**Contemporary Engineering Sciences, Vol. 7, 2014, no. 14, 661 - 670**
**HIKARI Ltd, www.m-hikari.com**
**http://dx.doi.org/10.12988/ces.2014.4672**

# Comparison Study of Personal Information Protection Laws in South Korea

**ChoYee Nam**

Center for Information Security Technologies (CIST)
Korea University, Seoul 136-701, Korea

**Kyungho Lee**

Center for Information Security Technologies (CIST)
Korea University, Seoul 136-701, Korea



**Abstract**

For the recent personal information leaks, it is urgent that the protection provisions for personal information and the countermeasures for personal information leakages be established. As the importance of personal information security grows, the government has enacted related laws and regulations and published the guidelines for managing personal information. However, unlike the government's goals and wishes, each laws and regulations only intensify confusion. The structural defects are found in the privacy laws by the comparative analysis of related laws and regulations. This paper presents the integrated suggestions for the distributed laws and regulations of personal information in Korea. For the laws and regulations causing confusion, integrated guideline is suggested according to the analysis of Sarbanes-Oxley Act in U.S

**Keywords**: Information Security, Personal Information, Personal Information Protection

## 1. Introduction

As Internet develops, personal information which had been stayed in documents or storage has become floating along with a lot of information on the

Internet. In particular, the development of E-commerce has related personal information to money.

Recently appeared 'SMishing' attack is able to make the attacker take monetary gain via mobile phone payment. Thus, monetary gain from personal information breaches results in sudden increase of personal information breaches. According to National Statistical Office, the number of consultation for personal information leaks is growing every year. In the report from National Statistical Office, the number of consultation was 122,245 in 2010, 166,801 in 2012 and 177,736 in 2013.

As the importance of personal information has emerged, "Personal Information Protection Act" was enacted March 29th, 2011. The purpose of "Personal Information Protection Act" is to compensate blind spots to regulations for personal information included in different existing laws.

Currently, the laws related to personal information protection includes "Personal Information Protection Act" that is a general law, "Electronic Financial Transaction Act", "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc" and "Enforcement Decree of the Use and Protection of Credit Information Act", etc. However, regulations for personal information protection are distributed to several different laws. Inconsistent regulations demonstrate no effectiveness causing confusion to the organization collecting and using personal information.

In this study, comparison study on laws about personal information is conducted and the guideline of integrated laws regarding personal information is suggested as a result of comparison study.

## 2. Background – Relationship between general law and special law

The structure of laws regarding personal information in South Korea consists of a general law and special laws. General law is the law which is applicable to all targets. Special law, on the other hand, has limited range of targets at the same level of general law. Special law is applied to limited circumstances, person or area. It means that the range of special law is smaller than the range of general law. For example, the relationship between general law and special law is similar to the relationship between "Act on Special Cases concerning the Administration of the Seoul Special Metropolitan City" and "Local Autonomy Law". "Local Autonomy Law" is applied to nationwide, but "Act on Special Cases concerning the Administration of the Seoul Special Metropolitan City" is only applied to Seoul Metropolitan City.

And the relationship between general law and special law can be defined according to the priority. According to the principle of special law to be applied first, special law applied first over general law. In other words, special law is first applied to certain circumstances, person and area while general law is applied

later to the rest which is not the target of special law as long as it is not contradictory to the special law.

Considering that special law is limited to special targets, it is the normal structure that the punishment prescribed by special law is stronger compared to the punishment prescribed by general law.

## 3. Comparison study on laws concerning personal information protection

### 3.1 Research Range

The range of comparison study is the law including regulation concerning personal information protection and applicable to personal information breach incidents. The law concerning personal information protection includes “Personal Information Protection Act”, “Electronic Financial Transaction Act”, “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc”(Act on Information and Communications Network) and “Enforcement Decree of the Use and Protection of Credit Information Act”(Credit Information Act)

The Korean government enacted “Personal Information Protection Act” to deal with collecting and processing personal information expanded as a result of expansion of information-telecommunication devices and promotion of e-government. Existing privacy related laws were limited to certain areas, but enactment of. “Personal Information Protection Act” make the government become capable of prevent the damage caused by misuse of personal information throughout society. Unlike “Act on Information and Communications Network”, “Electronic Financial Transaction Act” and “Credit Information Act”, “Personal Information Protection Act” is applied to all targets unless special law does not exist for the target.

“Act on Information and Communications Network” is enacted to promote the use of information communications network and to protect the personal information for the users of information communications services. Information communications network service is to provide information utilizing telecommunications equipment and mediate supply of information. “Act on Information and Communications Network” is applied to targets supplying information communications network services and personal information used in information and communications network.

The purpose of “Electronic Financial Transaction Act” is to secure the safety and reliability of electronic financial transactions. Electronic financial transaction is automation transaction and supply of financial products or services through electronic devices by financial company or electronic financial business operator. In other words, “Electronic Financial Transaction Act” applied restrictively to

electronic financial transactions targeting financial companies and electronic financial business operators.

"Credit Information Act" is to foster credit information business and to protect privacy from misuse of credit information. Credit information is information used to determining credibility of trade opponents such as information to identify credit information object, information about transactions and information to judge credibility. Therefore the range of "Credit Information Act" is limited to credit information which is a kind of personal information and the target of the law is companies for credit information business.

Following Figure1 represents the range of the laws concerning personal information protection.

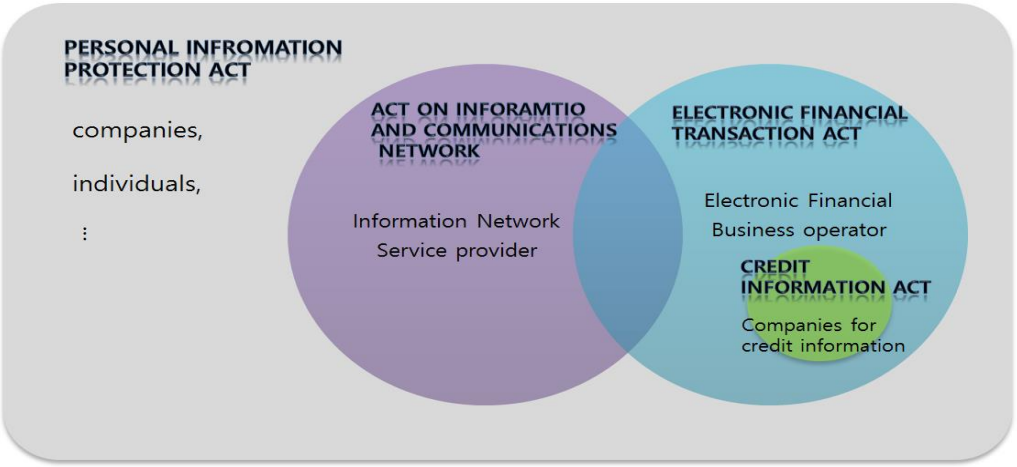


**Figure 1 The application range of laws concerning personal information**

"Act on Information and Communications Network" which targets to information and communication service providers applied first prior to a general law, "Personal Information Protection Act". Also for financial companies and electronic financial business operators, "Electronic Financial Transaction Act" is applied prior to "Personal Information Protection Act". For the credit information business companies among financial companies, "Credit Information Act" has priority over "Electronic Financial Transaction Act".

According to the purpose of special law to specially control certain circumstances, person and places, regulations of special law should be stronger than those of general law in the structure of special law and general law.

### 3.2 Research Method

The method used in the comparison study consists of two steps. Firstly, a certain situation is selected to compare the laws concerning personal information protection. The articles applied to the same incident are derived from each laws regarding personal information protection regulations. The incident used in this study is suggested below.

| |
|---|
| The personal information is disclosed from the company because the company doesn't have a measure to protect personal information that a President decree has suggested. The information disclosed by the company's fault includes "resident registration number". |

Then, the degree of punishment for violation of the article derived from the first step is compared.

### 3.3 Result for Comparison Study

The articles applicable to the situation are suggested in Table1. Applied target is different depending on the type of business. But the articles from each law are applied to the same situation. All the articles compared in the study are applied when personal information including social security number has leaked and the company who is responsible for the leakage doesn't have measures to protect personal information.

| law | Article number | Article |
|---|---|---|
| **Personal Information Protection Act** | The article 34-2 | The Ministry of Security and Public Administration may impose penalty surcharge not exceeding 500 million WON on a business if a user's resident registration number lost, stolen, leaked, altered, or mutilated because it has not taken measures according to a Presidential Decree. |
| **Act on Information and Communications Network** | The article 64-3 | The Korea Communications Commission may impose penalty surcharge not exceeding 100 million WON on a telecommunications business operator if a user's personal information lost, stolen, leaked, altered, or mutilated because it has not taken measures according to a Presidential Decree. |

| | | |
|---|---|---|
| **Electronic Financial Transaction Act** | **The article 49** | **Any person who has offered, divulged, or used for any purpose other than the conduct of business, electronic financial transaction information shall be punished by imprisonment of not more than five years or by a fine not exceeding thirty million WON. And according to joint penal provisions, not only shall such actor be punished, but also such corporation or individual shall be punished by a fine prescribe in the relevant Article.** |
| **Credit Information Act** | The article 52 | No person who is or was an executive or employee of a credit information company, etc. and a person entrusted with the processing of credit information shall disclose or use any personal confidential information, including credit information and privacy(hereinafter referred as "personal confidential information") acquired during the course of business for non-business purposes. Any person who violates this article shall be punished by imprisonment for not more than five years or by a fine not exceeding fifty million WON. And according to joint penal provisions, not only shall such actor be punished, but also such corporation or individual shall be punished by a fine prescribe in the relevant Article. |

**Table 1 The articles applicable to the same situation**

As a result of comparison study, some structural defects are discovered. The degree of punishment for the violation of personal information protection law which is a general law is much heavier than those of special laws. According to Personal Information Protection Act, a fine not exceeding 500 million WON is imposed on the company who is responsible for the leakage. But for the companies under the influence of Act on Information and Communications Network, less than 100 million WON is imposed as a fine. And Electronic Financial Transaction Act imposes a fine not exceeding 30 million WON and Credit Information Act imposes 50 million WON as a fine for the same situation. The Figure2 shows the amount of fine for the violation of each law. The structural defect that the degree of penalty is heavier than special laws could be seen in the

Figure2.

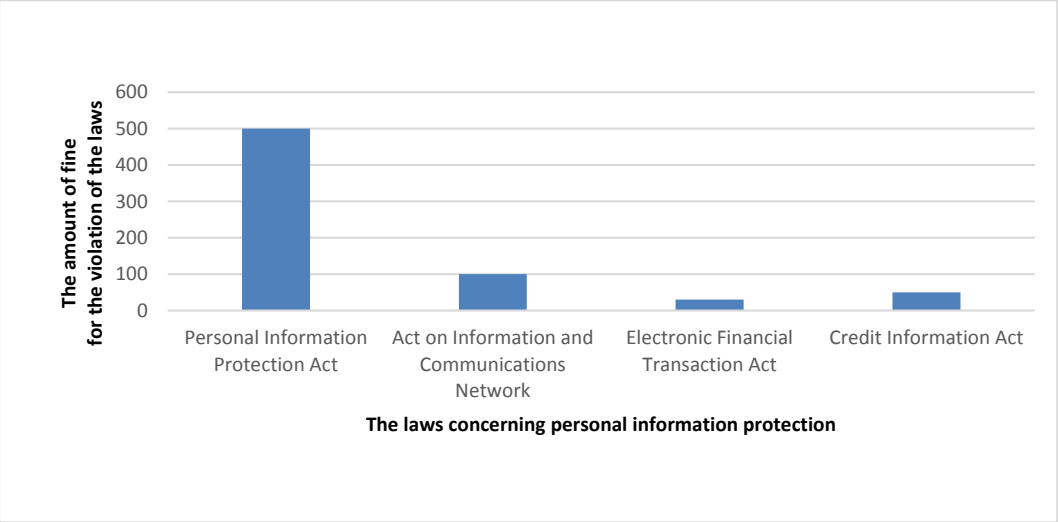


**Figure 2 the amount of fine for the violation of each law**

The structural defects in the privacy laws could be the hole to mitigate the punishment for the leakage of personal information. It means that a fine could be reduced from 500 million WON to 30 million WON when special law is applied. The targets of special laws are information network service provider, financial company or electronic financial business operator, and companies for credit information protection. Therefore small amount of a fine for the violation of the articles related to social security number leakage is imposed to those companies. This could be the cause of low effectiveness of laws. Thus, the structural defects in the privacy laws should be revised as soon as possible.

### 3.4 Case Study

The laws concerning personal information are applied to recent personal information breach incidents in orders and the results of punishment for each laws are compared.

Last January 2014, the prosecution announced that a large amount of personal information had leaked by South Korea's three major credit card companies. The number of information leaked by credit card companies including social security number, phone number, and card numbers is 140,000,000. This was the largest ever in South Korea. Since the kind of leaked information is financial information and credit card information, "Personal Information Protection Act", "Electronic Financial Transaction Act" and "Credit Information Act" are applied to the incident.

According to the article 34-2 of “Personal Information Protection Act”, up to 500 million WON is levied on each credit card companies for the leakage of personal information when only “Personal Information Protection Act” is applied. However under five years of imprisonment or up to 30 million WON is levied for each credit card companies when “Personal Information Protection Act” and “Electronic Financial Transaction Act” is applied. Also, if “Credit Information Act” is applied in addition to “Personal Information Protection Act” and “Electronic Financial Transaction Act”, up to five years or 50 million WON is imposed to the companies. In this case, over 10 times greater than the amount of fee imposed by special law is levied by general law.

Other recent personal information breaches in South Korea shows similar result. In the same year, one of the major tele-communication companies, K company, leaked personal information of over 1/5 South Korean. K company is information and communication service provider. Therefore it is under the influence of “Personal Information Protection Act” and “Act on Information and Communications Network”. The cause of personal information leakage was insufficient measure for the systems storing personal information which violates the article 34-2 of “Personal Information Protection Act” and the article 64-3 of “Act on Information and Communications Network”. In this case, the amount of fine is different depending on which law is applied. When both “Personal Information Protection Act” and “Act on Information and Communications Network” is applied to this incident, 100 million WON is imposed. But, if only “Personal Information Protection Act” is applied, the amount of fine becomes 500 million WON which is five times of the fine for a general law.

The case study shows that it is possible for special laws to allow to escape strong punishment for the subject which should be strictly restricted and protected for its importance. The abnormal structure of general law and special law hinders the effectiveness of privacy laws alleviating the stringency of punishment. Therefore even if the government intensifies the punishment regulations, the intensified punishment has no effect on preventing personal information leakage. Therefore the laws concerning personal information should be reviewed thoroughly in the aspect of the structure of general law and special law and revised to regulate with integrated standards.

## 4. Sarbanes-Oxley Act, U.S

Sarbanes-Oxley Act(SOX) is U.S act about standards of financial audit for companies. SOX is enacted in 2002 to raise accuracy and credibility of other companies’ disclosed information in accordance with securities act and any other purposes. Not only the regulations on companies were intensified but also the punishment for violating company and executives was intensified. The main context of SOX includes authentication and extended responsibility for the board member’s financial statements, reinforcement of internal control system,

installation and management of Public Company Accounting Oversight Board(PCAOB), Strengthening the independence of auditors and protection for whistle-blower.

Section 404 in SOX is about management assessment of internal controls. Section 404 instructs that an annual evaluation of internal controls and procedures is included in financial reports and companies have responsibility to install and assess the internal control systems. Generally, internal control refers to selected procedures or systems to minimize the potential risk in company. In this context, internal control framework referred to the act is suggested by COSO(the Committee of Sponsoring Organizations of the Tradeway Commission). Although SOX is the act for financial audit, most of financial information stored in IT systems and business is conducted over IT Systems. Therefore the internal controls include overall IT system controls. The punishment for the violation of the internal controls is from at least a million dollars to 20 million dollars. The internal controls in companies have improved as a result of strong internal controls and punishment of SOX in U.S.

However, internal controls in South Korean companies, especially the controls over personal information are much lower compared to the standard of SOX. Internal controls over personal information are suggested in the article 34-2 of "Personal Information Protection Act" and the article 64-3 of "Act on Information and Communications Network". The fine for the violation of the internal controls is only up to 50 million WON. Moreover if the special law is applied prior to general law, only 10 million WON is imposed to the violation company. To increase the level of internal control to protect personal information effectively, the structure of special law and general law should be improved and the punishment should be heavier as SOX.

## 5. Conclusions

The importance of protecting personal information grows because of recent personal information breach incidents. To prevent further damage, "Personal Information Prevention Act" was enacted and other existing laws are revised to intensify the regulations. However, unintegrated privacy laws from abnormal structure of general law and special law have structural defects. To achieve primary purpose of privacy laws, the laws should be reviewed thoroughly and revised considering the structure of general law and special law. SOX in U.S could be a good standard to intensify the internal controls about personal information in companies.

**ACKNOWLEDGEMENTS.** The work was supported by a Korea University Grant.

## References

[1] National Statistical Office, http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366

[2] Personal Information Protection Act

[3] Act on Promotion of Information and Communications Network Utilization and Information Protection, etc

[4] Electronic Financial Transaction Act

[5] Enforcement Decree of the Use and Protection of Credit Information Act

[6] definition of general law and special law, http://www.law.go.kr/lsTrmInfoP.do?q=&p1=&pg=1&seq=0&fsort=10&outmax=50&lsTrm=%EC%9D%BC%EB%B0%98%EB%B2%95(%EB%B3%B4%ED%86%B5%EB%B2%95)%ED%8A%B9%EB%B3%84%EB%B2%95#click0

[7] Yongsu Lee, The general consideration for internal controls and the case of U.S, *KISDI,* (2005)

[8] Marios Damianides, Sarbanes-Oxley and it Governance:New guidance on it control and compliance, *Information Systems Management,* (2006)

[9] F.L. Crane, H. Low, P. Navas, I.L. Sun, Control of cell growth by plasma membrane NADH oxidation, *Pure and Applied Chemical Sciences*, **1** (2013), 31 - 42. http://dx.doi.org/10.12988/pacs.2013.3310

[10] Sarbanes-Oxley Act, https://www.sec.gov/about/laws/soa2002.pdf

**Received: May 1, 2014**