BADM 590
Seminar in Business Administration
IT Governance Report

Act on Protection of Private Information in Japan

Takashi Kozuka
Abstract
For business entities, personal information is useful for their marketing and new product
development. However, there are increasing risks in this digital age associated with it. If
it is maliciously used, people get suffered.
In this report, I focus on Act on Protection of Personal Information which has been
enforced since April 2005 in Japan. My objective is to identify the background of the
establishment of this act, what this act is, what problems business entities are facing,
what IT solutions there are to solve those problems.

Magnitude of new types of frauds in Japan

Telemarketing frauds
In this fraud, a criminal pretends to be relative of victims, police, and lawyers. Then,
he/she makes a telephone call to victims, trying to deceive them. In many cases, they
create false incident like car accident, saying "Mom, I got car accident. Unfortunately, I
forgot to pay for the insurance and they said that they can't pay for the liability I have. If I
don't pay for it, I'll be in jail. Can you transfer the money into this account?" According
to National Police Agency in Japan, the total amount of money related to this fraud is 19

Fake check fraud
In this fraud, a criminal tends to use Internet to reach to potential victims. He/she send
false bills to them. Typical case is that he or she claims that the victims had used porn site.
According to National Police Agency in Japan, the total amount of money related to this fraud are about 5 billion yen in 2004, 2005 and 2006.

**Advanced fee fraud**

In this fraud, a criminal tends to use Internet to reach to potential victims. Typically, he/she send an e-mail to a victim, saying "This mail is from IRS. According to our record, you've overpaid your tax. You can get it back if you pay for the fee to advance the process" According to National Police Agency in Japan, the total amount of money related to this fraud are about 4 billion yen in 2004, 7 billion yen 2005, and 5 billion yen in 2006.

Because of the magnitude of these frauds, people in Japan are getting more sensitive about their personal information than before. This means that if a business entity leaks their customer information; its reputation will be seriously damaged. Additionally, because the Act on the Protection of Personal Information has been enforced since April 2005, if a business entity doesn't comply with the act, it might not be able to get a job from their business partners.
The Protection of Personal Information


This act was promulgated on May 30, 2003, and enforced on May 30, 2003 except for Chapter 4 to 6 and article 2 to 6 of Supplementary Provisions. On April 1, 2005, this act was completely enforced. In the following, I picked up articles which are relevant to this report.

**Definition of Personal Information (Chapter 1 Article 2.1)**

In this Act, "personal information" means information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).

**Definition of Personal Information Database (Chapter 1 Article 2.2)**

In this Act, "a personal information database, etc." means a set of information including personal information as set forth below:

1. a set of information systematically arranged in such a way that specific personal information can be retrieved by an electronic computer; or
2. other than those described in the preceding paragraph, a set of information designated by a Cabinet order as being systematically arranged in such a way that specific personal information can be easily retrieved.
**Definition of entity handling personal information (Chapter 1 Article 2.3)**

In this Act, "an entity handling personal information" means an entity using a personal information database, etc. for its business; however, the following entities shall be excluded:

1. The State institutions
2. Local public bodies
3. Independent administrative agencies, etc. (which means independent administrative agencies as prescribed in Paragraph 1 of Article 2 of the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. (Law No.59, 2003; the same shall apply hereinafter))
4. Local independent administrative agencies (which means local independent administrative agencies as prescribed in Paragraph 1 of Article 2 of the Local Independent Administrative Agencies Law. (Law No.118, 2003; the same shall apply hereinafter))
5. Entities specified by a Cabinet order as having a little likelihood to harm the rights and interests of individuals considering the volume and the manner of use of personal information they handle.

**Basic Philosophy (Chapter 1 Article 3)**

In view of the fact that personal information should be handled cautiously under the philosophy of respecting the personalities of individuals, proper handling of personal information must be promoted.
Duties of Entities handling with Personal Information (chapter 4)

In this act, there are duties of entities handling with personal information. An entity has four categories of duties to comply with.

Duties for protecting personal information

1. Specification of the purpose of use
2. Restriction by Purpose of Use
3. Proper Acquisition
4. Notice of the purpose of use at the time of acquisition
5. Handling of complaints by entities handling personal information

Duties for protecting personal information database

6. Maintenance of the accuracy of data
7. Security control measures
8. Supervision of employees
9. Supervision of trustees
10. Restriction of provision to third parties

Duties for responding to the request from a person who is listed in the database

11. Public announcement of matters concerning retained personal data
12. Disclosure
13. Correction of the personal information data
14. Stopping the use
(15) Explanation of reasons
(16) Procedures to meet requests for disclosure and others
(17) Charges

**Duties for responding to the request from the ministry which governs this act**

(18) Collection of reports
(19) Advice
(20) Recommendations and orders

In sum, an entity which is handling with personal information has to protect personal information and personal database. In addition, it has to respond to the request from a person which is listed in the database. The request could be disclosure, correction, stopping the use of the personal information and so on. Finally, an entity which is handling with the personal information must respond to government request. For example, if the state or local government requests inspection of how an entity is dealing with the personal information, the entity must collect a data and give reports to the government.

**Penal Provisions**

An entity who violates orders issued under Paragraph 2 or 3 of Article 34 shall be sentenced to imprisonment of not more than six months or to a fine of not more than 300,000 yen. And also, an entity who does not make a report required by Article 32 or 46 or who has made a false report shall be sentenced to a fine of not more than 300,000 yen.
**Reaction of citizens in Japan**

Because of this act, citizens in Japan are getting more sensitive about protecting personal information. For example, there are many sue cases in which a person who was damaged by his personal information leakage sued the entity. Bad reaction is that people are too sensitive to participating census. Another bad reaction is that health care industry was too sensitive to disclose personal information in a serious disaster. This law doesn’t prohibit census or disclosing personal information in a serious disaster. Japanese government is trying to correct these misunderstandings.

**Reactions of Entities handling with personal information**

This act facilitated the implementation of IT solutions for protecting personal information. And also, they tend to consolidate personal database so that they can manage personal information efficiently. In extreme case, some are hesitating with having identifiable information such as name and contact. In this case, they just have relevant information such as age or area for their marketing analysis purpose. Negative impact for the entities handling with personal information is that they have to precede deleting, collecting, and disclosing requests from their customer. Some requests are not necessarily processed according to the acts. However, this act is simply a burden for any entities handling with personal information. Negative reaction does occur. This law requires entities to notify the usage of personal information. Some company set broad definition of the usage, saying, “We use your personal information for our any operations.” This kind of notification of usage confuses customers. Some guidelines are needed both for protecting personal information and for using personal information successfully.
Investigation of accidents of personal information leakage

In 2005, National Consumer Affairs Center of Japan (NCAC) did a survey. The surveyed entities were the ones who had been leaked personal information. They got 45 cases to analyze. Following are the summary of the survey.

The contents of the personal information which was leaked

According to the survey, not only name and contact information but also sensitive information such as credit card number had been leaked. There are 41(91%) cases in which identifiable information such as name was leaked. There were 34(75%) cases in which contact information such as phone number, addresses and e-mail address were leaked.

The reasons of the leakages

There were 39 (87%) of cases in which the entity did an investigation why it had leaked personal information. The number of cases which the reason of leakage was identified is 29 (64%). Other 10 cases, the reason couldn’t be identified. They categorized the reason into 4 types.

(1) Carelessness of employees (16 cases)

Employees left the information in public place such as train (3 cases). Employees sent specific customer’s information to other customers (3 cases), third party (distributors) lost when they transfer something (4 cases) etc.

(2) Employee theft (12 cases)

Employees or employees of ODM, CDM or CM theft steal personal information, save it to storage media, take it and give or sell it to someone else. There were 7
cases of employee theft, and there are 3 cases of ODM, CDM or CM employee’s theft.

(3) Theft (7 cases)
Employees or employees of outsourced company leave documents of personal information in a car or somewhere else, and the data was stolen.

(4) Problems in computer system (6 cases)
Due to some system error or problems, the personal information which was on a server had been leaked.

**Administrative structure**

At the time of the cases, 34 (76%) entities out of 45 had policies regarding to the protection of personal information. They claimed that they had privacy policy and rules, they had dedicated personnel to administrate, and they did access control over the information system. However, they also claimed that implementation wasn’t enough.

Some claimed that education of employee wasn’t enough also.

On the other hand, there were only 2 cases in which outsourcer had rules ODM, CDM or CM. There are difficulties in administrate external company.

As we can see here, most of the leakages come from human error or malicious intent.

Next I’ll discuss about the functions and IT solutions needed to solve these issues.
Functions and IT solutions to protect personal information

Data Encryption
In order to protect personal information, we need to take care of employee’s carelessness. With data encryption software, we can encrypt HDD itself and external disk device such as CD, DVD, and flush memory. And also, such kind of software has a capability of encrypting e-mail message or attached files. Data encryption minimizes the risk of leakage of personal information when employees or distributors lost it because of their carelessness. In Japan, Hitachi Software Engineering Co., Ltd has been dominating this type of software market.

Biometric Authentication
Biometric authentication is another way to protect personal information. With this, we can minimize the risk of the leakage from real theft. There already are lots of personal computers which has this function. Interesting thing is that some manufactures has started to use biometric authentication other than personal computers to protect personal information. Because of the Act of Protecting Personal Information, lots of companies have coped with personal computers. However, few of them cope with the most basic media, “paper”. Konica-Minolta has developed the copy machine which has biometric
Authentication.

Access Control

It’s important to determine who can access, read, edit, copy, and take the personal information. To limit the people who have access to the information is to minimize the risks of leakage. Hitachi Software Engineering again has been providing such software which limits access control of both print and external disks to specific users.

There are solutions to give access control over specific files. Digital Rights Management software is one of them. Two major office document companies, Microsoft and Adobe have been implemented DRM capability into their products. And also, NEC in Japan is trying to implement DRM capability for any files.

Monitoring & Scheduling

Even if we use all the functions above, the risks associated with malicious employees or employees of outsourcers can’t be perfectly addressed. Monitoring is the key here. In the case of the leakage from Dainippon Print in Japan, they logged the access to the computer system which has personal information. However, because they audit the log once a month, they couldn’t identify the leakage from employees of the outsourcee. Then, they
started to monitor the access once a day. However, to monitor all the data inside a company isn’t feasible. So, we need to identify the important data to monitor or we have to consolidate important data and manage it rigorously.

**Insurance**

Even if we do all the things, we can’t make the risk of leakage zero percent. However, we have to take care of this risk. SOMPO Japan made such an insurance to cover potential loss from personal information leakage.
Other consideration

Protecting Intellectual Property

There are increasing needs to protect intellectual property in Japan in addition to personal information. For example, trade secret was stolen from Denso and confidential information of Ages Combat System was stolen from Ministry of Defense. These incidents have made people in Japan more sensitive to protect “information”. IT solution providers which have solutions for protecting personal information are now providing solutions to protect intellectual property too.

J-SOX implementation

In FY 2008, Japanese version of SOX will be enacted. J-SOX is based on COSO framework. Unlike U.S SOX, Japanese SOX mentions about IT governance. In addition, Ministry of Economy, Trade and Industry is providing guidance of implementing IT governance too. So lots of IT solution providers tried to sell their solutions related to J-SOX. Information protection is somewhat related to IT governance. For example, access control functions are needed to ensure the validity of audit. Presumably, IT solution providers which have been provided the solutions for protecting personal information are now providing solutions for J-SOX too. For example, Hitachi Software Engineering bought a consulting company which has public auditors to enhance their solution for IT governance. Another example is that TIS made an alliance with Protivity to provide a solution for J-SOX.
Conclusion

Private information needs to be protected. Japanese government enforced Act on Protection of Private Information to the entities handling with private information. Entities have been complied with the legislation. However, information leakage can’t be stopped perfectly because of human error. Human error or malicious intention is the biggest issue in this area. IT solutions should cover this human error.