Chapter 4
RFID V. Privacy Risks and Solutions

Yimeei Guo and Ying Luo

Abstract Radio frequency identification (RFID) is a generic term for technologies that use radio waves to automatically identify objects. An RFID chip comprises a microchip and a tiny antenna that transmits data from the chip to a reader. The reader is activated whenever the antenna comes into range, and the data can be used to trigger an event—such as raising an alarm or signaling that a pallet of goods has arrived in a warehouse. Usually, the range is no more than a few feet. But there are concerns that such applications will breach the privacy rights of individuals and threat the security of both organizations and individuals. There are also a range of technical, business, and political barriers to RFID's development. To avoid being off the pages limit, this paper wants to focus on the critical privacy risks to individuals by RFID. Then, it discusses feasible legal and technical solutions to RFID with some emphasis on the former, i.e., selective current legislative developments in different jurisdictions, to provide companies with insight on what compliance with legislations may entail and to assist companies in possible self-regulation to address these concerns as well. Finally, this article presents its conclusion and suggestion aiming at a healthy and sound atmosphere to RFID's development.

Keywords RFID · Privacy risks · Solutions · Self-regulation

Published by "Proceedings of the 4th Int'l Conference on Innovation & Management" Vol. II, 2007.12.5-6, pp.1849-1853<ISTP indexed>

Y. Guo (✉) · Y. Luo
Management Science Department, Xiamen University, Xiamen 361005,
People's Republic of China
e-mail: yimei_guo@necmail.xmu.edu.cn

Y. Luo
e-mail: yuhe_ly@sina.com

Y. Guo (ed.), *Research on Selected China's Legal Issues of E-Business*,
DOI 10.1007/978-3-662-44542-6_4

4.1 Introduction

Radio frequency identification (RFID) is a generic term for technologies that use radio waves to automatically identify objects. An RFID chip comprises a microchip and a tiny antenna that transmits data from the chip to a reader. The reader is activated whenever the antenna comes into range, and the data can be used to trigger an event—such as raising an alarm or signaling that a pallet of goods has arrived in a warehouse. Usually, the range is no more than a few feet.

The chips can be incorporated into a range of products and have an advantage over barcodes in not requiring a line of sight between the chip and the reader. They offer a means of navigating complex global supply chains, allowing companies to track their products from factory to distribution centre, from warehouse to sales floor.

The decision taken by leading global retailers to mandate use of RFID by their suppliers, aided by the emergence of global technical standards, has eliminated any doubt that the technology will be used on a broad scale, says a report by the economist intelligence unit (EIU) released in early 2006. Pilot programmers in retail, consumer goods, logistics, life sciences, automotive, and government are under way and are already producing tangible benefits such as reduced costs, better inventory control, and improved responsiveness to consumer demand.

The supply chain is becoming smarter as a result of the technology, with companies such as Wal-Mart, Tesco, and Gillette using it to track inventory and improve stock replenishment. But to fulfill its potential, the technology needs to be integrated into operational management tools such as enterprise resource planning (ERP) software. It highlights RFID's role as a catalyst for much greater collaboration between companies along the supply chain.

For example, it says a retailer referring to a specific product with one numbering system and a department store that refers to that same product—but with a different numbering system—has no idea that each is selling the same item. By utilizing RFID technology, the two companies could change that situation by sharing consistent data that would allow collaboration through purchasing, development, and promotion of the product.

Outside of the supply chain, a range of other applications are emerging, especially in applications that enhance customer convenience, such as "contactless payment" systems. Another growth area will be in identifying and authenticating people or items for safety or security purposes, such as within passports or to verify a patient's identity at the operating table.

But there are concerns that such applications will breach the privacy rights of individuals and threat the security of both organizations and individuals. There are also a range of technical, business, and political barriers to RFID's development.

To avoid being off the pages limit, this article wants to focus on the critical privacy risks to individuals by RFID. Then, it discusses feasible legal and technical solutions to RFID with some emphasis on the former, i.e., selective current legislative developments in different jurisdictions, to provide companies with insight on what compliance with legislations may entail and to assist companies in possible self-regulation to address these concerns as well. Finally, this article presents its conclusion and suggestion aiming at a healthy and sound atmosphere to RFID's development.

4.2 Privacy Concerns to RFID

While RFID technology has the potential to provide numerous benefits and opportunities for businesses, it also raises concerns for consumers regarding the privacy of their personal information. Although privacy concerns may be premature given current RFID technology and limited adoption of this technology, there has already been considerable debate regarding privacy and security of personal information and the measures necessary to safeguard personal information.

For instance, Paula Bruening, Staff Counsel at advocacy group the Center for Democracy and Technology, warned at a U.S. Department of Commerce workshop on RFID on April 6, 2005, that RFID is one example of a growing trend toward businesses collecting and using their customers' personal data.

Bruening also pointed out: while most current forms of RFID are not capable of compromising privacy by doing things such as tracking customers' movements, the technology is rapidly moving forward and may soon catch up to consumer and privacy advocates' fears.

In essence, privacy advocates have said that RFID uses small processors and antennas that are integrated into a paper or plastic label. Those chips can then be read by an electronic scanner, and unlike barcodes, RFID chips withstand dirt and scratches. As the range of RFID scanning grows beyond the current 25 ft (7.6 m), RFID could allow corporations and governments to track people's movements and purchases.

But representatives of RFID technology vendors including Texas Instruments and Microsoft, along with users PepsiCo and General Motors, talked of the potential for RFID to revolutionize the way companies manage their inventories, fight counterfeiters, and stop shoplifters.

Generally, privacy concerns regarding adoption of RFID technology include (among others) the following:

- The unauthorized reading of RFID tags.
- The security of personal information contained on RFID tags to prevent the unauthorized use or dissemination of such information.
- The ability of third parties to profile individuals by their possessions containing RFID tags.
- The use of RFID technology to provide covert tracking or surveillance of individuals.

It is possible that many of the public's privacy concerns could be addressed through industry self-regulation, which would require adherence to privacy policies encompassing fair information practices and possible implementation of privacy-enhancing technologies. Given the increasing rate of adoption of RFID, public perception of a privacy threat to personal information, and lack of current standard industry practices to address these concerns, there is mounting support for the need for legislation to address these privacy risks.

4.3 Solutions to RFID Privacy Risks

4.3.1 Legal Solutions

4.3.1.1 The European Union

The European Union (EU) is exploring ways to protect citizens' privacy with regard to personal data gathered using RFID technology. The union created a working group that in mid-January 2005 published its first assessment—"Working document on data protection issues related to RFID technology" (also Known as "Working Document 105"). The group is asking individuals to e-mail comments on its findings by March 31, 2005, to markt-privacy-consultations@cec.eu.int.

The document outlines RFID's potential in a variety of business sectors, including health care, retail, pharmaceutical, and logistics, and calls attention to the need for companies to comply with principals in EU privacy directives whenever personal data are collected using RFID technology. The document also guides makers of RFID tags, readers, and applications, as well as standards bodies, on their responsibility to develop privacy-compliant technology.

Europe already has sweeping privacy laws in place to protect consumers across the continent. For example, retail stores must disclose the presence of RFID tags on products and the presence of readers, how the retailer intends to gather and control the information, the purposes for which the information will be used, who will control the data, how to discard the tag from the product, how to exercise the right to access the information on the tag, and more.

The new working group says it has found other issues with regard to RFID that need to be addressed. RFID technology increases the potential for direct marketing with item-level tagging, since shoppers could be recognized and their movements tracked while in stores, according to the group.

Another concern for the EU working group is the use of applications that link an RFID-enabled plastic card with a consumer's bank account number to enable payment processing, similar to a credit card, without having to swipe the magnetic strip.

Manufacturers of RFID equipment and applications should be held equally responsible for building tags, readers, and printers that protect consumers' right to privacy, the document states. The group stresses there is continuing need for further research and development on issues related to encryption that protect personal information on the tags. It wants to make sure the RFID tag does not divulge information that would link the consumer with the product which the consumer is buying. If the tag is permanently affixed to the garment, for example, the working group says there should be a way the consumer can delete the information written on the RFID tag or cut it out once the garment is paid for.

For passports and other government-issued identification that must not be altered, the working group suggests using standard authentication protocols from the International Standards Organization (ISO) to encrypt the data and make it unavailable to those without authorization.

In short, according to the European Commission (EC) which has announced the beginning of a public inquiry to identify citizens' concerns about the technology as above mentioned, new legislation may be required to regulate the widespread use of RFID tags.

4.3.1.2 The United States

On a national level, there is little law currently directed at RFID privacy issues. Of some significance, however, is a not-for-profit lobbyist named consumers against supermarket privacy invasion and numbering (CASPIAN), which has been dedicated to protecting consumer privacy in the marketplace. This organization drafted the "RFID Right to Know Act of 2003," which seeks amendments to the "Fair Packaging and Labeling Program," the "Federal Food, Drug, and Cosmetic Act Relating to Misbranding," and the "Federal Alcohol Administration Act" (Title 15, Chaps. 36 and 94).

Though no legislation has been enacted based on CASPIAN proposed Act, it does address privacy concerns with a set of primary requirements:

- "Notice": Labels that are conspicuous in size, location, and contrasting print are required on products containing RFID tags with a warning that the tag can transmit unique identification information to a reader both before and after purchase.
- "Limitation of Use": Businesses are prohibited from: (1) combining or linking an individual's non-public personal information with RFID tag identification information beyond what is required to manage inventory; (2) disclosing such information to a non-affiliated third party; or (3) using RFID tag identification information to identify an individual.
- "Education": Requiring the Federal Trade Commission (FTC) to establish appropriate standards for businesses to follow to protect an individual's personal information and publish documents to educate the public about RFID technology.

In other national RFID privacy dialogue, U.S. Senator Leahy of Vermont presented a speech entitled "The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security" in March, 2004. Leahy encouraged public discussion of the issues and spoke of the possibility of congressional hearings on RFID technology.

While RFID legislation on the federal level is still taking shape, at least 12 states introduced legislation to address privacy concerns raised by the implementation of RFID technology (including CA, MD, MA, MO, NV, NH, NM, RI, SD, TN, TX, and UT) in 2005. The proposed measures in these bills vary significantly, from simply calling for the establishment of a task force to address the implications of the proliferation of RFID technology, to requiring RFID "kill" technology to deactivate RFID tags upon completion of sale, to seeking to establish criminal liability for misuse of personal information obtained through RFID. However, many of the proposed bills have common minimum requirements. Often among the requirements are including conspicuous notice requirements similar to those in the CASPIAN proposed Act.

4.3.1.3 China, the Hong Kong SAR, and Taiwan

With Integration of the world's culture, economy, and infrastructure driven by the lowering of political barriers to transnational trade and investment and by the rapid proliferation of communication and information technologies, developing countries are fast learning both best practices and mistakes of retailing giants in developed countries. For countries such as India, Brazil and China, usage of RFID in retail stores is minimal; nonetheless, these countries are gearing up to meet Wal-Mart and other retailer's mandates.

Here, we would like to examine current laws and regulations related to privacy in China, the Hong Kong SAR, and Taiwan (if any) as follows:

- China

The Chinese Constitution—like that of the former USSR—provides limited rights to privacy, notably the declaration that "the freedom of the person of citizens of the People's Republic of China is inviolable" (Article 37) and that "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law." (Article 40)

China has decided to introduce legislation to tackle the misuse of personal data in daily life. The Institute of Law of the Chinese Academy of Social Sciences has drafted the "Personal Data Protection Act of the People's Republic of China" and submitted the draft act to the Information Office of the State Council in January 2005.

The bill aims to balance the free movement of information, which is recognized as important in modern society, with protection of basic human rights. The scope of the protection will extend to personal mobile phone numbers, family addresses, medical history, and career status. The Bill also regulates some "hot topics." For example, it will provide rules for installation and use of cameras in public areas, as well as photography and video recording without consent.

Once enacted, violation of the Bill will trigger not only civil liability but also administrative and criminal liability.

Nevertheless, compared with the US legislation procedure to RFID having started already, it seems that China still has a long way to go.

- The Hong Kong SAR

Hong Kong was the first part of the region to enact legislation based on the EU Directive, with a Personal Data (Privacy) Ordinance covering the public and public sectors and a Code on Access to Information. The statutory Privacy Commissioner (PCO) is currently engaged in work of particular importance regarding privacy aspects of identity cards and health databases.

Notably, the Hong Kong International Airport has announced that it has adopted RFID technology in its baggage handling and cargo services in August 2005. It is believed to be one of the first such projects to go live worldwide in the industry.

If the tags were to contain information personal to the traveler (such as the name, flight number, address, or even passport number) that a signal reader could detect, the set of data stored on the tag would constitute "personal data," and the Personal Data (Privacy) Ordinance would come into play.

Under Data Protection Principle 4, the airport authorities and airlines would be required to take "all practicable steps" to protect such data against unauthorized access. This would certainly entail consideration of encrypting the data so as to make it unusable by third parties.

- Taiwan

Across the straits, the 1994 Taiwanese Constitution articulates a restricted right of privacy, i.e., that "The people shall have freedom of privacy of correspondence." That has been extended through legislation such as the 1995 "Computer-Processed Personal Data Protection Law" (*CPPDPL*) concerning the collection and use by government agencies and some private sector bodies of personally identifiable information.

The 1995 law requires that "collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose," with a principle right of data access, correction, and deletion. Data flows to countries without privacy legislation can be prohibited.

As to the content recording and the data collecting by RFID tag, it is argued by some expert from Technology Law Center, Information Industry Institute (III) in Taiwan that they both should be limited by CPPDPL.

4.3.2 Technical Solutions

Opponents of RFID tags have proposed measures to sidestep the chips' relentless information gathering, ranging from disabling the tags by crushing or puncturing them to simply boycotting the products of companies which use or plan to implement RFID technology. One way to destroy the tags is to microwave them for several seconds.

Another method is to obstruct the information gathered by RFID readers using blocker tags. When carried by a consumer, blocker tags impair readers by simulating many ordinary RFID tags simultaneously. Blocker tags can also block selectively by simulating only designated ID codes, such as those issued by a particular manufacturer.

As claimed by some experts, blocker tags may be available from many sources, merchants may include them for free with purchased goods, or consumers may be able to buy them at the checkout counter. Consumer rights organizations may supply them for nominal cost. As noted earlier, there is no reason why blocker tags should not be cheaply and widely available.

4.4 Conclusion and Suggestion

There is certainly a great deal of public debate regarding RFID and privacy concerns. While industry self-regulation may be able to address many of these concerns, legislation will continue to be proposed as the appropriate solution until standard privacy procedures and technologies are adopted.

While this article provides an overview of RFID legislation in the EU, USA, China, the Hong Kong SAR, and Taiwan, there are other international implications, including momentum for legislation in other geographic regions.

When formulating privacy policies and procedures relating to RFID implementation, companies should be aware of the current issues being discussed by regulatory bodies and the proposed legislations relating to RFID. Companies could then better assess what measures should be adopted to address compliance with possible RFID-related laws.

Although RFID technology has many current and future benefits, yet policymakers need to be aware of potential privacy and security problems of the rapidly evolving technology. RFID has the potential to expand what people around you know about you, and its uses are worth a policy debate.

Nevertheless, policymakers should not focus new rules on all uses of RFID when many existing uses cause no privacy or security problems. Just as James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, a Washington think tank, puts it: “If you’re putting a chip in the ear of a cow, is there really a privacy concern?” “A one-size approach won’t work.” And although rules on the proper use of RFID are needed, they could be industry rules instead of ones set by the government.

Finally, this article suggests that standard bodies and academic institutions need to harmonize hardware and software standards globally, while companies should lay out a framework that helps them understand and address the process changes required to get value from the technology.

References

Ari Juels, Ronald L. Rivest, and Michael Szydlo. 2007. *The blocker tag: Selective blocking of RFID tags for consumer privacy.*http://66.102.7.104/search?q=cache:7prnEPBlP0EJ:theory.lcs.mit.edu/~rivest/JuelsRivestSzydlo-TheBlockerTag.pdf+RFID&hl=zh-CN%20target=_blank.

Growth of RFID must respect privacy, says EIU, OUT-LAW News. 9 Mar 2006. http://www.out-law.com/page-6715.

Grant Gross. 2005. *RFID policy panel raises privacy concerns*. 6 Apr 2005. http://www.infoworld.com/article/05/04/06/HNrfidprivacy_1.html.

Kenneth A. Adler, Esq. 2005. *RFID and privacy issues: A snapshot of proposed laws.*http://www.rfidproductnews.com/issues/2005.09/feature/08.php.

Laurie Sullivan. *The European Union works out RFID privacy legislation.*http://informationweek.com/story/showArticle.jhtml?articleID=59301363.

Peter Sayer. 2006. *EC to investigate RFID privacy concerns*. 9 Mar 2006. http://www.techworld.com/applications/news/index.cfm?NewsID=5536.

Shaping ubiquity for the developing world. Paper presentation and panel discussion at International Telecommunications Union (ITU) Workshop on Ubiquitous Network Societies, 6–8 Apr 2005. http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Paper_Ubiquity_and_developing_world.pdf.

Vanessa Huang. 2005. *China contemplates privacy legislation.* 7 Mar 2005. http://www.twobirds.com/English/publications/articles/China_contemplates_privacy_legislation.cfm.

Zhenhao Gu. 2006. *The potential legal problems of RFID. TEEM monthly*. http://www.teema.org.tw/publish/moreinfo.asp?autono=2845.