https://doi.org/10.48009/2_iis_2007_241-347

RADIO FREQUENCY IDENTIFICATION TECHNOLOGY AND CONSUMER PRIVACY

Marzie Astani, Winona State University, mastani@winona.edu
JoEll Bjorke, Winona State University, jbjorke@winona.edu

ABSTRACT

Radio frequency identification (RFID) technology has helped many organizations to reduce cost. Nevertheless, there are challenges and issues associated with RFID adoption. The most common internal challenge for many organizations is justifying the investment and modification of processes. However, there are external issues such as privacy and security that companies need to deal with. The focus of this study is to show the business value of RFID technology and the related issues, especially consumer privacy issue that organizations need to be concerned about.

Keywords: Radio Frequency Identification (RFID), Application Issues, Consumer Privacy

INTRODUCTION

Organizations invest in technological innovations to gain competitive advantage in the marketplace. Enterprises making major investments in technology need to realize that although technology is an enabler, the adoption of new technology could pose a complex challenge, especially with the rapid pace of technological change.

The most recent technology in which organizations are investing to gain competitive advantage is radio frequency identification, RFID. This technology has the potential of impacting an organization's business profoundly. Many organizations have adopted this technology and others are in the process of doing so. Although the initial drive for RFID adoption was supply chain management, today many organizations are involved in implementing RFID to solve business problems [2]. The growth for RFID technology has been estimated to be over 112 percent for 2007. The budget for manufacturing initiatives that have already been underway in 2006 will increase 61 percent in 2007. This will add 51 percent of new demands in the RFID market in that sector [20].

RFID technology has penetrated into different business sectors very quickly. Many companies have implemented RFID technology and have already seen the business value of it. For example, retailers Wal-Mart and Target, which had started RFID adoption in 2003, later mandated the use of RFID tags by all their suppliers at the palette level by 2005. In 2007, Wal-Mart is moving the usage of RFID tags to the item level. The U.S. Government's Department of Defense (DOD) is following the same path. Several other pilot projects are underway to implement RFID at the item level [2]. In addition, there have been many other applications of this technology in the airline industry, food and drug industry, hospitals, and many government agencies.

Organizations invest in RFID expecting to reduce cost and achieve a return on investment (ROI). A recent survey of 150 manufacturers using or planning to adopt RFID technology indicates that they expect the technology to help them in three general areas: 1) optimizing the procurement and management of raw materials, 2) monitoring equipment, parts and personnel in the production environment, and 3) providing forward demand visibility into the supply chain [27]. Investing in RFID technology, like any other major investment, requires careful research of the technology and a critical analysis of its implementation. Organizations need to review and address implementation issues such as internal processes' modification, cost, compliance, scalability, security, and consumer privacy issues [27, 20, 31]. Consumer privacy is the most publicized issue among all RFID adoption issues. In 2006, several companies such as IBM, RFIDSec, and SmartCode along with lawmakers tried to address this issue [28 and 22]. The effort in search of finding a solution is continuing in 2007.

This study attempts to show issues and challenges that management face in the deployment of RFID, especially the privacy

issue. In particular, the emphasis will be on the privacy issue and laws (or lack of them) to protect citizens. This paper presents a brief description of RFID technology and applications followed by the discussion of the consumer privacy issue related to RFID applications. Finally, the future direction of RFID technology and the conclusions will be discussed.

RFID TECHNOLOGY

Although RFID applications in business environments have been on the rise for the past three decades, the history of this technology can be traced back to military identification friend or foe (IFF) systems during the Second World War [14]. Later, the technology evolved into the popular bar code, which was printed on almost every conceivable piece of packaging moved and sold worldwide. RFID is the latest technology that can precisely identify objects [36]. Both bar codes and RFID technology are used as a support tool that automates processes and improves operations management by reducing labor and eliminating human error. In addition, this technology supports decision making by providing essential information about the status of goods being supplied. However, RFID tags are a more sophisticated technology than bar codes. The tags are readable without a line-of-sight requirement and from much further distance, as well as being easily embedded in objects. For example, tags can be read through a variety of packaging materials, including wood, plastic and cardboard. Tags can also be reprogrammed easily and are capable of working in harsh environments such as outdoors and around chemicals. Currently, RFID tags are capable of carrying 96 bits of information, compared with 19 bits for bar code technology [2, 5].

RFID technology involves the transmission of a radio signal between a tag and a reader. The tag contains a chip with embedded information such as an identification number, bar code number, and serial number. The reader sends a continuous signal at a given frequency to 'read' the data stored on the tag [27]. There are two types of RFID tags: active and passive. Active tags are battery-operated while passive tags are not. Active tags focus on providing only an identification number and possibly some information, such as a description or transportation history, relating to the tagged object. Passive tags need to be "illuminated" by the radio waves emitted by a specialized reader to provide only an identification number. Passive RFID tags are particularly appealing because they operate without battery, which makes them very small and inexpensive, while they can be subjected to new and interesting design possibilities. For example, they can have the shape of a coin, stick, label, or capsule for the purpose of attaching them to an object [2, 30].

RFID systems work in different frequencies depending on the application. For example, the 125 KHz frequency tends to be used in chips for cars as well as asset management. These tags are used in industrial environments so they are usually thicker and less flexible since they contain coils. The 13.56 MHz frequency systems can be used for item-level management (for example books in libraries and inventories) or in supply chain environments for goods on a conveyor belt. The 13.56 MHz has a typical read/write distance of 1.5 meters [14, 5]. The International Telecommunications Union (ITU) authorizes RFID systems to work within the Industrial-Scientific-Medical bands [27].

RFID technology has many capabilities, which makes it very beneficial for logistics, stock handling, and traceability and fraud controls applications. RFID applications and some issues that they have created will be discussed next.

RFID APPLICATIONS AND ISSUES

There is an increasing demand for RFID applications, especially in the supply chain management market. RFID applications can be either in an open-loop or closed-loop. Open-loop applications tend to be in a controlled environment because of the managing issue of the constant inflow and outflow of materials. A closed-loop environment is much smaller and self-contained and easy for implementing RFID technology [27].

Supply chain management applications of RFID fall into the open-loop category. For example, RFID adoption by retailers Wal-Mart and Target, which started in 2003, is an open-loop application, where the industry collaboration is enhanced. Within this application, labels on the objects allow them to become part of the global networks to provide a wide range of new and emerging services. Items can be identified at various points in the distribution system to ensure that they are sent to the correct location.

This information, which is delivered in real time, can be shared with all interested parties, the sender, the forwarder, and the customer awaiting the shipment, all with minimum human intervention. The decision makers can use this information to meet the demands of a global economy by responding rapidly to changing patterns of demand while also improving customer service levels [5].

In 2005, Wal-Mart made it mandatory for suppliers to start tagging their merchandise pallets and cartons. A few other enterprises such as Metro AG, Tesco, Target, and Best Buy made similar requirements for their suppliers. Among Wal-Mart suppliers, Gillette was one of the early participants since its products are reportedly among the most stolen from retail shelves in the US [25]. Wal-Mart is planning to apply tags at the item level in 2007. Similarly, the US Department of Defense (DOD) initiated RFID adoption in 2003. By 2006, DOD issued a series of RFID policy guidelines requiring passive tags to be applied to all freight/cargo containers, cases, pallets, and individual 'high value' items that require the military's UID (Unique Identification Code) [29].

While applications in supply chain tend to be long term and perhaps with no immediate return on investment, there are more focused and localized applications (closed-loop) that can provide incremental justification for the RFID investment. These include warehousing, asset location/tracking, people location, mobile payments, in-process inventory tracking, repair and maintenance, and luggage tracking. The U.S. Food and Drug Administration (FDA) has adopted RFID technology to prevent counterfeiting prescription drugs. Public libraries are using RFID to track books [13]. An interesting application of RFID is by the DeKalb County Juvenile Court to track the location of files through the entire workflow. As a file moves from the central file room to the team room and individual offices, the location can be viewed on any network computer. This allows the court to prevent misplaced or lost files [23].

There are many challenges and issues for RFID adoption including insufficient RFID standards, security concern (especially in wireless RFID), cost, and privacy. Insufficient RFID standards are being addressed by the standard establishing organizations including International Standards Organization (ISO) and EPCglobal [14, 30]. The security concern is alleviated by controlling the physical environment so that malicious users can't access the tags. This is relatively easy in closed-loop situations, but very complex in open-loop situations such as a supply chain, where the tags are typically moved along with the products. As with the Internet, security is a moving target and needs to be handled on a case-by-case basis [13, 31, 33]. The issues of cost in adopting RFID technology relates to the cost of RFID system components and setup, a concern that all organizations share. But with the widespread use of RFID technology, it is expected that the cost would be reduced significantly [5]. However, for a firm's management, the cost of process modification/change and associated data integration in RFID implementation is a major concern. In a 2006 survey, 62 percent of 150 manufacturers participating stated that data integration is one of the top concerns in an RFID initiative [20].

Among all RFID related issues, the violation of consumer privacy has received the most publicity and is the most challenging for organizations. This issue has contributed to the failure of several RFID projects. Major companies worldwide such as Metro Group in Europe and Gillette have scrapped RFID programs following consumer backlash. In Gillette's trial program, RFID-enabled razor packages sold by the United Kingdom retail giant Tesco was canceled when privacy advocates protested, stating that retailers and manufacturers could monitor razors that had gone home with a customer and use the technology for surveillance [10, 26]. Lawmakers in several U.S. states, including California and Massachusetts, are considering whether to implement RFID-specific privacy policies [4].

Although some organizations try to minimize the consumer privacy concern, the issue is real and worldwide. Privacy advocates such as Katherine Albrecht, the founder of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), have raised concerns about the risk of personal information abuse and consumer aversion to retailers collecting their personal data. Mainstream newspapers such as the Washington Post and the New York Times have published articles on the legitimate questions raised by privacy advocates.

PRIVACY ISSUES

The growing number of RFID applications has fueled concern about potential violations of privacy [24]. The concern arises out of the fact that the stored data on the RFID tags may be linked to individual's personal information. Further, the presence of the tags may not be known to consumers, enabling monitoring without consent by the item's seller and potentially others. In addition to the unauthorized collection of information, consumers may be subjected to an undesired use or sale of their personal information. A theft of that information is another major concern.

One response to these concerns is to allay any cause for alarm [16]. The high costs associated with RFID technology will limit, as a practical matter, any extensive deployment of RFID tags and readers [3]. However, as previously indicated, there appears in fact to be a rapid increase in the uses of RFID. It is further argued that users of RFID won't adapt the technology in a way that will offend their customers and cause injury to the long-term interests of the business [16]. Yet Wal-Mart's experiment with tagged lipsticks at its Broken Arrow store in 2003 is cited as evidence early in the roll out of RFID technology of just such abuse [18]. Finally, the counter argument should the implementation of RFID adversely affect consumer interests is that existing legal protections are sufficient to redress any harm [3]. The following section reviews the evaluation of current law as it pertains to RFID abuse.

Existing Legal Protections

There are multiple sources of protection against privacy violations under current law: federal and state constitutions, statutes, administrative regulations, and case law or common law. The application of those laws to RFID is, to date, not established [17].

Constitutions - First, there are provisions in the U.S. Constitution and several state constitutions that protect privacy rights [8]. Most notably, the Fourth Amendment in the federal constitution prohibits unreasonable searches and seizures [35]. Is the collection of data from a RFID reader unreasonable? The cases interpreting this provision have found violations when information is obtained under circumstances where there is an expectation of privacy, such as in one's home [21]. In the context of RFID, therefore, there would appear to be no protection if the information is collected from a reader in a public place. Moreover, constitutional restrictions apply only to governmental actions and will not cover collection of information by RFID technology by private enterprises [8].

Statutes - The second source of potential protection is based primarily on existing state and federal prohibitions against fraud. The Federal Trade Commission Act prohibits unfair and deceptive trade practices [1]. This arguably encompasses misrepresentations or omissions about the collection or use of data from RFID tags [18]. The FTC reportedly does not, however, monitor the use of RFID technology and has not brought any related enforcement actions [34]. Future actions are anticipated to be limited due to the fact that the FTC could only proceed against companies that voluntarily provide privacy policies [18]. Even then action may depend on the availability of limited resources and would be unsuitably slow [18].

Other federal statutes cited as potentially applicable are the 1974 Privacy Act, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act (HIPPA) [11]. The first of these, the Privacy Act, is limited to governmental action and only to the use, not collection, of data [11]. The others have likewise been evaluated as largely ineffectual with regard to RFID privacy issues [11]. Although HIPPA includes the most specific protections as to the collection and use of data, it applies only to health care information [11].

Administrative Regulations - At the federal level, many administrative agencies have considered the impact of RFID in their respective regulatory fields. The privacy implications are most directly related to the consumer protection role of the FTC. The agency held a workshop in June 2004 to examine the issues but subsequently determined that it should defer to industry self regulation [18].

Common Law - Finally, common law theories have been evaluated as an avenue of recourse in the event of RFID abuse. Theories advanced include those protecting contract, tort, and property rights [3, 11, 15, 18]. The most commonly discussed possibility, an invasion of privacy based on intrusion upon another's seclusion, suffers the same disadvantage of

constitution and statutory provisions discussed earlier. It would not apply to private information available in a public place [18]. In addition to problems in meeting the requirements of the individual theories, common law actions do not provide widespread deterrence [11, 18]. The recourse is after the fact, is directed at identified defendants only, and varies from state to state.

In summary, although there are many existing laws to protect an assortment of privacy interests, none directly address RFID technology in a way that will deter undetected data collection and use. As a result, proposals for new and more targeted methods of protection have been proposed.

Proposed Protections

The proposed protections can be classified into two categories: self and government regulation.

Self Regulation - New technologies are being developed to address consumer privacy protection. For example, a technology developed recently, Gen2 protocol, allows for "kill" functionality, which permanently disables a tag at the point of sale. However, for the retailers and manufacturers, it is very appealing to have the relevant information stored in RFID tag accessible in the event a consumer returns a tagged item. Therefore, the challenge confronting retailers and consumer package goods manufacturers is to find a balance between consumer privacy protection and the benefits of post-purchase RFID tagging [24]. In recent months, several companies have offered some solutions. In November 2006, IBM licensed "clipped tag" technology, which allows a consumer to tear off a piece of the tag after the item has been purchased. This limits the read range significantly, which means the tag can be read at very close range, therefore preserving the post-purchase benefits [25]. Yet another technology solution is from a Danish company, RFIDSec, which has developed a technology that puts a tag in "silence mode" (the data would be unavailable for reading) when an item is purchased. However, an authorized party can reawaken the tag at the time the item is returned. In addition, the company offers another technology that allows encryption of data being communicated between the RFID tag and the reader [24].

Government Regulation - At the federal level, amendments to the Privacy Act and the Electronic Communications Privacy Act discussed above have been proposed [9]. More specifically, Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) drafted an act entitled the RFID Right to Know Act of 2003 which included amendments to an assortment of federal statutes, particularly those directed at packaging/labeling and privacy [7]. Its provisions require conspicuous labels notifying consumers that a package contains a RFID tag and that the tag could transmit identification information to a reader. Moreover, it would have prohibited linking an individual's nonpublic personal information with RFID tag information, disclosing an individual's nonpublic personal information in association with RFID tag information, and using RFID tag identification information to identify an individual. It would have required the FTC to adopt regulations to implement its provisions. The FTC, as discussed above, declined to do so. A proposal entitled "Opt Out of ID Chips Act" also was not successful [18].

State legislative proposals, on the other hand, have been more prolific. RFID related proposals with regard to a range of data privacy issues have been reported as under consideration in nineteen states, including the following: California, Maryland, Massachusetts, Missouri, New Hampshire, New Mexico, Nevada, South Dakota, Tennessee, Utah, and Virginia [3, 18, 32]. The proposals vary with labeling most commonly required [18]. None have been adopted.

Future proposals may look to the guidelines issued by the Center for Democracy and Technology on privacy best practices for deployment of RFID Technology [6]. Although "not designed as a blueprint for legislation," the guidelines call for clear and conspicuous notice to consumers when information is collected and linked to personal information as well as when a choice exists as to the use of RFID technology. Reasonable access to personal information collected is in addition to reasonable security of tagged information.

FUTURE DIRECTION AND CONCLUSIONS

Many factors have contributed to the increased demand for RFID applications, especially in the supply chain management market. Industry collaboration, technical developments and the numerous advantages that the technology can bring are among these factors. However, there are several issues associated with RFID applications of which consumer privacy protection is perhaps the most publicized.

RFID applications are increasing. Current law does not adequately address potential invasions of privacy. Changes in law to restrict abuses are anticipated to develop from state legislation and common law rather than federal legislation or constitutional cases [17]. Simultaneously, self imposed technological solutions and privacy practices are evolving.

REFERENCES

1. 15 U.S.C. 45 (2000).
2. Borriello, G. (2005). RFID: Tagging the World. *Communications of the ACM*, 48(9), 34-37.
3. Brito, J. (2004). Relax. Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature (Electronic Version). *UCLA Journal of Law and Technology*, 5.
4. California RFID Restrictions Get Governor's Veto. (2006). Available: http://www.rfidupdate.com/articles/index.php?id=1218. Accessed January 20, 2007.
5. Another Link in the Chain. (2004). *Card Technology Today*, April 11.
6. *Center for Democracy & Technology*, (2006). CDT Working Group on RFID: Privacy Best Practices for Development of RFID Technology. Available: http://www.cdt.org/privacy/20060501rfid-best-practices.php. Accessed February 21, 2007.
7. *Consumers Against Supermarket Privacy Invasion and Numbering*. (2003). RFID Right to Know Act of 2003. Available: http://www.nocards.org/rfid/rfidbills.html. Accessed January 25, 2007.
8. Dalal, R (2006). NOTE: Chipping Away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights. *Boston University Law Review*, 86, 485.
9. Delaney, K. (2005). RFID: Privacy Year in Review: America's Privacy Laws Fall Short with RFID Regulation. *I/S: A Journal of Law and Policy for the Information Society*, 1, 543.
10. Eckfeldt, Bruce. (2005). What Does RFID Do For The Consumer? *Communications of The ACM*, 48(9), 77-79.
11. Eden, J. (2005). When Big Brother Prioritizes: Commercial Surveillance, The Privacy Act of 1974, and the Future of RFID. *Duke L. & Tech. Rev*., 20.
12. Evans, Bob. (2005). Business Technology: RFID Is Already Providing Its Value. *Information Week*, Available: http://www.informationweek.com. Accessed February 11, 2007.
13. Gadh, Rajit. (2005). RFID Moves Beyond Supply Chain Mandates. Computer World. Available: http://www.computerworld.com. Accessed February 11, 2007.
14. Glidden, Rob et al. (2004). Design of Ultra-low-Cost UHF RFID Tags for Supply Chain Applications. *IEEE*, August, 140-151.
15. Handler, D. (Spring 2005). The Wild, Wild West: A Privacy Showdown on the Radio Frequency Identification (RFID) Systems Technology Frontier [Electronic Version], *Western State University Review*, 32, 199.
16. Harper, J. (2004). RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98 Lb Weakling. *Competitive Enterprise Institute*, 89, 1-12.
17. Herbert, W. (2006). No Direction Home: Will The Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery? [Electronic Version], *I/S: A Journal of Law and Policy for the Information Society*, Spring/Summer, 2, 409.
18. Hildner, L. (2006). Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology – Specific Legislation at the State Level [Electronic Version]. *Harvard Civil Rights – Civil Liberties Law Review*, Winter, 41, 133.
19. Hostetter, D. (2005). When Small Technology is a Big Deal: Legal Issues Arising from Business of RFID [Electronic Version]. *Shidler Journal of Law, Commerce & Technology*, Autumn, 2, 10.
20. Klien, Russ. (2007). Aberdeen on RFID Adoption in Manufacturing. Available: http://www.rfidupdate.com/articles/index.php?id=1219. Retrieved February 11, 2007.
21. Kobelev, O. (2005). Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and

the Need for Legislative Response [Electronic Version]. North Carolina Journal of Law & Technology, Spring, 6, 325.
22. Moskowitz, P. A. Andris, L. Moris, S. S. Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag. *RFID Journal Live*, May 1-3, 2006.
23. Philips, Dale. (2005). Strategic Applications of Technology: County-Level Case Study in the State of Georgia. *The Public Manager*, Summer, 32-36.
24. Privacy Rights Clearinghouse. (2003). RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. November 20. Accessed June 21, 2006. http://www.privacyrights.org/ar/rfidposition.htm.
25. Ramachandra, Girish. (2005). Learning from RFID: Strategies for New Technology Adoption. *SETLabs Briefing*, 3(3).
26. Rennie, Elizabeth. (2006). Staying On Course. *APICS magazine*, February, 28-33.
27. RFID: Not Just for Retail Anymore. (2007). *Information Management Journal*. Available: http://www.technewsworld.com/rsstory/55673.html. Retrieved February 11. Accessed February 11, 2007.
28. RFID Tag Balances Privacy and Retailer Interests. (2006). Available: http://www.rfidupdate.com/articles/index.php?id=1145. Accessed February 11, 2007.
29. Roberti, Mark. (2004). DOD Releases Final Policy. *RFID Journal*. Available: http://www.rfidjournal.com/article/articleprint/1080/-1/1. Accessed February 11,2007.
30. Sakamura, Ken. (2001). Radio Frequency Identification And Noncontact Smart Cards. *IEEE*, 4-6.
31. Stajano, Frank. (2005). RFID is X-Ray Vision. *Communications of the ACM*, 48(9), 31-33.
32. Songini, M. (2006). Wisconsin Law Bars Forced RFID Implants. *Computerworld*, June 12.
33. Sullivan, Laurie. (2005). Privacy And RFID: Are The Tags Spy Chips? *InformationWeek*. Available: http://www.informationweek.com. Accessed February 11, 2007.
34. Swedberg, C. (2004). FTC Readies an RFID Report. *RFID Journal*. Available http://www.rfidjournal.com/article/view/1151/1/1. Accessed February 12, 2007.
35. U.S. Const. Amend. IV.
36. Want, R. (2005). RFID: A key to automating everything. *Scientific American*, January, 56-65.