-mails. It has made a series of MOUs for the exchange of information with privacy protection bodies of the United Kingdom, Canada, Australia, etc. KISA is well versed in the changing technologies of communications and surveillance - tapes, photography, tracking of digital communications, and so on to enhance privacy protection.

Ⅳ. Other Considerations

As the Internet population surpassed 70 percent of the whole population for the first time in Korea in 2004, the conventional cyber-crimes including frauds in communications and on-line games decreased. But new types of cyber-crimes such as defamation on the Internet or privacy invasion are on the sharp increase.

Incidents Regarding Data Protection

KISA said the Internet users' report of privacy infringement in the private sector in the first half of 2004 amounted to 12 thousand, 44 percent increase over the same period of the previous year. The reported invasion upon privacy was listed from information service providers' no response to users' withdrawal of consent, no procedure at all of exit, unauthorized use of other's name, residence registration number or ID cards to cyber-defamation, etc.

How come 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 a everyday occurrence in this Information Society? There must be something not to resist in doing business or playing games in the cyberspace.

In the Information Age, personal information is not only intangible assets but also valuable objects to be protected from outside attacks. We have to be cautious not to submit our personal data just for simple data searches or for meaningless sweepstakes. In oder to curtail privacy infringement, we have to think whether or not our personal information is appropriately priced, not to mention taking necessary measures and proper legislation.[13)]

Now the debates on the residence registration number are almost over. The government is going to introduce an alternative ID as early as possible. Therefore

13) Eun-Jeong Lee, Legal Advisor to the National Assembly, Financial News, August 30, 2004.

we need not write in our residence registration number any more when applying for a membership of the Internet portal site or game site.

Lawmaker Lee Eun-Young, former professor of law, of the ruling Uri Party made a suggestion to revise the current Data Protection Act, which would be effective until a new comprehensive data protection law is enacted, as follows:[14)]

- Anybody that collects personal information without the data subject's consent is subject to harsh punishment of imprisonment up to three years or fines up to 30 million won;
- Private companies as well as national agencies are restricted to collect privacy-sensitive personal information and to use them for other purposes than data subjects consented for;
- Such privacy-sensitive personal information as DNA data, medical records, marital status, etc. is classified as highly sensitive data, whose collectors orprocessors are required to take strict leakage preventive measures; and
- National agencies and private companies shall not ask users to submit residence registration numbers just for identification.[15)]

Reinforced Regulation against Spam

Nowadays electronic commerce on the Internet is largely conducted by small businesses. These small office, home office (SOHO) businesses usually take to the Internet via unsolicited commercial mails, i.e., spam. So it is not desirable to block altogether such spam mails.

The Korean government tried to cut down spam receiving by 50 percent through draconian regulations and Spam-preventive technologies. MIC once considered even

14) Dong-a Ilbo, May 30, 2005.

15) The Korean society is getting more and more sensitive to the residence registration number. The recent happening took place on the Web site of a government agency. In April 2005, the Financial Supervisory Service disclosed negligently for several hours the personal information including the residence ID number of major shareholders of large companies at its Internet data room. In practice, the private data used to be represented by "*", but computer systems couldn't do the job accidently.

shutting down port 25, the gateway of spam, which is usually used for the Outlook Express mail client-server.

There are two ways in curtailing unwanted messages, i.e., "opt-in" and "opt-out." In order to block spam messages via mobile phones or facsimiles, the opt-in method which allows sending messages subject to prior consent of the recipient is effective.

In fact, under the newly amended Data Protection Act which came into force on March 31, 2005, the government has fined advertisers who send text messages or call customers for promotions without receiving prior consent. The new regulation applies to mobile phones, fixed-line phones and fax, but not e-mail. Automated telemarketing calls are prohibited. For calls made in person, marketers are only allowed to call customers who have consented to such advertisements on their Web site. MIC is working more easily with prosecutors and police in its crackdown on unwanted advertisements because, under the opt-in system, advertisement through the designated device proves illegal. And violators would be fined up to 30 million won (equivalent to U$30 thousand). Even if customers have agreed to receive promotional phone calls, advertisers must receive additional permission from them if they want to send text message ads between 9 p.m. and 8 a.m.[16)]

MIC urged the mobile phone companies to revise the general terms like "Unlawful spamming would cause the termination of services," and to sincerely respond to users' calling for "No more receiving 060 calls."

16) Until then, advertisers were allowed to contact customers unless the customers asked them not to. Citizens were complaining their lines were busy with advertisements offering credit card loans or real estate deals, and 060 calls on sexual content. Advertisements in these three areas made up about 90 percent of all mobile spam ads. JoongAng Daily, March 30, 2005. However, the regulation does not apply to enterprises subject to door-to-door sales or electronic trade laws, such as companies that do direct sales in school papers, cosmetics or water filters.

Ⅴ. Conclusion

It is imperative to ensure the appropriate protection of personal information so as to encourage e-commerce and trans-border data flow to and from South Korea. On the other hand, it is necessary to upgrade the international cooperation in the IT-related areas with the less-developed countries. For example, entering into call center agreement with a foreign data processor in a country without any legislation on the appropriate data protection, Korean IT industries are required to pay attention to secure proper safeguards on data protection.

When Pandora's box was open, the last item inside the box was "hope." In Korea, the scope of use of the controversial ID number should be constrained to such original purpose as administrative use while an alternative ID number is being sought. The recent U.S. counter-measures like biometrics passport after the 9/11 terror attack show us the resemblance to the Korean experiences in the 1960s and 1970s.[17)]

At the same time, the Korean government efforts to provide appropriate remedies to the damaged Internet users, and to curtail unwanted spam mails should be acknowledged. South Korea has exerted itself to enhance the data protection throughout the Asia-Pacific countries by playing a leading role in establishing the APEC Privacy Framework. In this context, the aforementioned draft bills should be processed in due course because real implementation could stop the violation of privacy and ensure the successful cross-border e-commerce.

17) In the 1960s and 1970s, the restriction to the right to privacy was legitimatized on account of the North Korea's present threat to the South, Korean people's traditional respect of the Asian values, and the unique Korean mentality about self-centered privacy protection. For example, ordinary Korean citizens say, "As far as data protection is concerned, I'm OK when I lose nothing even though someone else is in trouble." So they are aggressive in criticizing other's wrong doings on the Internet in so far as they are not affected by it.

References

EPIC and Privacy International, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments,* Electronic Privacy Information Center Washington, DC, 2001.

KISA, *2003 Personal Information Protection White Paper,* Korea Information Security Agency, January 2004. (in Korean)

Park, Whon-Il, *A Study on the Data Protection Measures in line with EU Directive,* November 2001 (in Korean).

_____, *Survey of the Level of Data Protection in Korea based upon the Global Standards,* December 2002. (in Korean)

_____, "The Data Protection Legislation in Korea," *The Internet Law Journal,* No. 1, Korea Internet Law Association, June 2002.

Rule, James et al, *Privacy@40: A Comparative Study of Eight Jurisdictions* (forthcoming in 2006).

Schwarts, Paul and Reidenberg, Joel, *Data Privacy Law,* Michie, 1996.

Sung, Sun-Je, *CyberLaw,* 2003. (in Korean)

UNESCO Korean National Commission, UNESCO Proceedings of the *International Forum on Privacy Rights in the Digital Age,* Seoul, 27-29 September 2005.

Yi, Changbeom and Ok, Ki-Jin, "Korea's personal information protection laws," *Privacy Law & Policy Reporter,* Vol. 9, No. 9, 2003. (in Korean)

Lee, Eun-Jeong, Financial News, August 30, 2004.

Digital Times, May 31, 2005.

Dong-a Ilbo, May 30, 2005.

JoongAng Daily, March 30, 2005.

PIDMC cases, Korean Personal Information Dispute Mediation Committee cases database on WorldLII at <http://www.worldlii.org/kr/cases/KRPIDMC>

새로운 개인정보보호법 제정의 움직임

박 훤 일*

우리나라는 OECD 가입을 계기로 OECD 프라이버시 보호원칙에 입각한 개인정보보호법을 공공부문과 민간부문으로 나누어 시행하고 있다. 그러나 EU 개인정보보호지침 등의 국제기준에 비추어보면 다소 거리가 있다.

이에 따라 정부와 시민단체에서는 공공부문과 민간부문을 아우르는 개인정보보호에 관한 일반법을 제정하기로 하고 각기 의원입법 형태로 국회에 법안을 제출하였다. 그러나 구체적인 내용에 있어 차이가 있는 데다 절충안의 도출이 어려워 아직 본격적인 법안 심의에도 착수하지 못하고 있다.

다만, 개인정보와 관련하여 시급히 개선을 요하는 사항은 2004년과 2005년에 꾸준히 개정작업이 진행되었다. 예컨대 2004년에 개정된 정보통신망법의 주요 내용을 보면, 자동적인 개인정보의 수집 시 이용자의 동의를 얻게 하고 정보통신서비스 이용자가 서비스제공자에 대하여 제3자 제공 등의 명세를 요구할 수 있도록 하며, 소액분쟁은 5인 이하의 조정부에 의한 신속간이 절차를 통해 해결할 수 있게 하였다. 또 스팸차단 소프트웨어를 무상 보급하고, 개인정보를 침해하는 내용의 국제계약을 체결하지 못하게 하며 정보통신망 침입행위의 미수범을 처벌하는 등의 개정이 이루어졌다.

국회에 제출되어 있는 개정법률안의 핵심 내용은 개인정보피해구제의 실효성을 확보하기 위해 사실조사권 및 시정명령 등 실질적 권한을 갖는 개인정보보호 감독기구를 두는 것이다. 정부안에서는 당초 인권위원회 산하에 두는 것으로 하였다가 동 위원회의 반대로 국무총리실에 두는 것으로 수정하였다. 아울러 개인정보의 침해요소를 사전에 분석하고 제거할 수 있는 '개인정보사전영향평가(PIA) 제도' 및 사업자의 평가·인증 시스템의 도입을 요한다. 다만, 이

* 경희대학교 법과대학 조교수, 국제법무대학원 인터넷법무학과 주임교수

법의 일반법적 성격을 명확히 하고, 신용정보보호법 및 금융감독기구의 설치에 관한 법률 등에서 정하는 감독기구의 검사를 받는 기관(은행, 증권사, 보험사)에 대하여는 적용을 배제하기로 하였다.

이에 대하여 시민단체들은 민주노동당 노회찬 의원과 공동으로 법안을 마련, 국회에 상정하였다. 이에 따르면 개인정보보호를 위한 전담독립기구를 설치하는 외에 개인에게 집단소송권과 개인정보 이용중지청구권을 부여하고, 현재 과태료 수준인 개인정보 침해 행위에 대해 형사처벌까지 가능토록 처벌기준을 강화한 것이 특징이다.

그러나 동 개정안은 개인정보보호기구에 너무 과다한 권한을 주고 있으며, 과도한 규제로 오히려 관련산업의 발전을 저해할 수 있고, 개인정보 DB 등록제도와 집단소송제, 사전영향평가제 등은 좀 더 시간을 두고 검토해야 한다는 비판이 제기되고 있다. 아무튼 전자정부, 전자상거래의 발전을 위하여는 법개정이 시급한 실정이다.

Key Words: personal information, data protection, privacy, OECD Principles, dispute mediation, oversight body, spam mail, privacy impact assessment (PIA), class action

[박훤일, 「국제법무연구」 제10호, 경희대학교 국제법무대학원, 2006.2.]