RFID Tags:Legal Issues and Guidelines in Japan

RFID Tags: Legal Issues and Guidelines in Japan

Takato NATSUI*

1. Introduction

Applications for electronic technologies that utilize radio frequency identification (RFID) are proliferating. In Japan too, RFID products such as Hitachi's μ chip are being put to practical use, and RFID technologies will be used in tickets for the Expo 2005 Aichi, which is scheduled to open later this year. Thus, the use of RFID in day-to-day life is becoming increasingly common.

RFID was originally developed for military applications, but in conjunction with later advances in electronics and precision processing technologies, it came to be used as a private-sector product in the form of miniature electronic tags for distribution and warehouse management. Although RFID tags are extremely small electronic products, they are equipped with calculation functions, memory functions, input/output functions, and communications functions—like miniature computers—and as a result, concerns have been raised with regard to privacy and personal data that is recorded in RFID tags. Specifically, there are doubts about the application of the consent requirement imposed by the European Directive on the Protection of Personal Data when collecting personal data by means of stealth deployment of RFID tags without the consumer's or customer's knowledge. Identical legal issues are also presented in the context of Japan's Personal Data Protection Law and judicial decisions concerning the protection of privacy in the United States.[1]

This article focuses primarily on those legal issues regarding RFID that involve questions of privacy and the protection of personal information, but also touches on other significant legal issues, providing basic information necessary for understanding the current status of the legal issues and presenting an overview of actions taken by various national governments and private organizations. This article is not intended, however, to provide detailed technical information concerning RFID.

2. Approaches to the Legal Issues

There are some who believe that the legal issues concerning RFID are quite

---

* Professor, Faculty of Law, Meiji University, Tokyo
MEIJI LAW JOURNAL, Volume 13 (March 2006)

[1] See, Simson Garfinkel, Beth Rosenberg ed., RFID – Applications, Security, and Privacy, 2005, Addison Wesley

unique. There is also the misunderstanding that to the extent that there are no specific laws addressing RFID, anything is permissible. Both of these propositions are true. And as any legal scholar knows, however, both opinions are incorrect.

The Civil Law Applies to Improper Disclosures of Personal Information

If a mistake in the design, application, or operation of an RFID tag that is part of a tracing system results in an improper disclosure or use of personal information, for example, an individual who suffered harm as a result thereof could seek compensation from the designer, developer, or operator of the system in question under the provisions of Article 709 of the Civil Code relating to tortuous conduct. Similarly, if such an error corresponded to a defect in the product, then the Product Liability Law would apply. In such cases, there is absolutely no need for the existence of a special law concerning liability arising from the use of systems that use RFID. The existence of legal liability can be determined based on conventional determinations of fact and legal interpretation of the Civil Code and other laws.

(1) Even though Guidelines are Voluntary, they can Serve as Standards for Determining the Existence of Negligence

The Japanese government has adopted guidelines concerning the use of RFID tags. These guidelines will be introduced in this article. Such guidelines have the role of preventing the occurrence of legal disputes while promoting uses that take advantage of the benefits of RFID technologies. The use of guidelines, however, is entirely voluntary and they have no legal compulsory force whatsoever. The internationally recognized and fundamental understanding is that persons who do not wish to comply with such guidelines may ignore them completely. Consequently, the guidelines themselves cannot be expected to deny the possibility of businesses that will act in violation of the guidelines. This is also true of the Guidelines concerning the Protection of Personal Information adopted by relevant ministries in relation to the Personal Data Protection Law. Accordingly, it is extremely important to investigate questions of the applicability of general law without regard to the existence of absence of guidelines. Nonetheless, in courts of law addressing questions of civil liability, guidelines concerning RFID tags may serve as crucial indicators or standards for determinations of whether a business acted in accordance with the duty of due care (that is, whether the business acted negligently) . In this sense, such guidelines must be investigated thoroughly and carefully, and complying with them is quite important and valuable.

(2) Accidents Caused by RFID Technology can Result in Death or Injury Caused by Negligence in the Conduct of Business

RFID technologies as well as the products and services that apply them are used in various situations within society. Law that can apply to legal issues arising from technologies and products used for some purpose within society are

equally applicable to RFID technologies as well as the products and services that use them. Consequently, if a traffic accident occurs because of a malfunction in a traffic control system that uses RFID tags, for example, death or injury caused by negligence in the conduct of business may be established under the Criminal Code, and penalties may be imposed under the Criminal Code or the Road Traffic Law.

(3) As Industrial Products, RFID Tags Must be Safe

RFID tags are industrial products, and consequently, the components and materials used must be safe, and various laws and regulations concerning safety are directly applicable. If a certain RFID products lack adequate safety as an industrial product, the manufacturer may be subject to administrative guidance or sanction under applicable law. If RFID tags are applied directly to foods or processed materials, laws such as the Food Safety Law may apply. In addition, RFID tags are a type of computer, and therefore recycling laws such as laws and regulations on the use and recovery of computer devices may also apply.

(4) Regulations concerning Radio Waves Apply to RFID Tags

RFID tags use radio waves, and therefore, laws and regulations concerning the allocation of radio bandwidths and output strengths apply. Similarly, in circumstances where there are concerns about detrimental impact from radio waves on the control of other devices (from, for example, use of electronic medical equipment during aircraft takeoff and landing) , the applicability of related laws and regulations must be examined carefully.

(5) Summary

It is important to understand that legal issues concerning RFID technologies and the products and services that use them are not unique, but are no more than one variation of general legal issues.

3. RFID and the Protection of Privacy and Personal Information

Various individuals have expressed concerns regarding violations of privacy and issues of protection of personal information with respect to the use of products and services that employ RFID technologies.

(1) Concerns about Violations of Privacy

In the United States, there are private organizations that address issues of privacy as a whole (such as the Electronic Privacy Information Center and the Electronic Frontier Foundation) and organizations that deal with the protection of privacy as it concerns RFID tags (such as Consumers Against Supermarket Privacy Invasion and Numbering) . These organizations continuously express opinions concerning the potential for violations of privacy resulting from RFID tags and make proposals including specific measures to address their concerns. Unfortunately, there are no similar organizations in Japan addressing issues concerning the protection of privacy.

(2) How can Violations of Privacy Result from the Use of RFID Tags?

There are two types of RFID tags: active and passive. Active tags continuously generate their own radio waves (such tags include the tags used to monitor the behavior of wild animals), while passive tags transmit the data stored in the tag only in response to a radio signal received from a transceiver. Use of either type of tag on people will result in the provision of private information such as location and route data concerning the person with the tag to others.

In addition, while there are tags that contain information only about the tag itself, there are also tags that have the ability to store internally personal information such as customer data. If the data stored in the tag is improperly revealed to others, a violation of privacy or disclosure of personal information will occur.

Moreover, information obtained from RFID tags can be stored in databases and matching performed with data used to identify specific individuals, which means that all of the information in the database becomes personal information. If the database is not protected by adequate security, violations of privacy may occur. Violations of privacy and disclosures of personal information can also occur if the transmissions between RFID tags and transceivers are intercepted.

In light of this analysis, issues concerning privacy and protection of personal information cannot be addressed properly without considering at what stages, and in what manner violations can occur.

(3) Under what Circumstances can Violations of Privacy Result from the Use of RFID Tags?

If we consider the situations in which violations of privacy can occur depending on the actual use of RFID tags, we can imagine the following examples.

(a) Financial Information

If credit cards and prepaid cards use RFID technology, it will be possible to exchange wirelessly various types of information including the amounts of charges, payment status, and arrearages for virtually all types of payments. If information security for these cards cannot be ensured, however, the information stored or recorded within the cards or information that is being transmitted can be intercepted, resulting in a violation of privacy or disclosure of personal information.

(b) Medical Information

If medical charts, treatment records, and testing records contain RFID tags and the tags contain personal information, without adequate information security, third parties may be able to intercept information relating to a patient's condition when the patient is simply walking down a hospital hallway carrying the records or cards with him.

(c) Shopping

If clothing, foodstuffs, and other consumer products have RFID tags without adequate security, a third party may be able to detect wirelessly all of the items that a customer has placed in a shopping cart and obtain private information such as the customer's shopping habits.

(d) Position Data

Cell phones and entry cards that employ RFID technologies but do not ensure adequate information security allow the holder's position and movements to be detected wirelessly, enabling a third party to trace the holder's routes and locations visited. In such a case, the holder's freedom of choice of where to live and freedom of movement guaranteed in Article 22 Paragraph 1 of the Japanese Constitution may be infringed and violations of privacy may occur.

(4) How should these Issues be approached?

As these examples show, there is the potential for violations of privacy in all social settings with regard to the use of RFID tags. In Japan, these issues have not been addressed as significant problems and there are few instances of the mass media, researchers, and private organizations expressing interested in them, but these issues are always present or at least lurking in the background. Nonetheless, it is a fact that the application of RFID technologies including RFID tags has a variety of effects.

Consequently, it is necessary to consider policies to ensure that products and services that use RFID technologies can be put to maximum benefit while preventing and eliminating abuses such as violations of privacy.

The most important thing here is the development of suitable policies that balance privacy interests with the benefits of the technologies. These types of policies are already expressed in a variety of related guidelines, statutes, and proposed statutes.

(5) What is the Fundamental Policy?

It is possible to examine and propose the necessary elements of such policies from a variety of different approaches, but the policies that are shared and approved by legal systems and guidelines in a number of countries are as follows.

(a) Ensuring Information Security

When private and personal information is gathered, stored, and transferred by RFID tags and other technology applications, it is necessary to ensure high levels of information security using technological means by encrypting the information itself, introducing encryption technologies to radio communications, and incorporating security functions into the RFID chips.

(b) Proper Handling of Personal Information

Persons who handle private and personal information including its collection, storage, and transfer have an obligation to handle that information "properly" as specified in the provisions of the Personal Information Protection Act. The measures for ensuring information security as required by the duty to handle personal information properly include both technological means and non-technological means (such as information security management and information security education).

(c) Notice of the Presence of RFID Tags and Transceivers

Individuals such as consumers have the right to refuse the collection of private and personal information through the use of RFID tags and other means except in cases of legal or contractual obligation. Effectively guaranteeing this right of refusal requires that notice be provided concerning the presence of the RFID tags and transceivers that are to be the subject of the individual's refusal. Accordingly, the presence and functions of RFID tags and transceivers must be displayed prominently. In many instances, use that is not based on consent (stealth deployment) will likely constitute unlawful conduct.

(d) Notification of Privacy Policies and Security Policies

When collecting private or personal information using RFID tags, the collecting party must provide notice of its privacy and security policies as they relate to the collection, management, and use of such information. In most instances, the posting and disclosures of such policies on a Web site will not be adequate.

(e) Ensuring the Right to Refuse Use of RFID Tags

Individuals such as consumers must be able to refuse effectively the collection of personal and private information through the use of RFID tags and transceivers except in the case of legal or contractual obligation. For example, the removal or destruction of RFID tags at the time of payment or when theft-prevention tags are no longer needed must be fully permissible.

4. Guidelines Concerning the Use of Electronic Tags in Japan

In Japan, guidelines relating to the use of RFID tags and the protection of privacy and personal information were issued jointly by the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) and the Ministry of Economy, Trade and Industry (METI). The guidelines are entitled the Guidelines for the Protection of Privacy with Regard to Electronic Tags (ID Tags) (adopted on June 8, 2004; hereinafter referred to as the "Government Guidelines") [2].

(1) Explanation by METI concerning the Background to Adoption of the

---

[2] Official document of the Guidelines in Japanese can be downloaded at: http://www.soumu.go.jp/s-news/2004/pdf/040608_4_b.pdf

Government Guidelines

The Background and Overview of the Adoption of the Guidelines for the Protection of Privacy with Regard to Electronic Tags (ID Tags) issued by the METI explains the background to the guidelines as follows.

- Consumers do not have an adequate understanding of the unique properties of electronic tags (IC tags) that allow information to be read from electronic tags remotely when products are sold with electronic tags affixed to them.
- As a result, consumers are not aware that electronic tags are affixed to products, and it is possible that in the future, information such as the characteristics of products in their possession may be read in ways that consumers do not wish as they move about in their daily lives.
- It may be difficult to respond adequately once problems have occurred, and accordingly, METI has decided at this time to adopt specific guidelines for the protection of privacy and to make them available to related business organizations.
- Specifically, the Study Group on Improving Product Traceability (sponsored by METI with the participation of the Ministry of Land, Infrastructure and Transport, the Ministry of Agriculture, Forestry and Fisheries, and the Ministry of Health, Labour and Welfare) adopted guidelines on December 22, 2003, concluded the public comment period on February 21, 2004, and publicly announced the guidelines on March 15, 2004.
- In addition, METI and the MPHPT adopted the guidelines as the official government guidelines and announced them on June 8, 2004.
- The Japanese government plans on cooperating with international standardization organizations such as the International Organization for Standardization (ISO) to promote international collaboration on the protection of privacy with regard to the use of electronic tags.

(2) Explanation by the MPHPT of the Background to the Adoption of the Government Guidelines

The MPHPT explained the public announcement of the Guidelines for the Protection of Privacy with Regard to Electronic Tags in the following manner: "On March 30, 2004, the Study Group on Advanced Use of Electronic Tags in the Age of Ubiquitous Networks of the MPHPT compiled the Guidelines for Privacy Protection in the use of RFID Tags in its Approach to Advanced RFID Applications (final report). On March 16, 2004, the Ministry of Economy, Trade and Industry (METI) developed the Guidelines to Protect Privacy concerning RFID Tags. Subsequently, the MPHPT and METI have been conducting negotiations on development of common guidelines. Recently, the two ministries reached agreement and jointly adopted the Guidelines for Privacy Protection with Regard to RFID Tags."

(3) Why did the MPHPT and METI Adopt Joint Guidelines?

RFID tags are a type of information technology for the identification of individual objects using wireless communications, and are used to trace products and commodities. Since RFID tags use wireless communications, they fall within the scope of the communications legal system supervised and regulated by the MPHPT, but to the extent that they are related to business using information technology, they fall within the scope of the information industry, which is supervised and regulated by METI.

Accordingly, the both MPHPT and METI investigated the protection of privacy with regard to the use of RFID tags from the perspectives of their own areas of responsibility. As a result, METI's Study Group on Improving Product Traceability produced an interim report that addressed RFID tags and privacy issues and the MPHPT's Study Group on Advanced Use of Electronic Tags in the Age of Ubiquitous Networks produced a final report that also addressed this issue.

If the two ministries proposed differing guidelines addressing the same issues of privacy, the potential for abuse would be substantial, and accordingly, the ministries engaged in extensive negotiations to reach agreement on joint guidelines adopted by both the MPHPT and METI.

(4) Legal Status of the Guidelines

The legal status of guidelines was discussed in general terms. Guidelines are not statutes and are no more than voluntary decision-making guides. Accordingly, failure to comply with guidelines does not immediately result in a violation of the law. It is expected, however, that the guidelines will function as key standards in determining the presence or absence of tortuous conduct, failure to perform obligations, product liability, and death or injury caused by negligence in the conduct of business.

Consequently, complying with the Government Guidelines for business using RFID tags can be interpreted as an indication of the legal standard of care which may be generally required within a particular industry.

(5) Objectives of the Government Guidelines

The stated purposes of the Government Guidelines (Article 1) are "to clarify fundamental matters common to various industries for the protection of consumer privacy with regard to the use of electronic tags while encouraging the beneficial use of electronic tags, protection the interests of consumers, and promoting the acceptance of electronic tag use by the public." In other words, the Government Guidelines are intended to serve as guidelines for the protection of consumer privacy with regard to the use of electronic tags.

(6) Scope of Application of the Government Guidelines

The Government Guidelines state in Article 2 that they "establish rules that should be followed by businesses that handle electronic tags and goods with

electronic tags affixed in circumstances where electronic tags remain affixed to goods even after they have been transferred to the consumer." As can be seen in this provision, the Government Guidelines create rules concerning the protection of privacy with regard to electronic tags affixed to products that have been provided to customers. Consequently, the Government Guidelines do not apply to RFID tags that do not raise issues of the protection of consumer privacy. The Government Guidelines do not apply, for example, to RFID tags used to track the movements of wild animals, birds, and fish, RFID tags used for healthcare or medical treatment purposes, or RFID tags for police, security, and information security purposes.

(7) What Rules Apply to Situations where the Government Guidelines Do not Apply?

It must be remembered that even in situations where the government guidelines do not apply to the use of RFID tags, other rules do apply depending on the specific circumstances.

Applicable law provides that RFID tags may not be harmful to the health of employees and patients involved in the use of RFID tags. Also, when RFID tags are used for criminal investigations, all provisions of the Japanese Constitution and Criminal Code regulating the conditions for proper procedures apply. Even in circumstances where RFID tags are used with the general public in ways not related to private commerce, the principle of good faith, a general principle of civil law, will apply, and the principle of good faith may apply in the form of the duty to inform or the duty to explain, depending on the specific circumstances.

(8) Notice of Tag Use

Article 3 of the Government Guidelines, entitled Notice concerning the attachment of Electronic Tags, states: "In instances where and electronic tag is affixed to a product even after the product is in the consumer's possession, the consumer must be informed or notice provided in advance that an electronic tag is attached to the product, the location of the tag, the nature of the tag, and the information recoded in the tag (hereinafter referred to as "Electronic Tag Information") or the product or its packaging must include labeling that informs the consumer of the Electronic Tag Information. Efforts shall be made within stores in a manner that consumers are aware of such information or notice."

Consumers make the decisions whether they will provide access to products with RFID tags and have the right to deny such access based on their decisions. This means that they must be notified of the presence of RFID tags. Stealth deployment is as a general principle not permitted. The act of displaying products with RFID tags without informing consumers for purposes that go beyond the scope necessary for surveying consumer trends or security, for example, likely constitutes unlawful conduct. In such cases, the failure to provide notice because more accurate statistics can be obtained when notice is not provided based on a specific statistical survey theory would probably not be

sufficient grounds. The assertions that all consumers must consent to all requests for statistical surveys, surveys of consumer trends, and tracing of purchased products, except in cases of legal obligation and that consent is provided automatically are not legally supportable and are untenable from the perspective of protecting consumers.

It seems likely that that provision of notice by electronic means such as posting the information on a Web site is not sufficient. Consumers make purchasing decisions based on products that they can hold in their hands on the spot, so it is necessary to make it possible for consumers to confirm the presence of RFID tags with their own eyes on the spot. Accordingly, Article 3 explicitly provides for a labeling method: "the product or its packaging must include labeling that informs the consumer of the Electronic Tag Information."

Article 3 of the Government Guidelines is closely related to the protection of privacy and personal information, and therefore, it is also directly related to Article 4, entitled Reservation of the Consumer's Rights concerning Reading of Electronic Tags. This means that whether consumers opt in or opt out, if consumers are not aware of the presence of RFID tags, they are not able to make any decisions. When exercising the right specified in Article 4 of the Guidelines, consumers must of course be notified about the presence of RFID tags, and therefore, we can conclude that RFID tags to which Article 3 does not apply are automatically not subject to Article 4 as well.

(9) The Consumer's Right to Choose

Article 4 of the Government Guidelines, entitled Reservation of the Consumer's Rights Concerning Reading of Electronic Tags, provides: "When businesses affix to products electronic tags that remain affixed to the products after possession has been transferred to the consumer, if the consumer requests that the electronic tags be made unreadable based on an understanding of their properties, a method for making the tags unreadable at the consumer's option shall be explained or displayed in advance or indicated on the product or its packaging."

Article 4 of the Government Guidelines applies to "products [with] electronic tags that remain affixed to the products after possession has been transferred to the consumer." If the RFID tags are removed or destroyed at the time of payment, Article 4 will not apply to any legal issues that might arise after that point.

After purchasing a product with an RFID tag affixed, the consumer must be able to make the electronic tag unreadable. Some possible methods for making tags unreadable mentioned in Article 4 include interrupting communications between the electronic tag and readers by covering the tag with aluminum foil, magnetically erasing all of the information stored in the tag or such portion of the information selected by the consumer including the unique identification number or making it impossible to read the information. The methods mentioned are only illustrative and not intended to preclude the use of any other

effective method. One such effective method would be simply destroying the tags.

As seen above, the provisions of Article 4 of the Guidelines are intended to operate in tandem with the provisions of Article 3 and require that the consumer be able to exercise the right to choose, premised on the consumer's knowledge of the tag's presence. Accordingly, even if an objective system the enables consumers to exercise the right to choose to make electronic tags unreadable, if the indications of the tag's presence are not proper, the consumer will not be able to exercise this right effectively.

(10) Traceability Functions will be Unavoidably Lost

The discussion up to this point may leave those individuals who want to pursue the possibilities of product traceability with some dissatisfaction. It seems that there are even some who claim that the destruction of tags would constitute a violation of intellectual properly rights and therefore is impermissible. Such an approach, however, has no basis in law.

Ownership of products that are sold transfers completely to the purchaser, that is, the customer, and ownership to any RFID tags transfers with the transfer of ownership of the product to the customer. A customer who has purchased a product and RFID tags may treat them in any manner within the scope of the customer's rights of ownership. From the perspective of the Civil Code, a business that sells a product to a customer has no rights of control over that product.

Consequently, when a customer elects to refuse the ability to read RFID tags as stipulated in Article 4 of the Government Guidelines, the traceability of that product will be lost, but this result in unavoidable.

With the exception of special instances where traceability is legally required such as for the control of infectious diseases or for control of hazardous substances, compelling consumers to maintain the traceability of products using RFID tags is not permitted by law.

If tracing using RFID tags continues without the individual's consent, the business may be liable for tortuous conduct or failure to perform obligations, depending on the specific circumstances.

(11) Provision of Information concerning the Benefits of RFID Tags

When consumers are aware of the presence of RFID tags and decide to allow their continued use based on their right to choose, they enjoy a variety of benefits. It is likely assumed that these benefits have primarily marketing objectives and that the overwhelming majority of the benefits are to the business. The benefits to consumers, however, are not insignificant. If a consumer accesses the data stored in an RFID tag affixed to a food product, for example, and is able to check on the location of origin and information on any additives, this is a benefit to the consumer.

In contrast, if the consumer decides to discontinue the tracing functions,

various societal disadvantages will also occur.

As a result, Article 5 of the Government Guidelines, entitled Provision of Information concerning the Societal Benefits of Electronic Tags, provides: "In instances where the consumer makes electronic tags unreadable in accordance with the provisions of Article 4 and potential benefits to the consumer and society are lost such as loss of information necessary for recycling resulting in environmental safety issues or loss of automobile repair history causing an impact on safety, attempts shall be made to provide labeling explaining the loss of these benefits or other means of providing this information to the consumer."

This means that when a business wishes to continue tracing functions using RFID tags, the business has the obligation of explaining to the consumer why it wants to continue the tracing function, how it will do so, what benefits can be obtained, and who can enjoy those benefits.

(12) Handling of Information that cannot be Used to Identify Individuals

Article 6 of the Government Guidelines, entitled Handling in Instances of Linking between Personal Information Databases Stored in Electronic Computers and Electronic Tag Information, provides: "Even when businesses cannot identify individuals from information stored in electronic tags, if databases of personal information stored in electronic computers can be linked easily with information stored in electronic tags and specific individuals can be identified, the information stored in such electronic tags shall be handled as personal information in accordance with the Personal Data Protection Law."

This refers to Article 2 Paragraph 1 of the Personal Data Protection Law, which defines personal information in the following manner: "Information concerning a living individual that allows a specific individual to be identified based on the information included such a name and date of birth (including situations in which other information that would make identification of specific individuals possible can be easily accessed) ."

Therefore, when any information is stored in an RFID tag, even when the information concerns an individual, if the information is not sufficient to identify specific individuals, the recorded information does not correspond to "personal information." Such an instance would be records of ID consisting entirely of numbers and codes. When such IDs can be combined with information outside the RFID tag and specific individuals can be identified, however, then the information is converted to "personal information." This would be the case where IDs read by a RFID reader are transferred to a database system and by referring to other information in a personal information database, and specific individuals can be identified or charged fees. In anticipation of this type of situation, Article 6 of the Government Guidelines provides warning that when the information stored in an RFID tag and information stored in a personal information database are linked in a manner that functions to allow identification of specific individuals, the Personal Data Protection Law.

Of course, when personal information is stored in an RFID tag, the Personal Data Protection Law applies. Also, even when the information is not linked to a personal information database, if linking the information stored in an RFID tag and a database (other than a personal information database) outside the tag or device makes it possible to identify specific individuals, the Personal Data Protection Law will apply. Thus, it is important to keep in mind that the Personal Data Protection Law applies to many situations other than linking between information stored in RFID tags and personal information databases.

In all of these cases, the business that operates the RFID tag and that handles the personal information must notify to the individual or disclose publicly the purpose of obtaining the personal information (Personal Data Protection Law Article 18), and unless the individual consents, may not use the information for any purposes other than those notified or disclosed (Article 16). Such businesses must also take appropriate measures for managing securely personal information (Article 20) or use RFID tags in such a manner that it is possible to fulfill the other obligations imposed on businesses that handle personal information as specified in the Personal Data Protection Law.

(13) Obligations in Situations where the Personal Data Protection Law Does not Apply

Article 6 of the Government Guidelines imposes obligations on businesses that handle personal information to which the Personal Data Protection Law applies. Even in cases where the number of records is too small to be a business that handle personal information under the law, persons who acquire and use personal information are nonetheless under an obligation to protect that information under Article 3 of the Law.

Article 7 of the Government Guidelines, entitled Limitations on the Collection and use of Information when Personal Information is Recorded in Electronic Tags, provides: "Businesses that handle personal information recorded in electronic tags shall attempt to notify the individual of the purpose of use or disclose the purpose when collecting and using personal information, regardless of the number of personal information records handled. If the information is to be used for any purpose other than the stated purpose, the business must attempt to obtain the individual's consent."

This provision corresponds to the provisions of Article 16 and 18 of the Personal Data Protection Law, but it is not intended to make the Personal Data Protection Law directly applicable.

Article 7 of the Government Guidelines refers only to situations where personal information is stored in RFID tags, but like Article 6 of the Guidelines, even when the information stored in an RFID tag does not identify a specific individual, if it can be linked to an external database in such a manner that allows for the identification of specific individuals, Article 7 of the Guidelines will apply by analogy.

(14) Ensuring the Accuracy and Security of Recorded Information

Article 8 of the Government Guidelines, entitled Ensuring the Accuracy of Personal Information Recorded in Electronic Tags, provides: "Businesses that handle personal information recorded in electronic tags shall attempt to fulfill the following conditions with respect to personal information recorded in electronic tags, regardless of the number of personal information records handled." Three conditions are specified.

1. The business shall maintained accurate and up-to-date information as necessary in consideration of the purposes and content of the personal information recorded in electronic tags.
2. Upon request from a consumer, the business shall disclose personal information concerning the consumer recorded in electronic tags and any personal information concerning the consumer that is linked to identifying information stored in electronic tags.
3. The business shall prevent any loss, damage, tampering of, or improper disclosure of information recorded in electronic tags.

This provision corresponds to Articles 19 (ensuring the accuracy of data) , 24 (public release of matters concerning personal data) , 25 (disclosures) , 26 (correction) , 27 (suspension of use) , and 27 (security and management measures) of the Personal Data Protection Law.

Of these obligations, it is thought that ensuring accuracy and implementing security and management measures can be carried out primarily through technological and management responses, and technological responses are particularly important. The risks when information recorded in electronic tags is not encoded have long been pointed out, but this does not mean that there are no concerns as long as data is encrypted.

In contrast, disclosure and correction are primarily management issues, and a business that does not adopt thorough management regulations and create organizations that make possible the implementation and enforcement of those regulations cannot be said to have fulfilled the conditions specified in Article 8 of the Government Guidelines.

(15) Appointing Information Managers

Article 9 of the Government Guidelines, entitled Appointment of Information Managers, provides: "Business shall appoint information managers and shall make publicly available contact information for such managers to ensure the proper management of information for the protection of privacy with regard to electronic tags and the appropriate and rapid handling of complaints."

Creating systems for handling complaints concerning the use of RFID tags is properly seen as falling within the scope of due care of a good manager, and if this duty is not performed, the party may be liable under the Civil Code for failure to perform obligations or tortuous conduct. This is also true if the public disclosure of contact information is inadequate and as a result complaint

handling does not function adequately.

(16) Provision of Accurate Knowledge and Information concerning RFID

The final article of the Government Guidelines, Article 10, entitled Provision of Explanations and Information to Consumers, provides: "Businesses shall provide information concerning the electronic tag usages, properties, benefits, and detriments to related organizations such as industry organizations and government agencies so that consumers can have an accurate understanding of electronic tags and make decisions concerning their own handling of electronic tags, and shall strive to promote consumer understanding of electronic tags."

Publicity activities that emphasize only the benefits of electronic tags and intentionally attempt to conceal their disadvantages not only violate these guidelines, may also constitute a violation of the Consumer Contract Law. Developers of RFID technologies and other engineers should bear this point in mind.