Traceability System using RFID and Legal Issues

Takato Natsui
Professor at Meiji University, Tokyo, Japan
Asuka-Kyowa Law Firm, Tokyo, Japan

[Abstract]

This paper presents the privacy issues, anti-trust problems and theft of trade secrets potentially caused by such tracking system and traceability function as database systems using RFID.

Also this paper presents some resolutions to prevent such problems based on both technological measures and good policy making.

[Keywords]

Anti-trust, Personal Information, Privacy, RFID, Traceability, Tracking, Trade Secret

1. Introduction

"*Electronic Product Code (EPC) is an emerging system that uses Radio Frequency Identification (RFID) for the automatic identification of consumer products. RFID is now being used in everything from automobiles to security pass cards, and it serves a variety of purposes. One of its widespread uses is in devices such as EZ Pass in the US and Liber-T in France that speed the passage of autos through highway toll booths.*" - EPC Guideline[1]

As it mentioned above, RFID device is a really new technology in the consumer products area. Of course RFID technology itself is not a new one. This technology has been used in the military area during past 50 years. For instance, RFID technology has been applied to distinguish the fellow air-fighter with enemy's air-fighter automatically. However applications of RFID technology are really emerging phenomenon in the private sector.

As long as it should be used only for military purpose, RFID technology would merely cause infringements of private rights. On the contrary in a private sector, there exists some possibility of legal issues that can be taken place by RFID applications[2]. Privacy invasion, illegal leakage of trade secrets and anti-monopoly issues may be involved in such legal issues.

However such problems can be taken place not by using of RFID chip itself but mainly by

[1] http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html
[2] Takato Natsui, *Smart ID and Privacy in Japan*, 2003
http://www.bakercyberlawcentre.org/2003/Privacy_Conf/papers/Day1/Natsui.pdf

operation of traceability system using RFID devices.

This paper shows some mechanism of causing such legal issues and proposes some private recommendation to prevent or moderate such legal issues.

2.0 What is RFID?

RFID is electronic chips or application devices using such chips which have a function of radio wave communication and of identification of such chips or devices.

There are many types of RFID device.

Some RFID devices have a memory function (data storage mechanism) inside such device itself, and some devices don't have such a function. Also there exist an active RFID and a passive RFID. The active RFID can send electronic wave from the RFID. On the contrary the passive RFID can't send any electronic wave by itself; such RFID can only reflect any electronic wave from a RFID reader/write system.

However in both cases, existence and identification of specific RFID device can be identified by the RFID reader/writer system (Fig. 1).

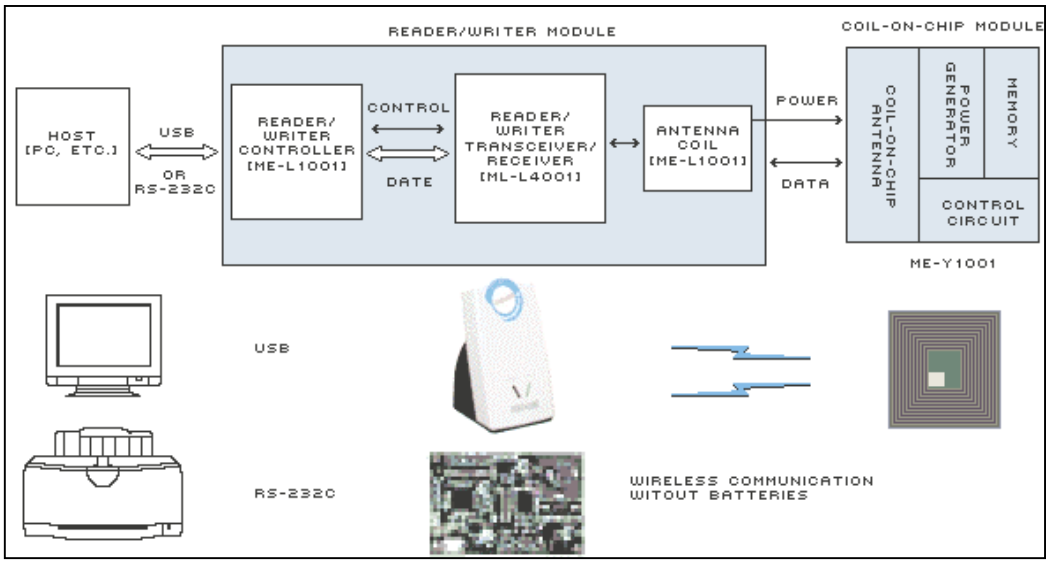

Fig 1: Hitachi RFID System Configuration

3.0 What is Tracking Data and Traceability?

As an application system using RFID devices, traceability system can be developed.

Traceability means a function for tracing specific items which would be distributed through some different ways. For instance, to avoid and suppress any BSE problem (cow disease), traceability systems have been developed and implemented in some countries. In many cases, such systems are using paper Tags or brands on cows, but in some cases RFID Tags have been used for

purpose the purpose of automatic identification of cow. The paper Tags, brands and RFID Tags are functioning as an identifier in such systems.

Every traceability system shall catch and identify any identifiers in the course of operation.

Tracking data means such identifier data itself or such data as that can identify the identification of such identifier and its location at the time. Tracking data may be collected in different events using same ID, and can be controlled by traceability system.

Therefore traceability means a capability of controlling tracking data or collecting tracking data.

4.0 Mechanisms of Causing Issues

Traceability system can identify which is/was/had been the location of specific item and what course such item follows/followed/had followed automatically.

To realize such a function tracking data shall be collected in some important spots. For example, in the case of consumer products, such spots can be set at the manufacturer, supply chains, retail shops and private houses (post sale). If such traceability system is functional then manufacturer or supply chains can retrieve such tracking data and identify the following of specific items.

Also if such tracking data stored in any database systems can be matched with any personal information or business corporation data then one can know who owns/owned/had owned such items or is/was/had been using such items as the result of data matching using such traceability system (Fig. 2).

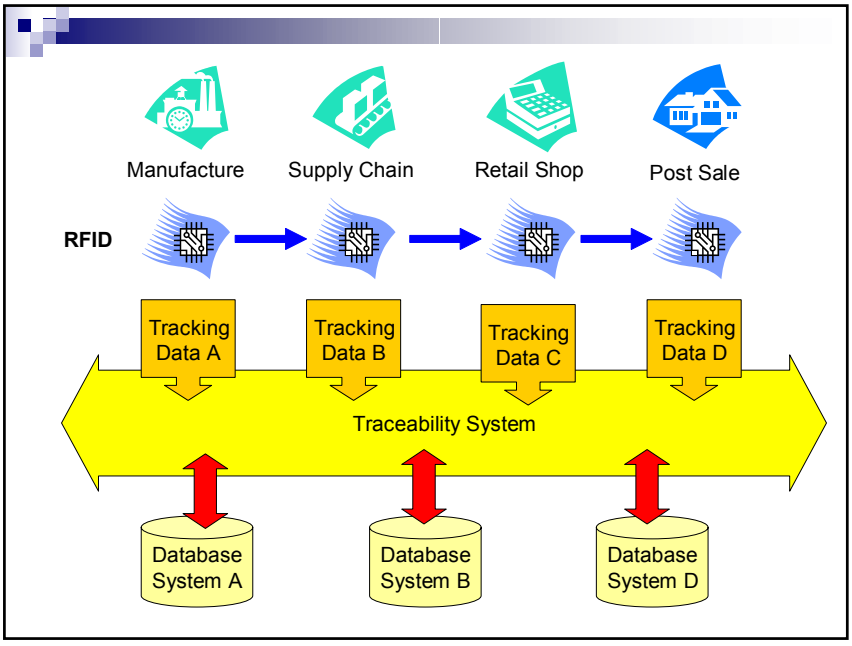

Fig. 2: Conception of Traceability System

These can be taken place by using both active RFID devices and passive RFID devices. Tracking data as an electronic wave can be collected by RFID reader/writer systems. If there is no RFID reader/writer in the world then no tracking data can be collected in any way.

This is similar to monitor cameras for security purposes on the street. If there is no monitor camera on the street then no one can be taken his/her photo and there is no privacy issue caused by any photos. Every systems or devices using RFID are same with this. Even if the RFID device is active type, any electronic wave emitted from such RFID device can not be recognized and identified without any RFID reader system.

Thus important point to find and understand causes of every legal issue exists mainly at the RFID reader/writer side (collector side) rather than at RFID chip side (identifier item side).

By the way, as long as such a traceability system shall be used based on legitimate policies or rules for administrators and users, as well as adequate security system shall be implemented in such a traceability system, possibility of legal issues caused by accessing such systems may be relatively rare.

However in special situations, even if such a system is designed and developed in accordance with such legitimate policies or rules, some special legal issues can be taken place.

For instance, in the case of active RFID Tags, many people can catch electronic wave from such Tags by using all-purpose RFID reader/writes and recognize what kind of good he/she is possessing. And also if criminals have a good skill of hacking then they can modify or remove any recorded data stored in specific RFID chips by using with specific RFID reader/writer devices without any consent or right. Such a usage of RFID reader/writer may be an illegal activity in many countries.

Of course, if the traceability system itself is hacked by criminals or misused by legitimate users (e.g. manufacturer, distributor, shop owner) then all personal data stored in such system may face a serious privacy invasion.

In addition, the structure of RFID chip itself has no ability to address any international rules for privacy protection completely. RFID reader/writer is same too. So we have to consider different way to protect consumer’s privacy from technological resolution.

On the other hand, in such cases as that relationship between retail shop and supply chain is a kind of confidential matters and they are using same traceability system, if outsider user can access such a system then the outsider may obtain all or a part of such confidential information.

Moreover, in such cases as that one company has in fact a big power to rule the specific market, such company can use any traceability systems for the purpose of research any information relating to concurrent companies and misuse such obtained information in an anti-trust situation. In such cases, probably, researched companies can not recognize what is taking place in the

traceability system at all.

These problems are sharing same mechanism that can cause such problems. That is a sharing of any data through the traceability systems[3]. To prevent such issues, I would like to emphasis the importance of access control.

This has two meanings.

1) Control for accessing identifier item (e.g. RFID Tags) from traceability system or tracking data collection system
2) Control for accessing stored data (e.g. tracking data) inside traceability system from out side such system

5.0 Legal Analysis and Resolutions

To prevent such legal issues as I mentioned above, it is important to develop and enforce good policies. Indeed the privacy issue relating to RFID itself is a well known matter. However, most people discussing this focus only on the RFID devices themselves. Such an observation lacks a perspective on the counter side (receiver side)[4]. I would like to emphasize the existence of other issues which relate to the receiver side not the RFID devices side.

5.1 For Privacy Protection

If one wishes to address such privacy protection laws as relevant EU Directives[5] and OECD guidelines[6] then one shall adopt such adequate mechanisms into any RFID traceability systems as that shall be able to get a complete consent for personal data collection, to inform the purpose of collection, to disclose any data stored in such systems, and to remove or modify such data if the personal information owner needs by using each RFID reader/write device.

Especially, EU Directive 2002/58/EC provides as follows:

---

[3] I know of recent attempts at "neutralizing" RFID communication or at so-called "de-identification" of identification data involved in RFID Tags. However, de-identified or neutralized RFID can easily be re-identified or de-neutralized in the traceability system with a data matching system.

[4] For example, see *Radio Frequency Identification (RFID) Systems* at EPIC Web Site: http://www.epic.org/privacy/rfid/

[5] DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf
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

[6] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/20/0,2340,en_2649_201185_15589524_119820_1_1_1,00.html

Article 9 Location data other than traffic data

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 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.

However it is impossible to develop such an RFID reader/writer that has a function of getting consent, informing purpose or removing data and so on. Usually, an RFID reader/writer only has the ability to process radio waves, and doesn't have any function to notify the existence of such a reader/writer or get any consent from anyone who has or wears some RFID Tags. Thus, EU Directive 2002/58/EC cannot be enforced effectively in the area of RFID reader/writers.

Despite such a lack of notification and consent-getting functions, the transparency in the course of personal data collection using an RFID tracking system shall be realized. The only way to resolve this problem is to establish the initiative of everyone who possesses any items attached to any RFID Tags at any data collection time, even if such a person's personal information would not be collected by the RFID Tags at the time. Stealth deployment of an RFID device and hidden handling (operation) of a traceability system shall be deemed to be illegal under the EU privacy directive 2002/58/EC, the Japanese Personal Information Protection Law and similar laws in the United States.

For the purpose of keeping such transparency, when one buy any items attached to RFID Tags, one shall have the right to know the existence of such Tags and a right of Opt-out from any

data collection using such RFID Tags at the purchase time.

Thus the only way to protect privacy interest is:

1) to establish good policy for privacy protection;
2) to implement the deactivate function;
3) to inform the existence of RFID; and
4) to provide a selection of deleting or destroying physically erasing or deactivating by electronic measures or removing from items.

Such public policy has been introduced into the current Guidelines on EPC for consumer products (see footnote 1.). Also METI (the Ministry of Economy, Trade and Industry of Japan) is now drafting a similar guideline for privacy protection.

5.2 For Trade Secret Protection and Avoiding of Anti-Trust Issues

Every business corporation user shall be able to know the technological construction of any traceability systems and who the users of such systems are, as well as to control and stop any access account of other users to access any data in such systems each other.

Also it may be very important to develop a good policy for controlling any access accounts that can prevent any trade secret issues and anti-trust issues.[7]

[7] Recent Web news pointed out this issue. For instance, see *RFID spy-chippers leak confidential data on the Web* by Thomas C Greene in Washington (posted: 10/07/2003 at 07:23 GMT)
http://www.theregister.co.uk/content/archive/31654.html