Smart ID and Privacy in Japan

Legal Issues of Tracking Using Radio Frequency Identification (Electronic Tags)

Takato Natsui
Professor, School of Law, Meiji University, Tokyo, Japan
Practicing Lawyer, Asuka Kyowa Law Firm, Tokyo, Japan
sumwel_h@kisc.meiji.ac.jp

Abstract

Smart ID refers to identification or authentication by means of a radio frequency identification (RFID) system. This is typical example of electronic identification measures. RFID is and will remain the most important device in this area, today and in the future. Such identification devices can be attacked easily by persons with criminal intent, however, and there are many cases, for instance, of ID theft and theft of credit card numbers on the Web.

Such ID theft may cause violations of privacy, give rise to various types of security issues, and lead to further economic crimes. Moreover, ID theft threatens the integrity of computer systems and other important activities on the Internet including electronic commerce and electronic authentication.

Traceability functions are themselves a key issues concerning privacy protection, especially in relation to RFID. Such discussions are very important. But at the same time, it may be more important to establish a more effective legal means—both in the enactment and enforcement of laws to prevent and punish such criminal conduct as ID theft and similar unlawful behavior.

These are common issues affecting all people who live in an advanced Information Society. We must examine these matters as soon as possible.

Thus, new legislation may be necessary on these issues, but such legislation shall be harmonized with relevant treaties and international agreements.

I would like to present outlines of Japanese laws and cases, point out important problems, and discuss my perspectives on these issues.

Key words

Smart card, RFID, electronic tag, privacy, security, encryption, ID theft, interception, communication

1. Introduction: Current Status

Smart ID refers to identification or authentication systems using radio frequency identification (RFID) systems, also know as the electronic tags or electronic bar codes. RFID systems are among the most attention-gathering electronic devices today as a means of joining the network world with the real world[1].

In Japan, many RFID systems are already used in the various area, for instance for

[1] *RFID In Retail: The Future Is Now*
http://www.mwvis.com/downloads/rfid_future.pdf

the purpose of preventing thefts in the bookstores or music CD shops (mainly installed inside of paper Tags or small plastic cases) or various types of payment IC cards (mainly installed inside plastic cards or credit cards; so-called smart card[2])[3].

Of course, RFID systems are not implemented with every type of smart card, but in Japan, there are many types of smart card in which RFID systems or radio frequency functions have been installed[4]. For instance, "Suica" (this plastic card is a kind of electronic wallet card system with an RFID function)[5] and "Edy" (this plastic card is a kind of an electronic money system with an RFID function; in many cases, Edy cards have other functions such as credit card or flight mile points card)[6] are very popular with the Japanese people (especially in the Tokyo area).

In addition, the Japanese government introduced a smart card system with a radio frequency identification function as the national ID card[7].

RFID is put into practice through the use of extremely small IC chips, and although internal memory capacities are limited, considering the rapid pace of technological innovation relating to circuit integration, there is little doubt that in the near future the memory capacity as well as the calculating and communication capabilities of RFID devices will increase dramatically and all the current functions of conventional computers will be incorporated into small ICs. Although some hold the opinion that because current RFID memory capacities are small, the risk of problems such as privacy violations are relatively low, this view fails to comprehend the current status and pace of technology development, leading to the unavoidable conclusion that such opinions indicate a profound lack of imagination concerning the future. Japanese companies are currently conducting product development with an emphasis on RFID miniaturization[8], but we must not overlook the fact that overseas the focus of development is not just on miniaturization but is also on enhancing RFID functions.

---

[2] ISO/IEC 7816

[3] The IDTechEx Web Journal, *Smart Labels Analyst*, Issue 21, October 2002
http://www.idtechex.com/slaoct02.pdf

[4] *Specification of IC cards with contacts complying with Japanese Industrial Standard*, July 1998, Version 1.1, Japan Ic Card System APplication council (JICSAP)
http://www.jicsap.com/stdwork/V1.1E.pdf

[5] *Introduction and Future Development of Suica Non-contact IC Card Ticketing System* by Akio Shiibashi
http://www.jrtr.net/jrtr32/pdf/f20_shi.pdf

[6] *The "Edy" prepaid e-money service launches*, Nov 8, 2001
http://ne.nikkeibp.co.jp/english/2001/11/1107edy_mobile.html

[7] See *Smart Card for Secure and Convenient Life*
http://magazine.fujitsu.com/vol52-6/v52n6a-e.html
See also *SmartCord, IST-2000-30168, Co-ordination mechanisms for eEurope Smart Card Charter implementation*
http://www.electronic-identity.org/download/Athens-eESCMeeting.pdf
and *IT Strategic Headquarters* in the Prime Minister Cabinet of Japan
http://www.kantei.go.jp/foreign/policy/it/index_e.html

[8] *Hitach/Maxell; In some applications - size will matter.For these, we use one of the world's smallest passive read/write chips.*
http://www.climarque.co.uk/passive/coil_on_chip.htm

Thus, the social potential of RFID is abnormally high, leading to apprehension concerning the various legal issues arising from being in a society where RFID is put into practice[9]. The fact the RFID tags are extremely small, electronic devices may also give rise to legal issues. Some potential legal issues include:

- Violations of privacy rights
  The combination of the product identification functions of RFID and the individual identification functions of electronic marketing including Point of Sales (POS) and credit card payment through data matching may lead to privacy violations[10].
- Disclosure and violation of confidential corporate information (Trade Secrets)
  Through the exact same mechanisms that give rise to the potential for violations of individuals' privacy by means of RFID, there is also the risk of disclosure and violations of the confidences of corporations, especially of trade secrets.
- Electromagnetic interference and allocation of the electromagnetic spectrum
  RFID are electronic devices that use minute radio waves, and as they proliferate, there is a danger that interference will occur. Also, there is currently no agreement whatsoever concerning what frequencies to use, posing the risk of complex problems including international trade friction[11].
- Code standards
  There is no international agreement on standards for the codes used by RFID systems, which may result in major obstacles to distribution and management including electronic commerce as well as payment[12].
- Environmental issues
  RFID tags contain heavy metals and other pollutants, and because they are extremely small, recovery or recycling is not feasible. As a result, pollutants contained in RFID tags may be discarded and accumulate in the natural environment and social sphere.
- Harm to human health
  RFID tags are devices that transmit and receive electromagnetic waves, and the impact of radio waves on human health is still unknown. Also, since they are extremely small metallic devices, if they can not be recycled or recalled completely after use, there is a risk that RFID tags or pieces of them could be inhaled, leading to potential conditions such as pneumoconiosis. RFID tips that are buried in a wall or

---

[9] See Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels, *White Paper, RFID Systems, Security & Privacy Implications*, published November 1, 2002
http://www.autoidcenter.org/research/MIT-AUTOID-WH-014.pdf

[10] See CASPIAN's Web Site. CASPIAN is one of the most well-known privacy advocate organizations in the U.S. It promotes privacy protection relating to RFID.
http://www.nocards.org/

[11] *Transmission Interference White Papers*
http://www.itpapers.com/cgi/SubcatIT.pl?scid=905
See also *Auto-ID Center UHF Class 1 RFID, RF and Logical Communication Interface, Specification* version 1.0.0
http://www.alientechnology.com/library/pdf/WP_AlienEPC_Class1UHFSpecFeedback.pdf

[12] About RFID standard in Japan, See Ubiquitous ID Center's Web Site
http://uidcenter.org/

furniture or under the road[13] can become potential pollutants. But this problem has not yet been analyzed and examined sufficiently.

- Products liability
  RFID tags are electronic devices, and consequently, they correspond to movables or personal property under the Japanese Civil Code. As a result, the Products Liability Law applies directly to all technical problems including bugs in the software incorporated within tags. This is also true under similar laws in foreign countries.
- Security
  RFID systems themselves are a type of independent computer system and include internal operating systems and software. As a result, infection of RFID systems by viruses and hacking are theoretically possible. At this time, however, there is no technological means of bug fixing internal RFID programs or upgrading the internal software. It is possible that this will be legally deemed a "defect" of the systems[14].

These are some of the potential legal issues. I this paper, I will address primarily issues concerning privacy relating to the RFID, focusing on the application of current legal systems and laws.

2. The Mechanism by Which Privacy Issues Arise

2.1 Comparison with printed bar codes

As in the case of tracking using software such as spyware, we can understand the issues of privacy as they concern RFID systems to be a part of the larger problem of violations of privacy through monitoring.

It is generally believed that the idea that RFID systems make possible tracking derives from the fact that they are primarily wireless devices. This idea, however, is not correct.

In fact, tracking in some sense is possible in any environment in which some "object" with tracking ID functions using a wireless or cable network can match data with individual identifications. For example, even in the case of bar codes printed on paper, tracking functions can be implemented by data matching product information with credit card payment information. The issue of privacy violations from bar codes printed on paper is not sees as more significant because of the lack of attention by legal scholars and the lack of interest by consumers.

Accordingly, the issue of privacy with respect to RFID is not one that arises from RFID, and is no more than an existing issue that has been expanded and made more apparent by RFID.

Similar problems arise from spyware that has been intentionally installed and can

---

[13] For instance, the Yaoyorozu Project of Japan is planning and examing such burying of RFID tips and other similar devices in walls and buildings, carpet, furniture, automobiles and other consummer goods, banknotes, checks and other authentication instruments, and under roads.
See *Background and Aims of Establishment* of Yaoyorozu project
http://www.8mg.jp/en/outline_goals01.htm

[14] See *Privacy and Authentication in Low-Cost RFID Tags, Ari Juels, RSA Laboratories*
http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pt-rfid/pt-rfid.pdf

also arise from the misuse of intelligent household appliances.

2.2 Comparison with ordinary computer systems

RFID is a small IC tip but it is also a kind of computer system[15]. Thus everything that can be performed relating to computer systems can be realized on RFID systems as well.

If any data involved in RFID is not encrypted, many types of privacy violations could be caused by hacking the data recorded inside RFID devices.

Of course, most RFID systems have a security mechanism (in many cases, encryption technology is incorporated into RFID tips physically). However, there is no entirely complete encryption technology or encrypted data. An old Chinese proverb says that there is no perfect shield that can protect against every halberd and there is no perfect halberd that can pierce every shield (i.e., logically, a perfect shield and a perfect halberd can not exist at the same time). If an RFID system does not have a practical and effective security system, the possibility of illegal access to RFID tips and decryption of encrypted data in RFID can not be completely prevented.

On the other hand, privacy violations can take place within equipment and data servers outside of the RFID system itself. Data collected through RFID is usually decrypted in an RFID reader device or a data server system. Thus, interception of decrypted data can take place outside the RFID system itself. For instance, an illegal spy device attached to an RFID reader device such as an illegal skimmer[16] for credit card readers may be developed and used in the future.

2.3 Location Data Tracking

In addition to the above, if tracking an RFID location is possible, then the privacy of location can be violated. For instance, a good wireless wave sensor device can intercept an electronic emission from RFID tip or other similar device, and if the ID of a user or the ID of specific good can be distinguished or identified by such interception, then data matching such as the location of specific person or good can be automatically generated, possibly in combination data with GPS information. Such data matching may be done without the consent of the individual who is in possession of something to be communicated by wireless to which RFID tips or similar devices are attached.

3. Parsing the Issues

When RFID is used simply to identify products and services in ways that bear no relationship to the general public, the issue of privacy violations does not arise, so it is necessary to understand these issues by separating them by context.

For example, when RFID is used as a tool to trace the country of origin of imported beef as a countermeasure against mad cow disease (BSE)[17], a tool to trace the country of

---

[15] IEEE Pervasive Computing Magazine, *Pervasive Computing Goes the Last Hundred Feet with RFID Systems*
http://www.computer.org/pervasive/pc2003/b2009.pdf

[16] The United States Depertment of Justice, *Public Advisory: Special Report for Consumers on IDENTITY THEFT*
http://www.usdoj.gov/opa/pr/2003/May/publicadvisory1.pdf

[17] e.g. *National Food Animal Identification Task Force, a united effort involving industry and government*

origin of imported agricultural products to protect consumers from problems arising from agricultural chemicals, a tool to trace the country of origin of marine products to prevent problems resulting from mercury poisoning, or as a means of controlling components and processes within a plant that is located far from consumers, there is no possibility of privacy violations arising from these uses themselves. To the extent that use is limited to these types of applications, RFID can be extremely effective for control purposes.

Of course, once meat or manufactured products that have RFID tags attached pass into the hands of the consumer, issues of privacy violations may arise in all subsequent phases (retail phases)[18]. As will be shown below, these issues, however, arise as a result of data matching and are not generated by RFID itself.

On the other hand, when RFID is using with human personal ID, direct privacy violation may be taken place, for instance in the area of a transportation security[19].

4. Privacy Violations through Data Matching

It is also possible, however, that issues concerning privacy violations resulting from data matching will arise in instances where RFID is used not to identify people, but to identify goods and services.

To the extent that RFID systems include identification functions, such problems may arise in retail payment situations and in all subsequent stages. This is one of the most significant criticisms of RFID with respect to privacy violations accomplished through tracking.

The same issues, however, arise with bar codes printed on paper. For example, bar codes printed on books can result in permanent tracking if they are matched with customer account numbers at the recycling stage by the recycling business. This type of issue, however, can be avoided Law through the legal control of businesses that handle personal information such as bookshops and recycling companies.

In contrast, the status of the issue with respect to RFID may be somewhat different. That is, as long as RFID functions are not terminated, RFID systems are electronic devices that have the ability to detect tags using radio waves. Consequently, persons other than businesses that handle personal information will be able to trace products with RFID tags that specific individuals are carrying through private or public means of detection. In this context, issues concerning privacy violations that are not covered the Law for the Protection of Personal Information (law No. 57 of 2003) [20]may arise.

---

http://www.animalagriculture.org/id/TaskForce/nat_foodanimalidtaskforce.asp
See also *Animal Identification & Information System, The Need for Identification*
http://www.wiid.org/index.php?action=why
and *NIAA National Identification Task Force*
http://www.animalagriculture.org/id/TaskForce/National_ID_Plan_November.pdf

[18] *Privacy advocates call for RFID regulation by Alorie Gilbert*, CNET News, August 18, 2003, 8:40 PM PT
http://news.com.com/2100-1020_3-5065388.html

[19] *Cargo Security Overview, Technologies, Government and Customs Initiatives, Global eye for transport research*, November 2002
http://www.eyefortransport.com/report/cargosecurity.pdf

[20] Administrative regulations and ordinances need to be drafted and enacted to enforce the Protection of Personal Information Law. The Japanese government must prepare such

For example, by simply carrying a detection device hidden in a briefcase or bag and approaching the subject individual in a train, it would be possible to detect all of the items that individual is carrying. In addition, if intelligent household appliances[21] were affixed with RFID tags, it would be possible to detect all of the appliances in a house from outside by the interception of emissions from wireless LAN systems or intelligent house systems or hacking into such systems.

If the RFID identifying codes detected with these types of detection devices and personal identifications were matched over networks in real time or later using batch processing, the privacy of the individual will cease to exist. When someone other than entities handling personal information performs this conduct, the Law for the Protection of Personal Information does not apply at all.

5. Technological Responses—Introduction of Functions to Terminate RFID Functions and Encryption

5.1 Functions to Terminate RFID Functions

In order to prevent privacy violations such as these, it is important first to address the hardware issues by loading physical functions into RFID systems in such a way as to prevent privacy violations, and to address the operational issues by establishing appropriate policies intended to protect privacy. Such measures can be understood as a part of the technology responses for preventing privacy violations.

Such functions are generally referred to as kill functions or deactivation functions[22]. There are two potential approaches to loading kill or deactivation functions into RFID tags.

- Physical Approaches
  In the retail context, after payment has been completed, subjecting the RFID tags to strong magnetic waves or heat rays can terminate RFID tracking functions, thereby physically damaging the tags. This is currently the most common method used when retail stores employ theft-prevention chips attached to products.
- Software and Firmware Approaches
  At the design stage, RFID standards should provide for switches to turn them on and off, and in accordance with uniform international standards, RFID functions should be shut off automatically in conjunction with the operation of being read by an RFID reader. Making the terminated functions non-restorable unless the RFID tag is

---

regulations and ordinances by June 2005.

[21] Japanese government is now promoting development and wide distribution of such intelligent household appliances.
See *Survey of Household Economy - Explanation of Survey Items*
http://www.stat.go.jp/english/data/joukyou/6.htm

[22] See *RFID 'kill' feature aims to soothe privacy fears* by Junko Yoshida, EE Times, April 28, 2003 (9:56 a.m. EST)
http://www.commsdesign.com/news/market_news/OEG20030428S0019
'Kill' switch disables Radio ID chips by Richard Shim, CNET News.com, May 6, 2003, 4:58 AM PT
http://zdnet.com.com/2100-1103_2-999794.html

processed by an exclusive RFID recycling plant in accordance with a suitable privacy policy will substantially reduce the risks of violations of privacy using RFID tracking functions.

5.2 Encryption

Encryption is an additional or supplemental but strong technological way to protect privacy in the course of operating RFID systems.

Encryption technology will be used in some parts of RFID systems; recorded data inside RFID itself, RFID reader, electronic communications between RFID tips and RFID readers as well as RFID readers and server systems (e.g. POS servers, membership management servers, the National ID servers and so on).

If fact encryption itself is not a perfect technology, but non-encrypted data or systems means naked data or systems. Such naked systems can not protect privacy and may permit illegal behavior (e.g., ID theft[23], hacking of systems, and illegal interception of communications data).

6. Legal Responses—the Needs for Legal Reforms

Under the current legal system, if legislation intended to prevent violations of privacy with respect to RFID were adopted, there would be no problem with taking appropriate legal responses. The current legal system, however, provides virtually no responses to potential issues raised by RFID systems.

6.1 Personal Information Protection Law

The Law for the Protection of Personal Information of Japan (law No. 57 of 2003) is not a privacy protection law. The law applies only to an entity handling personal information who has gathered a certain volume of such data.

The Law for the Protection of Personal Information (extract)

Article 2 (Definitions)

1. In this law, the term "personal information" means information about a living individual that contains such name, date of birth, or other description as will enable the identification of the individual (including such information as will allow easy reference to other information and will thereby enable the identification of the individual).
2. In this law, the term "personal database or the like" means a collection of information containing personal information that falls into either of the following categories:
   (1) A collection of information systematically arranged in such a way that specific personal information can be retrieved by a computer
   (2) Any other collection of information designated by a Cabinet order as being systematically arranged in such a way that specific personal information can easily retrieved otherwise
3. In this law, the term "entity handling personal information" means an entity

[23] The Federal Trade Commission: *Your National Resource for Identity Theft* http://www.consumer.gov/idtheft/

using a personal database or the like for its business. However, the term shall not include the entities enumerated below.

(1) State institutions

(2) Local public entities

(3) Independent administrative agencies (which term hereinafter means independent administrative agencies defined in Paragraph 1 of Article 2 of the General Law of Independent Administrative Agencies [Law No. 103 of 1999]) specified separately by law

(4) Special corporations (which term hereinafter means such corporations established directly by law or such corporations established by special acts of incorporation under special laws as are governed by the provisions of Item 15 of Article 4 of the Law for the Establishment of the Ministry of Public Management, Home Affairs, Posts and Telecommunications [Law No. 91 of 1999]) specified separately by law

(5) Entities specified by a Cabinet order as being unlikely to harm the rights and interests of individuals in consideration of the volume of personal information they handle and their manner of use

4. In this law, the term "personal data" means personal information constituting a personal database or the like.

5. In this law, the term "personal data held" means such personal data over which an entity handling personal information has the authority to disclose, correct, add, delete, suspend its use, erase, and suspend its supply to third parties as is specified by a Cabinet order as harming public or other interests if its presence or absence is known or as will not be erased within a period of not longer than one year that will be specified by a Cabinet order.

6. In this law, the term "person" as used with reference to personal information means a specific individual identified by personal information.

Article 15 (Specification of the Purpose of Use)

1. When handling personal information, each entity handling personal information shall specify the purpose of use of personal information (hereinafter called the "Purpose of Use") as strictly as possible.

2. Entities handling personal information may not change the Purpose of Use beyond the scope reasonability considered duly related to the Purpose of Use before the change.

Article 24 (Maintenance of the Accuracy of Data)

Each entity handling personal information shall endeavor to maintain personal data accurate and up to date within the scope necessary for the achievement of the Purpose of Use.

Article 25 (Security Control Measures)

Each entity handling personal information shall take necessary and proper measures for the control of security of the personal data it handles, including the prevention of leakage, loss, and damage.

Article 26 (Supervision of Employees)

When an entity handling personal information has an employee handle personal data, it shall exercise necessary and appropriate supervision over the employee to ensure the control of security of the personal data.

Article 27 (Supervision of Trustees)

When an entity handling personal information entrusts a person or entity with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the control of security of the entrusted personal data.

Article 32 (Collection of Reports)

The competent minister may have entities handling personal information report on the handle of personal information to the extent necessary for the implementation of the provisions of this section.

Article 33 (Advice)

The competent minister may advise entities handling personal information report on the handle of personal information to the extent necessary for the implementation of the provisions of this section.

Article 34 (Recommendations and Orders)

1. Where an entity handling personal information has violated any of the provisions of Articles 16 to 18, Articles 20 to 27, or Paragraph 2 of Article 30, if the competent minister considers it necessary for protecting the rights and interests of individuals, the competent minister may recommend the entity handling personal information to cease the violation and take necessary measures to redress the violation.
2. Where an entity handling personal information having received a recommendation under the provisions of the preceding paragraph does not take the recommended measures without due reason, if the competent minister considers that any infringement on the important rights and interests of individuals is imminent, the competent minister may order the entity handling personal information to take the recommended measures.
3. Notwithstanding the provisions of the preceding two paragraphs, where a entity handling personal information has violated any of the provisions of Paragraph 1 or 2 of this Article, Articles 20 to 22, or Paragraph 1 of Article 23, if the competent minister considers it necessary to take measures urgently in view of the fact of infringing on the important rights and interests of individuals, the competent minister may order the entity handling personal information to cease the violation and take necessary measures to redress the violation.

Article 56 (Penalty)

A person who disobeys orders issued under Paragraph 2 or 3 of Article 34 shall be liable to imprisonment of not more than six months or to a fine of not more than 300,000 yen.

Article 62 (Penalty)

A person who does not make a report required by Article 32 or 46 or who has made a false report shall be liable to a fine of not more than 300,000 yen.

Persons other than entity handling personal information, however, could commit many potential violations of privacy from the use of RFID. Thus, the Law for the Protection of Personal Information should be amended and legislation adopted to create a law that protects ordinary privacy.

6.2 Unauthorized Computer Access Law

In order to make legal responses to violations of privacy committed by detecting data stored in the internal memories of RFID tags, it is necessary to prohibit this type of conduct. The current Unauthorized Computer Access Law (Law No. 128 of 1999) applies only to unauthorized access by means of telecommunications lines to network computers connected to telecommunications lines[24]. Consequently, this Law does not apply to acts of unauthorized access to RFID tags, which are a type of standalone computer. The Unauthorized Computer Access Law should immediately be amended to make it applicable to unauthorized access of standalone computers as well.

Unauthorized Computer Access Law (extract)

Article 3 Prohibition of acts of unauthorized computer access

1. No person shall conduct an act of unauthorized computer access.
2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:
   (1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);
   (2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via

[24] On unauthorized access crimes in Japan, See, Japanese Information Security Status, February 3, 2003, Kei Harada, IT Security Center (ISEC), Information-technology Promotion Agency, Japan (IPA)
http://www.opengroup.org/sfo2003/proceedings/plenary_monday/harada.pdf

telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);
(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.

Article 4 Prohibition of acts of facilitating unauthorized computer access
No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

Article 6 Assistance etc. by Metropolitan and Prefectural Public Safety Commissions
1. The Metropolitan or Prefectural Public Safety Commission (each of the Area Public Safety Commissions in case of the Areas (that means the Areas mentioned in Article 51, paragraph 1, main part, of the Police Law (Law No. 162 of 1954); the same shall apply hereafter in this paragraph) except the Area which comprises the place of the Hokkaido Prefectural Police Headquarters: the same shall apply hereafter in this Article), in case an act of unauthorized computer access is recognized to have been conducted and if, for the purpose of preventing a recurrence of similar acts, assistance is requested by the access administrator of the specific computer involved in that act of unauthorized computer access, attaching to such request any documents or articles regarding referential matters, such as the situations of operation and management of that specific computer at the time of that act of unauthorized access, shall provide, when it deems such request reasonable, that access administrator with assistance, including provision of relevant materials, advice and guidance, so that necessary emergency measures can be properly taken in accordance with the modus operandi of that act of unauthorized access or its cause to protect that specific computer from acts of unauthorized access.
2. The Metropolitan or Prefectural Public Safety Commission may entrust to a person to be stipulated by National Public Safety Commission Regulation with all or part of the work of implementing a case analysis (which means making a technical study and analysis on the modus operandi of the act of unauthorized computer access relating to that request and the cause of such act; the same shall apply in the following paragraph) which is necessary for the providing of the assistance mentioned in the preceding paragraph.
3. A person who has engaged in the work of implementing a case analysis

entrusted by the Metropolitan or Prefectural Public Safety Commission in accordance with the preceding paragraph shall not reveal secret he or she has learned with regard to such implementation.
4. The necessary matters other than those stipulated in the preceding three paragraphs relating to the assistance mentioned in paragraph 1 shall be stipulated by National Public Safety Commission Regulation.

Article 8 Penal provisions
A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:
(1) A person who has infringed the provision of Article 3, paragraph 1;
(2) A person who has infringed the provision of Article 6, paragraph 3.

Article 9 A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

6.3 Payment Card Protection by Penal Code

In addition, Article 163bis of the Penal Code (Law No. 45 of 1907) prohibits any production of electromagnetic records relating to credit cards or similar IC cards used for payment with intention of fraud, and Article 163tre prohibits possession of illegally produced credit cards or similar IC cards used for payment.

Thus, the Penal Code of Japan can protect RFID tips relating to IC cards used for payment. However, these provisions apply only to physical credit cards used for payment. If the RFID cards don't have such payment functions, then these provisions of the Penal Code do not apply. There is no law that prohibits illegal production of IC tips itself.

Penal Code of Japan (extract)

Article 163bis Illegal production and use of an electromagnetic record on payment card
1. Any person who with the intention of misleading any business management of others, illegally produces such an electromagnetic record as to be provided for the use of the business management which consists credit card or other similar payment card for any fee or charge shall be punished with penal servitude for not more than ten years or a fine for of not more than one million yen. Any person who illegally produces such an electromagnetic record as to be provided for the use of debit card for withdrawal shall be same.
2. Any person who with the intention of paragraph 1 provides such an electromagnetic record as to be provided for the use of the business management shall be punished with the same penalty of paragraph 1.
3. Any person who with the intention of paragraph 1, transfer, lend or import a card which has an electromagnetic record illegally produced set forth in paragraph 1 shall be punishable with the same penalty of paragraph 1.

Article 163tre Illegal holding of an electromagnetic record on payment card
Any person who with the intention of paragraph 1 of previous Article, hold such a card set forth in paragraph 3 of previous article shall be punished with penal

servitude for not more than five years or a fine for of not more than 500 thousands yen.

6.4 Illegal Interception of Wireless Communications

The current Wireless Communication Law (Law no. 131 of 1950) includes penal provisions intended to protect the secrecy of communications. The law prohibits any theft-use and disclosure of information without consent or legitimate grounds (Article 109). However, this provision can be applied only to information that is handled by wireless communication stations (thus, it is not applicable to independent wireless electronic devices), and any illegal interception to wireless communications is not be punishable under the current law.

As a result, the Somu-sho (Ministry of Public Management, Home Affairs, Posts and Telecommunications) is currently preparing an amendment bill to punish interception of encrypted wireless communications.

6.5 Location Data

A major issue for many legal scholars has been whether location data should be considered a part of privacy data or not. Concerning this issue, a new EU directive [25] clearly indicates that location data can be processed only with the consent of users or subscribers.

EU Directive on privacy and electronic communications (extract)

Article 9

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.
2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.
3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

In Japan, however there is no law that directly governs the protection of location data.

7. Adoption of Appropriate Privacy Policies

Application of the Law for the Protection of Personal Information will require the adoption of privacy policies that conform to the Law. Such policies could require, for instance, the consent of the subject prior to the collection of personal information or notice of the purpose of collecting the information. Thus, a policy should be adopted that when personal information is collected using RFID or RFID and data matching, clear notice or notification that personal information is being gathered using RFID must be provided.

Also, even in cases that the Law for the Protection of Personal Information does not apply directly, policies intended to protect privacy on a level that can be accepted globally should be adopted including the fundamental principles for the protection of privacy indicated in the Law.

Accordingly, in any of the above situations, stealth application of RFID should be prohibited. When RFID is actually used, clear notice that RFID is being used to collect some type of information must be provided, just as in the case of security camera use. When RFID tags are incorporated into products or product labels, for example, the product or label should indicate the presence of the RFID tag. Similarly, when RFID tags are placed in home appliances or furniture, they should be labeled in large text on the surface so that everyone will be aware of the presence of the tags.

The above are what I believe to be the most important policies that should be adopted in the retail context[26].

8 Conclusions

We are facing a new crisis in the information society. RFID systems and similar electronic devices are the most important elements of this issue.

I would like to emphasis that there is no perfect technological means, perfect law or perfect privacy policy that can completely prevent privacy violations in relation to RFID systems and similar electronic devices. Technological means, laws, and privacy policies each have their own unique limitations. These are all complementing means, not solitary or independent measures to protect privacy.

If, however, one recognizes the seriousness of privacy violations in relation to RFID and similar electronic devices, then everyone can agree that more progress in means of protection and security technology, more effective laws and regulations, and more practical and meaningful privacy policies must be developed.

Thus, it is essential that we understand the details of the technological aspects of RFID and the limitations of current laws and privacy policies. The reality in Japan concerning this issue may serve as a good example to investigate and resolve these issues.

---

[26] *An RFID Bill of Rights* by Simson Garfinkel, October 2002
http://www.simson.net/clips/2002.TR.10.RFID_Bill_Of_Rights.htm