Final Term Paper

ON

RFID Privacy concerns and Compliance Issues

Elahe Javadi

May 2006

Abstract

Radio Frequency Identification, though not a new technology, has attracted attention in some parts of industry for a few years. The main advantages of RFID over optical barcodes are their uniquely identifiable authenticity and ability to be authenticated automatically. RFID tags and readers are still far from to be a commodity for companies; therefore RFID hardware manufacturer are struggling to find an efficient way to achieve the so-called 5-cent-tag goal set by market analysts. On the other hand, customer privacy advocates, have already established their campaign against what they call "spychip" or "the big brother barcode". CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) have proposed a model legislations for protecting individual privacy titled "RFID right to know act of 2003". The basic concern is that companies should notice consumers about RFID tag existence and provide them with the option to destroy it. In this paper, first I'll review the technology and the way it helps companies achieve their functional enhancement or reinvention goals. Then I discuss several of challenges exist in RFID deployment including privacy as one of the biggest obstacles; and then I explain the proposed solution by some organizations active in this area; Finally, I'll introduce some guidelines concentrating on the privacy concern of consumers.

Keywords

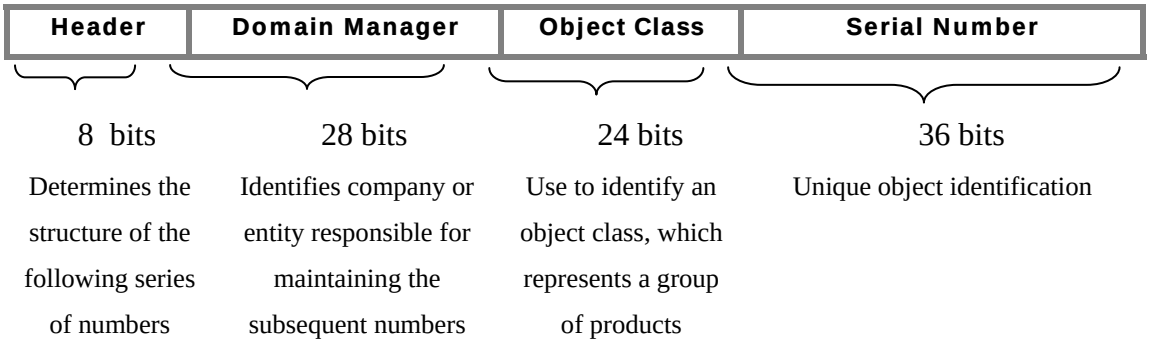
RFID, Privacy, EPC, Security, Threat

Introduction

Radio Frequency Identification is use of radio frequencies to collect information about physical objects to identify them. RFID lost competition to optical barcodes in 1960's; but seems to be the best choice now for companies to improve automation process. The technology has two hardware components: tags and readers. Tags are label-like chips attached to physical items and are able of storing identification data; readers or transmitters are the devices use to read that data and most likely provide the data to a middleware which in turn connects to Enterprise Information System. The

main advantages of RFID over its predecessor barcode are believed to be unique identification and automation [9]. Experts introduce numerous benefits to companies deploying RFID. Although RFID is not new, emerged and widely spreading data standards like Electronic Product Code introduced by EPC Global are new. An EPC stores important information about an item including manufacturer, supplier or retailer, product type and item serial number. This data is stored in a predefined format in which different bits of it should represent certain information. Figure 1 depicts a typical 96-bit EPC. As you see information about company responsible for product is stored before type and serial number and after header that in turn helps to identify the structure of the code.

Figure 1. Electronic Product Code



It's interesting that these EPC's can be part of different classes of RFID tags. Right now five different categories of EPC exist. There are two main classes of active and passive tags. Active and passive tags differ in the way they acquire their energy. Active tags do have a battery to provide them with their energy requirement while passive tags procure energy from radio frequencies transmitted by readers. There is also difference in tags regarding their programming features. Some can only be read. Some of them are write-once; manufacturer of the product is the most likely one to write on them for supply chain tracking benefits. Some tags are rewritable; to my knowledge, even early adopters like Wal-Mart, Procto-Gamble are still piloting second generation of class one tags which are write-once read-many passive tags. It seems to be a long way to deployment of class four and class five.

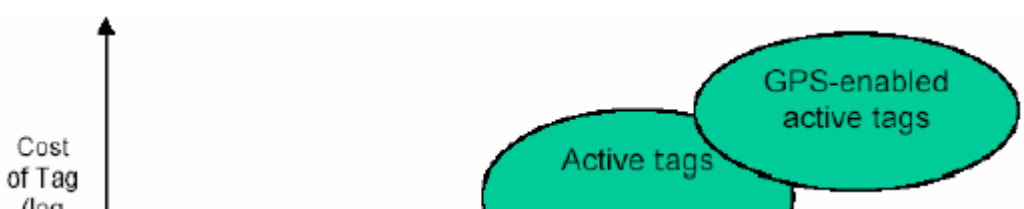
Table1. Summary of features of RFID Tag Classes

EPC Class	Definition	Programming
Class 0	"Read Only" passive tags	Programmed as part of the semiconductor manufacturing process
*Class 0+	"Write-Once, Read-Many" version of EPC Class 0	Programmed once by the customer then locked
Class 1	"Write-Once, Read-Many" passive tags	Programmed once by the customer then locked
Class 1 - Gen2	"Write-Once, Read-Many" passive tags. UHF Gen2 protocol ratified by EPC Global, Inc. on Dec. 16, 2004	Programmed once by the customer then locked
Class 2	Rewritable passive tags	Can be reprogrammed many times
Class 3	Semi-passive tags	
Class 4	Active tags	
Class 5	Readers	N/A
* Not an EPCglobal defined class		

Source: http://rfid.home.att.net/epc.htm viewed April. 2006

Derived from obvious application as tracking equipment in supply chain management, Garfinkel et al in [10] explain RFID tag applications in a few systems such as: automobile immobilizers in which, the car key incorporates a passive RFID tag that the steering column authenticates, thereby enabling vehicle operation. They also mention animal tracking; for this purpose, organizations and individuals are increasingly equipping pets, livestock, exotic animals, and endangered species with RFID tags to enable tracking, recovery, and management. In the US, many domestic cat and dog owners have RFID chips implanted in their pets. Payment systems, automatic toll collection and inventory management are all old examples of RFID application in industry and in day-to-day life. Not every type of tags is suitable for every kind of application and every type of item. National Academies of Science has allocation of tags-to-item diagram which is depicted in Figure2. It is an approximate guideline to see which tag is appropriate for which asset. Since this diagram is as of 2004, they still consider the bar codes to be a choice for consumer items and use RFID tags only when inventory and supply tracking matters.

Figure2. Types of Assets and Types of Tags



Source: National Academies of Science, 2004

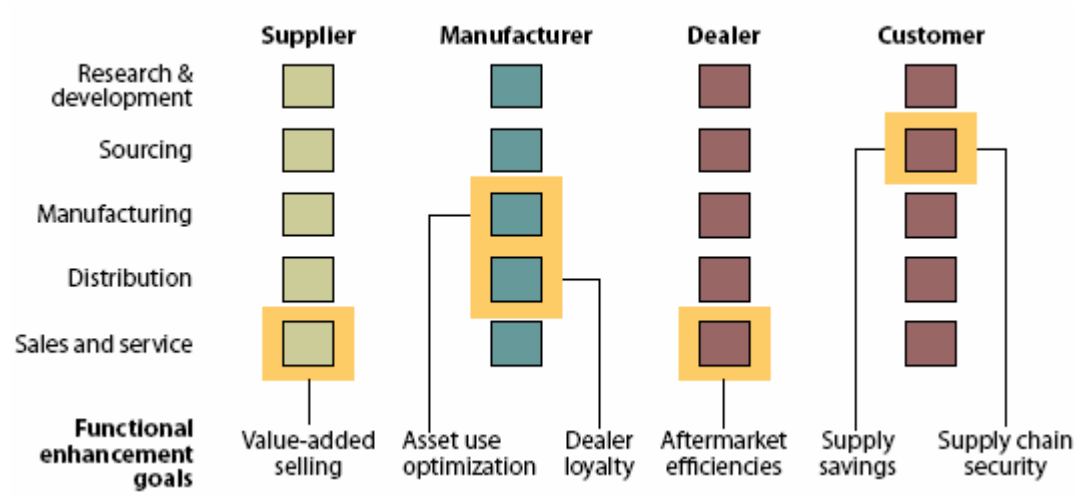
Why RFID?

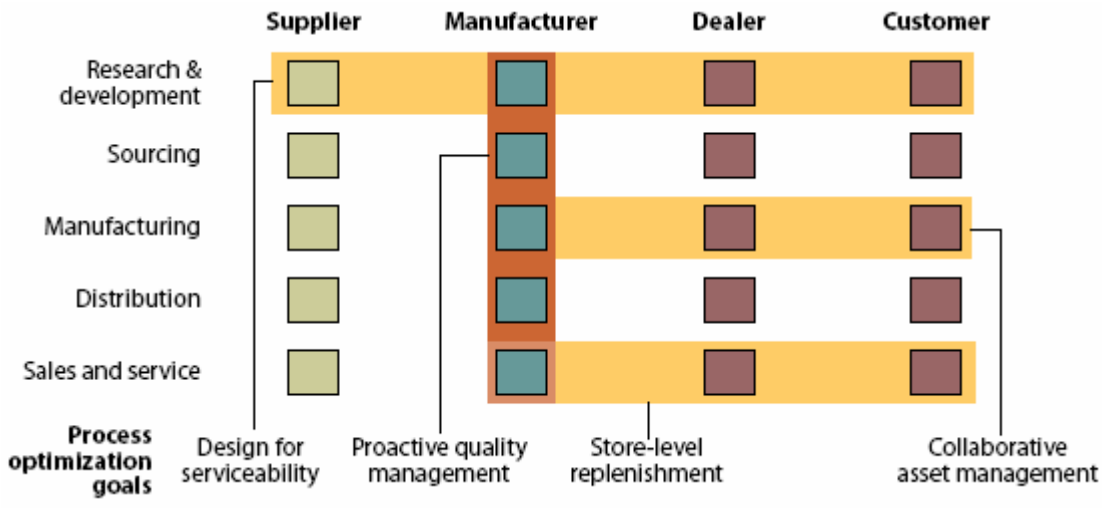
It's a good question to ask, why do companies adopt RFID? Do the benefits of RFID really overweigh the challenges of adoption process? For answering these questions we need to study the potential benefits and problems of adoption of this technology. All agree that three main parties initiated this wave: US Department of Defense, Wal-Mart and Tesco (Food Chain in Britain). Other than these three organizations and those that are closely related to them like top hundred suppliers of Wal-Mart-which are required to deploy RFID technology, there must be a set of reasonable benefits that motivates other organizations and companies to plan for RFID adoption. We start with what John Williams, director of the MIT Auto-ID Labs calls internet of things when he says "*There is simply an enormous amount of applied research that needs to be done to move RFID forward and realize the dream of creating the Internet of Things*." They believe RFID is a layer on top of the Internet, "*It envisions a global infrastructure - a layer on top of the Internet - that will make it possible for computers to identify any object anywhere in the world instantly*" (www.autoidcenter.org/aboutthecenter.asp, visited August 17, 2003); or similarly it's called extended Internet (X-Internet) by researchers in Forrester Research, Inc. who in contrast with privacy advocates believe that this trend will help companies boost regulatory compliance and increase customer loyalty. Yogesh V. Joshi at MIT (now at Wharton University of Pennsylvania) who has studied the impact of RFID on supply

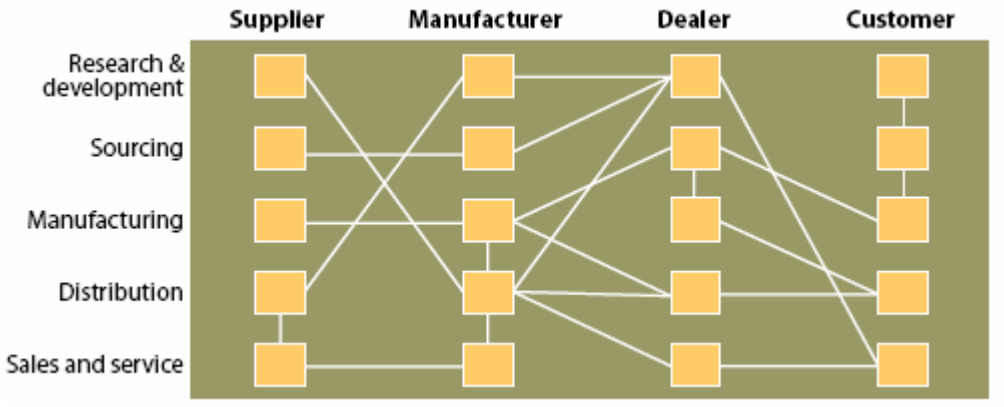
chain, talks about information visibility and demand visibility, while both of them affect supply chain dynamics, latter will bring about an enhanced forecasting power to the company.

More on benefits, Elgar Fleish in his study refers to RFID-like trends as "Pervasive Computing" that he believes reduces cost of integrating the Information Systems' world or virtual world to physical world. He also describes that pervasive computing increases time granularity and enhances management power in the way that they'll have more control on what's happening in their inventories, in their supply path and in their stores. Elgar Fleish also counts data granularity as other contribution of RFID to business applications which also helps in tracking purposes and market intelligence creation; but the point is that this great amount of raw data with increased granularity in both dimensions of time and object, needs advanced methods of filtering to extract the most useful information which matters for managers in different level of organizational hierarchy. I'll talk about potential challenges of RFID deployment in the next section. Researchers in Forrester Researcher, Inc. in [1] also explain an interesting point of view of what they call X Internet phenomenon. They divide firms into three groups and they do discuss RFID impacts on business separately for each group of firms. These three groups are conservative firms, efficiency-seeking firms and aggressive firms. As depicted in Figure3 they propose that conservative firms may use X Internet for functional enhancement in their organization. The main characteristics of these firms as identified by Forrester Researchers are that they have risk-averse culture and/or their IT spending is less than two percent of their revenue. Also they propose that efficiency-seeking firms use X Internet for process optimization purposes; main characteristics of this group of firms are that they are experienced in process improvement methods (i.e. ISO9000) and/or have the tradition of sharing the risk among trading partners. The third class of firms are what the Forrester Researchers call aggressive firms; which may use X Internet for a more advanced goal and that is business model reinvention. These firms are those which are under strong competitive pressure, need to expand market shares rapidly, have thin profit margin or too expensive products. These are all Forrester Researchers' prospect which sounds very interesting; however the classification may seem not to cover all kind of firms in the real world.

Figure3. Firms Use of X Internet for Different Organization Goals







Source: Forrester Research, Inc.

RFID Adoption Challenges

As I was going thorough the documents, reports or guidelines provided by standardization organization like EPCglobal, early adopters or RFID technology

researchers, I could feel how much concern still exist in this area mostly because of lacking standards and regulations or privacy-protection related legislations. This apprehension is obvious everywhere even if in Senator Patrick Leahy when he gives a speech about RFID at Georgetown University Law Center in March 2004: "*…the RFID train is beginning to leave the station, and now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights*." Again he says: *"there is no downside to a public dialogue about [RFID], but there are many dangers in waiting too long to start. We need clear communication about the goals, plans and uses of the technology, so that we can think in advance about the best ways to encourage innovation, while conserving the public's right to privacy."* Now we need to study how different parties engaged in this barcode-to-RFID transition process behave.

Manufacturers and Adopters

RFID manufacturers and adopters experience different problems from those of legislators and customers. Manufacturers are still striving to come up with cheap RFID tags and readers. Based on pilot projects conducted by Proctor & Gamble and Tesco and advice from other expert parties, Consumer Packaged Good (CPG) firms and retailers now believe that widespread adoption of RFID requires the price of tags to be as low as five cents. On the other hand, manufacturers believe that with the current small market of RFID adopters, they can't really lower the price that much. Manufacturers also think there is a price/functional complexity tradeoff; companies sometimes need functional features that make manufacturing obscure and therefore expensive. There is another issue of tag-reader dependency. Manufacturers which are making both of them are pro tag-reader high dependency because it makes their processes easier and also they believe this decrease cost of integration for adopters and also makes it more feasible to achieve optimal performance; however specialist manufacturer are pro tag-reader independency so that tags and readers standards could evolve better and every company could decide about tags and reader types separately according to compatibility standards. This debate still exists; some market watchers believe RFID tag/reader market is best suited for major companies like Texas Instruments (TI) which are able to lower the price by leveraging economy of scale and other think that there's a good opportunity in this market for specialist to introduce

and provide high-quality, functionally complex tags/readers for groups of companies that need it.

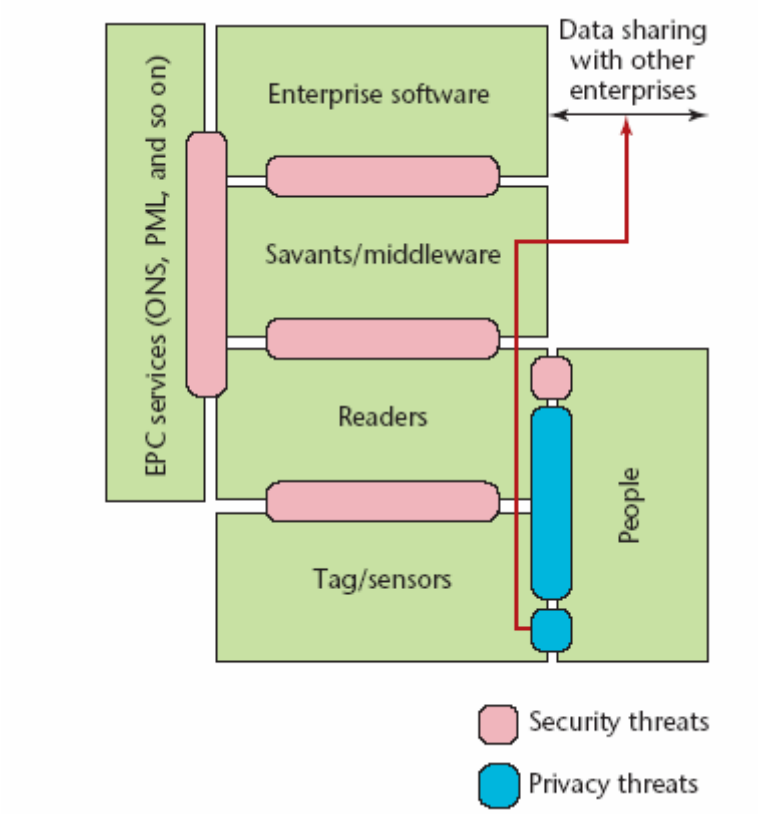
Also environmental conditions, being in the vicinity of radio-reflective materials (e.g., metals) and radio-absorbing materials (e.g., liquids) as well as ambient ,because they absorb the RF energy emitted by a reader significantly, reduce the range of an RFID system dramatically; therefore manufacturers need to consider this in their design. Health affect of high frequencies of radio frequency is a fact that all parties engaged in this area should study.

Moreover, adopters need to assess new requirements and risks that emerge from RFID-enabled Enterprise Systems. Having RFID hardware at hand, firms need to have the appropriate middleware connect the physical world to their enterprise applications, more importantly they need to change or redesign processes to support their new system.

Other than internal systems integrations and change management, companies need to integrate their boundary systems with those of their partner. This is especially true for retailers that engage in long paths of supply to procure their products. The RFID system will be more beneficial to all partners when they integrate their application just like the time before RFID deployed.

Finally, security and privacy are among crucial aspects of RFID adoption process. Juels in his research survey on RFID security and privacy [9], pointes out that many believe data-security problems – like that of authenticating readers to servers – involve already familiar data-security protocols. But the very massive scale of RFID-related data flows and cross-organizational information sharing will introduce new data-security problems**.** Garfinkel et al has in [10] use an easy-to-understand diagram of security and privacy threats in EPC network. As Shown in figure4, they consider tag/sensors and readers connection to be the origin of individual privacy threat and consumer/reader connections to be part of security threats which may cause problem to the internal Enterprise Information System.

Figure4. Security and Privacy Threats in an Abstract View of EPC Network
(Garfinkel et al., IEEE Security and Privacy, Feb. 2006)



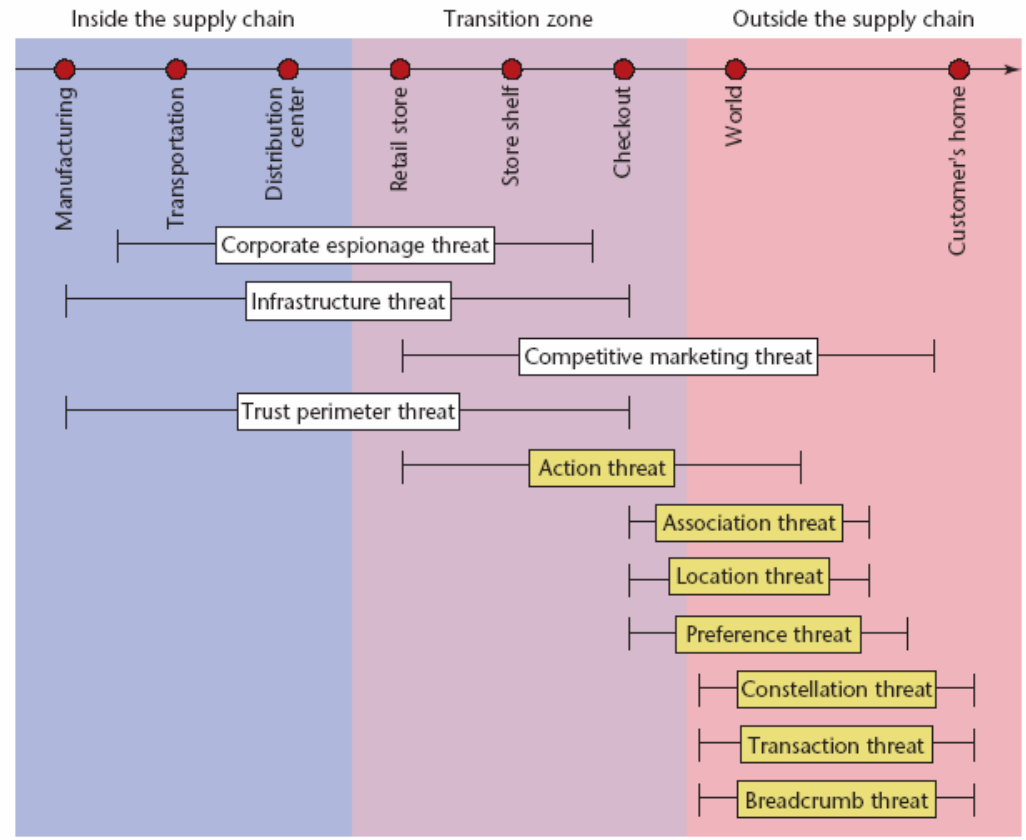
Individuals Consumers

Now we are coming on the other side to look at RFID technology and its consequences for our day to day life. Albrecht and McIntyre in their article call RFID as "The Big Brother Bar Code" and quote from California State Senator Debra Bowen that "The privacy impact of letting manufacturers and stores put RFID chips in the clothes, groceries, and everything else you buy is enormous."

Consumer privacy advocates believe that RFID simplifies gathering consumer intelligence and this may lead companies to pass the privacy red line more easily. There is also concern regarding reusable type of class 4 and class 5 tags. Organization for Economic Co-operation and Development in their recent report [5] suggests that manufactures should incorporate privacy as a high priority task during the hardware design, what they call *privacy by design*. OECD report, mentions infrastructure threat such as denial-of-service attack through, radio frequency signal jams as those on the enterprise side and not specific to RFID technology; also they mention skimming and eavesdropping; such as surreptitious reading/intercepting data on RFID tags, illicit tracking, Cloning and ID theft as those threatening both companies and consumers

[6]. However Garfinkel et al. their IEEE Security and Privacy article [10] have a more comprehensive approach to the security and privacy risks in RFID networks. In their study they classify EPC tag context into three zones: inside the supply chain, transition zone and outside the supply chain (Figure 5).

Figure5. Threat Context in EPC Deployment
(Garfinkel et al., IEEE Security and Privacy, Feb. 2006)



As depicted in figure 5, they also differentiate threats primary affecting corporation (white color) from those primarily affecting individuals (yellow color). I found it helpful for understanding different threats to overview their classification therefore I have the summary of the threat description in table2. Garfinkel et al tell a story of the cloning threat in which researchers at Johns Hopkins University and RSA Laboratories recently identified a serious security weakness in the RFID tag in Speedpass devices and many automobile immobilizer systems. Researchers also believe that tag read ranges are an important factor in discussions about privacy.

Table2. Garfinkel et al. Classification of Threats in RFID-equipped Systems

(IEEE Security and Privacy, Feb. 2006)

Threat	Description
Action Threat	An individual's behavior or intend is inferred by monitoring the action of a group of tags
Association Threat	The customer's identity is associated with the item's electronic serial number and unlike customer loyalty cards it can be done surreptitiously and also it associates with a customer's identity a unique product (name/brand…) not a group of products
Location threat	An individual is tracked if the tagged items he/she carries are known; or an item's specification is disclosed by unauthorized readers.
Preference threat	Customer preference is acquired at a low marginal cost by having when item tag uniquely identifies the manufacturer, the product type, and the item's unique identity
Constellation threat	The regardless of person's identity tags form a unique RFID shadow or *constellation* around the person and can be used by unauthorized entities to track people, without necessarily knowing their identities.
Transaction threat	It is easy to infer a transaction between the individuals when tagged objects move from one constellation to another
Breadcrumb threat	Individual's identity associated with items database Enterprise System. Even if they discard these *electronic breadcrumbs*, the association between them and the items isn't broken. And can be used, for example, to commit a crime or some other malicious act.
Corporate espionage threat	Tagged objects in the supply chain make it easier for outsiders to remotely gather supply chain data, which is some of industry's most confidential information
Competitive marketing threat	Tagged objects make it easier for competitors to gain unauthorized access to customer preference
Infrastructure threat	Although not specific to RFID, there is some vulnerabilities regarding system dependency on radio signals transmissions
Trust premier threat	Not specific to RFID, Sharing high volume of data introduces more risks

Legislators

Adam Arceneaux, technology risk consultant at Protiviti believes that legislators still have time to see what comes out of RFID technology in practice to decide about necessary regulations; he thinks consumer privacy would be of the first issue to

address. He explains that there will be two waves of concerns and therefore regulations, first of them would be those that have been brought by individual privacy advocates and the second would be those related more to security of financial transactions through RFID tags and readers. It can be inferred from Adam Arceneaux's point of view that some of the threats such as preference threats, and transaction threat illustrated in Figure4 by Garfinkel et al. are not new or specific to RFID, so there may be some burdens on companies regarding securing high volume of data but the process of doing that may not be complex. I'd like to mention filtering as a technique that companies need to invest on to make the database sizes more manageable. Mr. Arceneaux also believes that other regulations like those relating to electronic waste management are not so surprising challenges; however the industry moves forward and rules should address the problems organization and individuals face; otherwise the rules will be abstract and obsolete.

Waste management is still an issue; In Europe, the Waste Electrical and Electronic Equipment (WEEE) Directive mandates recycling of tags but if tags are embedded into items then the tags need to be removed first and recycled after that. Energy management, and radio frequency in some areas need license that legislative and standardizations organizations are in charge of. For any area of practice, there are different legislation in different countries and regions. Since one of the promising realms of RFID is supply chain support; and supply chain potentially incorporates long ways from one part of the world to another, it needs the tags and readers to meet international standards through the way. Technician may suggest that different tag standards are able to be read by the same reader, in that case the cost of the reader increases to support multiple standards.

CASPIAN has proposed a model legislation titled the "RFID Right to Know Act of 2003" that would require labeling of RFID tagged items. In the summary of bill it says" *To require that commodities containing radio frequency identification tags bear labels stating that fact; to protect consumer privacy, and for other purposes*."

Several state bills have been patterned after this model. In the United States, some states have initiated RFID privacy legislation, most notably California, where the state assembly considered (and rejected) bills in 2004 and 2005. A. Juels in [9] explain that often overlooked in policy discussion is the REAL ID Act, recently passed by the

U.S. legislature. This bill mandates the development of federal U.S. standards for drivers' licenses, and could stimulate wide deployment of RFID tags**.**

OECD has a privacy framework which is useful to start from and add technology specific aspects. The following are from "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" [5] and I cross-linked them with different threats in Garfinkel et al. classification in Table3.

1. Collection limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data quality: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the data subject; or b) by the authority of law.

5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual participation: An individual should have the right a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him (within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him); c) to be given reasons if a

request made under subparagraphs a) and b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles.

Table3. Cross Link between Garfinkel et al. Classification of Threats and OECD and EPCglobal Guidelines for Privacy

OECD Privacy Guideline	Garfinkel et al. Classification of Threat	EPCglobal Privacy Guideline
Collection limitation	Action threat	Consumer notice
Purpose specification, Openness	Association threat	Consumer education
Use limitation	Location threat	Consumer notice
Purpose specification	Preference threat	Consumer choice
Data quality	Constellation threat	Consumer education
Security safeguards	transaction threat	Record Use, Retention and Security
Individual participation	Breadcrumb threat	Consumer choice
Accountability	Infrastructure threat	Record Use, Retention and Security
Security safeguard	Competitive marketing threat	Record Use, Retention and Security
Security safeguards	Corporate Espionage threat	Record Use, Retention and Security

What I've done in Table 3 is to see which of the guideline may address which of those threats in Garfinkel et al. classification. For example last row shows that corporate espionage threat may be addressed by security *safeguard* requirement of OECD privacy guideline and Record use, retention and security in EPCglobal privacy guideline. EPC Global guideline for RFID adopters includes notice-choice-education-security; in the guideline they explain these requirements as follow [7]:

1. Consumer Notice: Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer Choice: Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer Education: Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarize consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record Use, Retention and Security: The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

However the issue of choice is considered the most complex one. Two-way readers that can be used to remove that the tags are expensive and so it may not possible for every supermarket to have that at every check-out counter. More importantly, activated tags can have a post-sale value to consumers [10]; so simply killing or removing them when products are purchased is not a cure-all for the RFID privacy problem. Consumers need those tags for return and guarantee purposes and repairs, physically or mentally impaired individuals can take advantages of tags to use readers to access contents of a product, brand and other information about it more easily.

Mr. Arceneaux (Risk Manger/Consultant at Protiviti), believes that technical solutions alleviate threats inside the supply chain and transition zone; he mentioned the example Wal-Mart and Target that would prefer their tags not be readable by each others' reader. This is a good example of competitive marketing threat and Mr. Arceneaux thinks second wave of solutions would be for that section. Juels in his survey on RFID security and privacy [9] gives example of some kind of protection methods like: tag pseudonyms, tag passwords, blocker tags and antenna-energy analysis. The same author in [8] states encryption methods on transmission device; and he explains that because of their intentionally simple design, EPC tags cannot support expensive, traditional cryptography and security functions—not even basic ciphers. Tight economic considerations suggest that this will remain the case for the foreseeable future.

Conclusion and Guideline for Future Adopters

The main question to ask when company thinks of RFID adoption are: how can we measure the value that RFID brings to organization? How can we asses marketing and inventory benefits on one hand and risk management costs, compliance costs and privacy and security provision costs on the other? If firm decides to have hosted implementation, there will be premier trust threat, then how can it manage privacy? It's interesting that according to Forrester Research Inc. experts, firm don't see the compliance hurdles as a big issue but they're concerned of technology maturity. Inferring from Protiviti Risk Consultant, Mr. Arceneaux speech, most of the threats classify by Garfinkel et al. like association threat, preference threat and competitive marketing threat are not new or specific to RFID. Therefore company might be able to overcome them rather smoothly during the time when they learn their best practices. Adam Arceneaux also thinks that the first wave of legislation will be on the consumer privacy protection side and the second wave would be on technical side to solve mostly the problems in transition zone, those related to financial transaction, credit cards, ID theft and cloning. He also thinks that legislators still need to observe industrial challenges in practice when RFID becomes more widely used and then they'll set regulations to address those issues. He also thinks that companies already complying with SOX would try to incorporate RFID compliance into their SOX compliance framework.

References

[I] Adam Arceneaux, Protiviti Technology Risk Consultant, May 2006, Phone interview

[1] C. S. Overby et al., "RFID: The Complete Guide", Forrester Research, Inc., Spring 2005

[2] Steve Hodges and Duncan McFarlane, Auto-ID Labs, Cambridge University, UK, Sep. 2005

[3] "Creating a RFID Privacy Plan", RFID Journal, May 26, 2003, http://www.rfidjournal.com/article/view/433

[4] http://www.spychips.com

[5] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980, www.oecd.org

[6] Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations, OECD report, Mar 2006

[7] http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

[8] A. Juels and S. A. Weis, "Defining Strong Privacy for RFID", RSA Laboratories, April 2006.

[9] A. Juels." RFID security and privacy: A research survey", IEEE Journal on Selected Areas in Communication, 24(2), February 2006.

[10] S. L. Garfinkel, A. Juels, R. Pappu, "RFID Privacy: An Overview of Problems and Proposed Solutions", IEEE Security and Privacy, May/June 2005, Vol. 3, No. 3, pp. 34-43

[11] Elgar Fleish, "Business Impact of Pervasive Technologies: Opportunities and Risks", Human and Ecological Risk Assessment, 2004, No.10, p. 817–829.

[12] http://www.nocards.org/rfid/rfidbillsummary.shtml

[13] K. Albrecht and L. McIntyre, "RFID: The Big Brother Bar Code", CASPIAN Consumer Privacy, ALEC Policy Forum, Winter 2004, Volume 6, Number 3, pp. 49-54.