RADIO FREQUENCY IDENTIFICATION: REGULATING INFORMATION PRIVACY PROTECTION

by

Deanna R. Laufer

B.S. Electrical and Computer Engineering
Cornell University, 2005

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Technology and Policy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2007

Signature of Author .....
Technology and Policy Program, Engineering Systems Division
August 10, 2007

Certified by .....
Robert Laubacher
Research Associate, Center for Collective Intelligence
Thesis Supervisor

Accepted by .....
Dava J. Newman
Professor of Aeronautics and Astronautics and Engineering Systems
Director, Technology and Policy Program

RADIO FREQUENCY IDENTIFICATION: REGULATING INFORMATION PRIVACY PROTECTION

by

Deanna R. Laufer

Submitted to the Engineering Systems Division on
August 10, 2007 in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Technology and Policy

Abstract

As applications of Radio Frequency Identification (RFID) become more profuse, the technology itself is stirring up some controversy. Due to its potential for amassing large amounts of information about both people and things, and the possibility of using the information for marketing, tracking, or even spying, numerous consumer groups are spearheading efforts to ensure that RFID does not breach their privacy rights. While there are some privacy laws regulating specific aspects of commerce, there are no laws which currently apply to the collection and use of information as it pertains to RFID. This lack of formal regulation allows companies to legally engage in practices which may encroach on consumers' privacy. However, RFID has the potential to optimize supply chain practices as well as provide other benefits to both consumers and businesses. As RFID use becomes more widespread, regulatory strategies should be considered to protect consumers' right to privacy while obtaining the benefits of using the technology.

This thesis explores consumer and industry opinion of RFID through a customized survey. Results of the survey found that consumer and industry opinion are similar in many aspects, especially in the concern for protecting privacy and the desire for a regulatory mechanism to enforce those privacy rights. This thesis addresses the question of whether market-based solutions, self-regulation, or government regulation is the best option for addressing consumers' legitimate concerns of privacy while allowing businesses to reap the benefits of using the technology. The regulatory options are compared and then discussed based on the needs of consumers and industry members as determined by the survey. Finally, four recommendations are suggested to provide guidance for ensuring a positive acceptance of RFID while acknowledging the privacy rights of consumers.

Thesis Supervisor: Robert Laubacher
Research Associate, Center for Collective Intelligence

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION/MOTIVATION

Radio Frequency Identification, or RFID, arose shortly after the development of radar, yet it was not until years later when its use became more prominent. One of its first major applications was for automatic toll collection, beginning in the late 1980s.[1] The 1990s saw wide-scale deployment of RFID toll collection across the United States. Applications were soon broadened to include parking lot access, campus access, and fare collection. With the technology evolving into smaller microchips and tags, the possibilities for RFID grew tremendously in the 21st century, from use in the supply chain to other locations in the marketplace and public sector.

As applications of RFID become more profuse and realized, the technology itself is stirring up some controversy. Due to its potential for amassing large amounts of information about both people and things, and the possibility of using the information for marketing, tracking, or even spying, numerous consumer groups are spearheading efforts to ensure that RFID does not breach their rights, specifically their right to privacy. One consumer advocate co-authored a book called, "Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move."[2] Some have even likened RFID chips to biblical predictions about the Mark of the Beast,[3] a concept from the Christian Bible describing how "the Beast" will require all people to receive the mark in order to buy or sell.

Some worried consumers are calling for boycotts of RFID tagged products. In 2003, the United Colors of Benetton, an international clothing company, announced that they would sew RFID tags into certain clothing items. Soon after, Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) led a boycott of Benetton products. Benetton then publicized that they would no longer be using RFID.[4] Other scare tactics include a website[5] dedicated to warning consumers to boycott Gillette products as they may contain tracking devices in the form of RFID chips.

In response to this negative publicity, RFID manufacturers and other members of the industry are trying to reduce the controversy by masking their use of RFID. They are referring to RFID tags

as radio barcodes, intelligent labels, electronic product codes, green tags, and contactless smart cards[6] in the hopes of taking the spotlight off their use of RFID.

While some of the publicly raised privacy concerns seem outlandish, many are actually quite warranted. In the retail industry, RFID does have the potential to track consumer purchases by linking product information obtained with RFID to personal information, such as credit card numbers obtained by the store. Tagging individual consumer goods with RFID creates the potential for large amounts of data to be collected, requiring strict security efforts to protect the data. While there is currently no federal legislation pertaining to RFID, many states have introduced legislation in the past few years, most which have not succeeded in passing. Recently, California re-introduced legislation aiming to restrict RFID use by the public sector.[7] While legislating RFID use too early may restrict innovation, there needs to be insurance that consumers and all citizens will feel secure in using this technology. However, if legislation is passed after many businesses have already incorporated RFID into their practices, they may face higher costs later in meeting any restrictions the legislation may place. There can be an even stronger backlash against regulation in the future when many businesses will be highly invested in the technology.

This thesis examines RFID use and its implications on information privacy and discusses policy options for protecting privacy. Applications of RFID span from use in the public sector for identification cards and transportation passes to use in the private sector in retail stores and in hospitals. In order to narrow the scope of the research, this thesis focuses on RFID use in the retail sector—in a warehouse, distribution center, or retail store—for individual consumer goods affixed with RFID tags, also referred to as item-level RFID tagging. Based on these specifications, the privacy risk of using item-level RFID is examined. This examination involves weeding through possible privacy implications of RFID and choosing those which are the most plausible for the specific situation chosen to assess. Once the risk is assessed, the thesis lays out the regulatory options available to protect information privacy from item-level RFID use, including market solutions, self-regulation, and government regulation. Finally, based on data collected about industry and consumer preferences, a recommendation is made for a regulatory

solution for ensuring consumer privacy as well as other actions businesses and law-makers should undertake to ease the acceptance of RFID.

To give readers a better understanding of the basics of RFID, Chapter 2 gives an overview of RFID technology, describes how it functions, and discusses some of the applications in the retail industry. Chapter 3 discusses the current privacy laws in the United States, illustrating the lack of privacy protection as applied to RFID use. Next, Chapter 4 focuses on the implications of RFID use, describing the most significant risks to privacy.

The following chapters describe the development, dissemination, and analysis of survey data used to understand consumers' and the industry's views about RFID. Chapter 5 discusses the survey methodology, describing both the consumer survey and the company survey used to assess their understanding of and concerns about RFID. This chapter also examines whether there is any inherent bias in the results due to the online method of data collection. Chapter 6 lays out an analysis of the survey results, including charts and tables illustrating consumer and industry views. In order to understand the best method of regulation, Chapter 7 introduces various methods and then recommends a solution based on the survey analysis from the previous chapter. Finally, Chapter 8 discusses some the analysis and gives recommendations about how lawmakers and industry members alike can use this work to further socially responsible RFID use.

CHAPTER 2: BACKGROUND ON RFID

Radio Frequency Identification is a method for automatically identifying tagged objects. Senator Patrick Leahy likened RFID tags to "barcodes on steroids."[8] RFID tags can be affixed to almost any object and store a unique identification number for that object in its electronic chip. The information embedded in the chip is communicated to an RFID reader through electromagnetic waves. When RFID readers are networked to computers, data from the tags can be read into an information system or database.

RFID is an improvement over barcodes because unlike barcodes, RFID allows for the capture of data without line of sight from the tag to reader and over longer distances. This eliminates the need for manual scanning, which is necessary when using barcodes. RFID also allows for the reading of hundreds of tags in seconds, whereas barcodes can only be scanned manually, one at a time. The Electronic Product Code (EPC), which is currently being used in conjunction with RFID tags for retail applications, can store more information than the barcode, which means many more objects can be uniquely identified.

RFID, however, is not without its flaws. Just as there were concerns voiced prior to the adoption of the Universal Product Code (UPC) symbol as the standard for barcodes, there is also concern about the cost and performance of RFID. Read rates may not be 100%, meaning that some tags may be missed by a reader, resulting in errors in calculations or miscounts. Tagging individual items is quite costly since installing RFID tags is more expensive than simply labeling a product with a barcode. Though RFID presents costs and performance risks, it also provides opportunities to increase efficiency and productivity and ultimately to save time and money.

The Technology

System Components

RFID tags, or transponders, consist of a miniature electronic chip, which stores data, and a small radio antenna which transmits data to a reader. In the case of most retail supply chain applications, the data will consist of a unique EPC. Tags can be either active or passive, depending on whether they contain a power source. Since passive tags are smaller and less expensive, they are more practical for use in retail supply chains. Tags can come in many sizes and can be embedded right into a product or placed on the disposable packaging, like a label.

RFID readers, or interrogators, consist of a radio frequency module, control unit, and an interface to communicate received data with a data processing system. Readers transmit a radio frequency signal to the transponder, which triggers an RF emission from the tag. The data contained in the tag is reflected or sent back to the reader.[9] The read range, the distance between the tag and the reader, is dependent on the frequency of the RF signal as well as the design of the tags and readers. Some readers will pass the information directly to an attached computer, while controlled readers may first do some validation and basic filtering of the signal.

Figure 1 illustrates the movement of data between components in an RFID system. In addition to the tags and readers, the system will contain other components which are part of an EPC network.[10] This network includes software used for receiving and sorting data, as well as integrating the data between systems. The software may also pass the EPC information to a directory service which uses the EPC to retrieve the location of information associated with the particular code in its database. A complete RFID system requires hardware and software for these purposes and for facilitating systems integration between RFID components and an organization's existing information system.

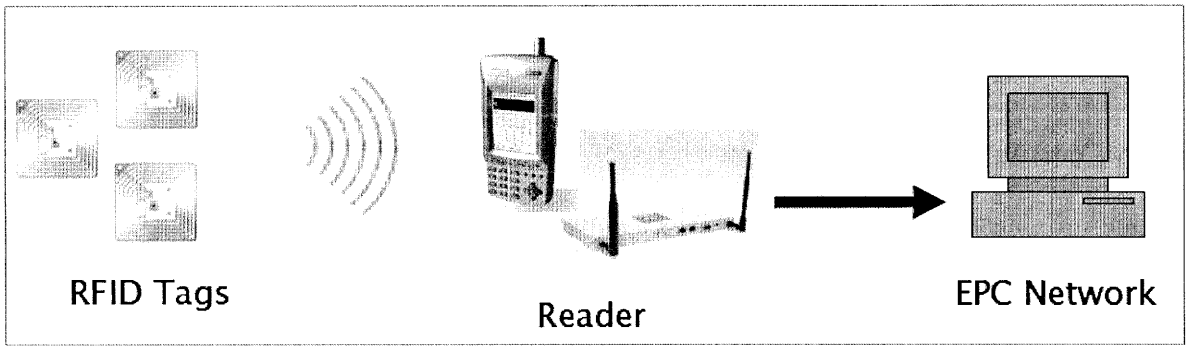

Figure 1: RFID system components.

Active and Passive Tags

There are two types of RFID tags: active and passive. Passive tags, which are smaller and cheaper than active tags, have no internal power source. They are powered by incoming radio waves transmitted by the reader, which are then reflected back and detected by the reader. Typical passive tags range in size between a postage stamp and a credit card, and can cost between 5 and 40 cents depending on the size and manufacturer. Passive tags are better candidates for retail use since they are less expensive and the tags will most likely be discarded after their first use.

Active RFID tags have an internal power source used to generate an outgoing signal. Active tags are more reliable than passive and can transmit at higher power levels, in more challenging environments and over longer distances. The downside of active tags is that their need for batteries gives them a finite shelf life and they can be more costly than passive tags. RFID devices used to collect electronic highway tolls make use of active tags.

Electronic Product Code

The Electronic Product Code is a successor to the Universal Product Code. EPCglobal, formerly the Auto-ID Center, oversees and leads the development of standards for EPC. Unlike the UPC, which contains only 12 digits and has one code for a type of product, e.g. a can of Diet Pepsi, EPCs are assigned for each unique product, e.g. for a particular can of Diet Pepsi. This distinction is possible since EPCs have more bits than UPCs, so there are far more combinations of bits.

The EPC is made up of three main partitions plus the header, which specifies the format of the EPC number.[11] The first partition is the manager code, determined by the manufacturer responsible for maintaining the code. The second partition specifies the object class, or type of object. The last partition encodes the unique object identification number. For an object with the same manager code and object class, there are at least 68 billion combinations of unique item numbers, allowing each item to have 68 billion unique identifications.[12]

Supply Chain Benefits from RFID

So far this thesis has discussed how RFID tags operate and their improvement over the barcode, but not their potential for saving time and money. RFID can have a great impact on the operations of manufacturers, distributors, and retailers in a supply chain. RFID has applications in manufacturing, logistics, and product support. It can transform processes throughout the supply chain, enabling reduction in labor requirements, faster throughput, and the collection and use of more accurate data.

RFID tags can be used on several types of containers in the supply chain, including pallets, cases, and individual items. Pallets are the largest shipment size of goods and are comprised of multiple cases. Cases contain a grouping of multiple items, the number depending on the type and size of item.[13] Since many shipments are done by the case or pallet, businesses may find it more cost effective to affix an RFID tag to each pallet or case for tracking it though the supply chain.

In a warehouse or distribution center, RFID has impacted supply chain management by automating processes and through improved accuracy in counting and tracking products. Tagged pallets and cases can improve warehouse and distribution center processes such as receiving, put-away, picking, and shipping by allowing for faster counting and verification of objects. Since RFID works without line of sight, it eliminates the need for manual scanning, saving labor time and reducing human error. RFID can improve the put-away and picking processes by

communicating with warehouse employees about which items to stock where and which items to pick. Again, this improvement both saves labor time and reduces errors.

In the retail store, case and item-level tagging can improve receiving and put-away processes, in a similar manner to the way it improves these processes in the warehouse. In addition, RFID can allow for tracking of tagged items in the store, thereby signaling suspicious movement of products by working in concert with store security systems. RFID can also be used to monitor inventory levels on shelves, signaling to store employees when stocks are low. By integrating point of sale data, RFID can provide visibility into the movement and sale of products, enhancing inventory management and demand planning.

There are seven primary distinct benefits from RFID tagging in the retail supply chain—enhanced customer relationships, automation, reduction in shrinkage, reduction in claims, reduction in inventory, reduction in unsaleables, and reduction in out of stocks.[14] Some of these benefits, such as automation, can be achieved without any collaboration with other companies, while some, including reduction in claims and shrinkage, require collaboration with the next partner in the supply chain. The other benefits—reduction in inventory, out of stocks, and unsaleables—require collaboration across the entire supply chain. While the last six benefits can be quantified, the first, enhancing customer relationships, is substantially more difficult to measure. Overall, consulting firm A.T. Kearney projected that a retailer could save 32 cents on every sales dollar if they fully utilize RFID applications, which is a remarkable cost savings.[15] Figure 2 depicts the seven main types of benefits derived from RFID in the retail supply chain setting and where they are likely to occur.

Automation

RFID reduces the labor required to find and count cases and individual items. Automating certain processes in the retail supply chain, including receiving, staging, order assembly, truck loading, and shelf stocking can decrease the labor costs and time needed to perform these actions.[16] By using RFID, manual labor, which was formerly required to scan barcodes to count the number of cases, will be reduced, allowing a reduced labor cost and faster throughput time.

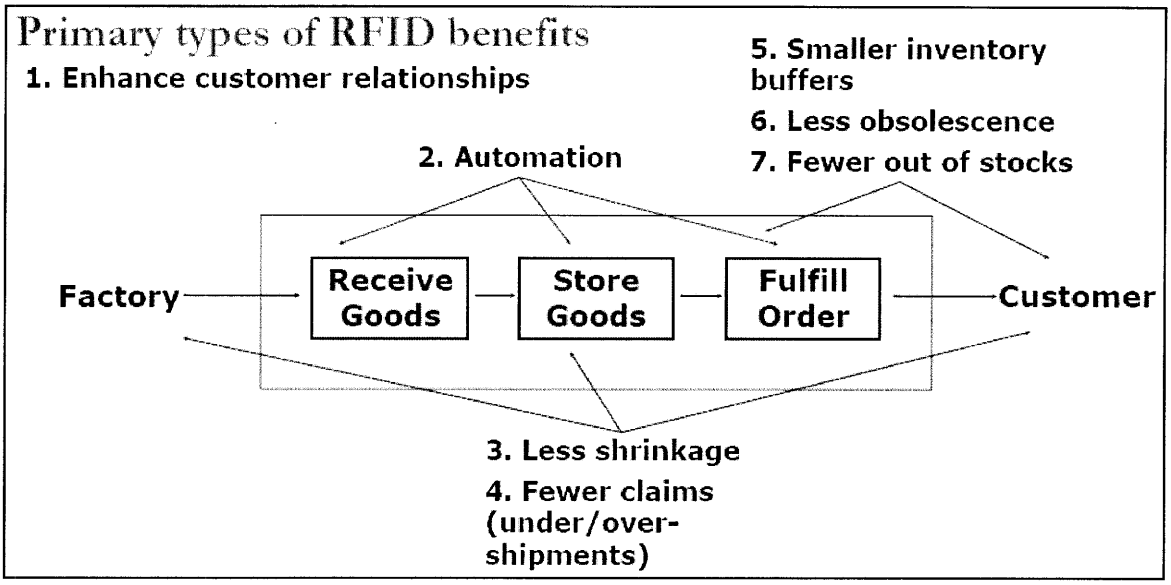

Figure 2: Primary types of supply chain benefits from RFID.[17]

Reduction in Shrinkage

There are three types of shrink, or loss of goods—internal theft, external theft, and paper shrink.[18] Internal theft occurs when employees steal goods. External theft includes shoplifting, fraudulent returns, or theft by outside parties that handle goods within the supply chain. Paper shrink is caused by process and administrative errors, including inventory imbalances, incorrect invoices, incorrect pricing, or scanning errors.

More accurate supply chain data enabled by RFID allows manufacturers and retailers to identify where theft is occurring and take measures to reduce it. RFID can also reduce the errors that lead to paper shrink. For a manufacturer, paper shrink can be reduced through accurate verification of delivery quantities, the ability to track returns, and the ability to verify inventory on hand. RFID allows paper shrink at the retailer to be mitigated by in-store verification of pricing and by enhancing the ability to verify physical inventory.[19] Both case and item-level RFID have the capability to reduce in-store theft by helping identify suspicious behavior and alerting store personnel. Item-level RFID tagging can also be used to reduce return fraud through unique identification of a product.

Reduction in Claims

Claims result when trading partners in a supply chain disagree about the number of units, cases, or items, in a shipment. Discrepancies that lead to claims typically occur due to process or administrative errors. Both parties to a claim must devote administrative time to investigation and negotiation. If a supplier is found to have sent an undershipment, it is responsible for replacing the missing goods and must sometimes pay penalties. RFID can reduce the cost associated with claims by tracking the movement of goods between trading partners, creating a more accurate record of a shipment. This reduces labor costs associated with claim investigation and re-shipments and penalty payments associated with claim resolution.[20]

Reduction in Inventory

To account for delays in transportation and/or inaccurate forecasting, retailers and manufacturers must keep a high amount of inventory on hand. Demand planning, order cycle time, and the replenishment process all affect inventory levels at retail stores and distribution centers. Notwithstanding existing control systems, implementing RFID will enhance these, reducing the amount of inventory kept on hand through more accurate and timely information about the quantities of goods present at key points.[21] Cost reduction can include both a one-time savings due to the reduction in overall inventory levels and ongoing annual savings in inventory carrying costs.

Reduction in Unsaleables

Unsaleables occur when a product can no longer be sold in new or perfect condition. Typical reasons for this occurrence are damaged goods, seasonal changes, and out-of-date products. Obsolescence can cause losses to the retailer and manufacturer with mark-downs, write-offs, returns, or destruction of products, especially in the grocery and pharmaceutical sectors. Seasonality, on the other hand, is more prevalent in the apparel and toys sectors, where changes in consumer tastes and fashion cause product mark-downs or stock write-offs. Finally, the consumer electronics sector is susceptible to unsaleables due to the frequency of new product introductions.[22]

To reduce loss associated with obsolescence, RFID can improve data integrity and supply chain visibility to optimize first-in first-out management. RFID can also improve trading partners' visibility to optimize safety stocks and maintain temperature conditions in the grocery sector. Better visibility can improve lifecycle management and inventory accuracy, reducing inventory levels and improving forecasting and pricing strategies.

Reduction in Out of Stocks

Out of stocks occur when consumers look for a product on the retail shelf and it isn't there. Out of stocks result in lost sales for both retailers and manufacturers. Shopper satisfaction surveys confirm the importance to retail customers of products being in stock. Studies of consumer behavior indicate that out-of-stock situations lead to lost sales in at least some percentage of cases.

The primary causes of out of stocks are inaccurate forecasting and untimely shelf-replenishment. On average, 75% of out of stocks are caused in the store, while the rest occur upstream in the supply chain.[23] Other causes include inaccurate store inventory levels, lack of timely inventory information, "lost" items which may be in the store but not in their proper location in the back room, and stocking products on the wrong shelf. RFID can reduce out of stocks by enhancing the accuracy of store ordering and enabling timelier shelf replenishment. Specifically, more accurate data and the ability to find tagged cases and items automatically allows improvement of the stocking, order, and fulfillment processes in the store.[24] Reducing out of stocks can increase sales for the manufacturer and retail store as well as increase customer loyalty.

Pallet, Case, and Item-Level RFID

Privacy concerns are only relevant if businesses are using item-level RFID tags, as opposed to case or pallet-level. Any tags on cases or pallet will not be on items sold to consumers, so there is no chance a consumer will take one of these tags out of the store. Since pallet and case tagging involve fewer tags, it is also a less expensive alternative to item tagging. Many companies currently implementing RFID in their supply chain, such as Wal-Mart and Metro Group, are only doing so at the pallet or case-level.

Manufacturers and retailers can receive different types and degrees of benefits from RFID tagging depending on the tagging level. By tagging pallets only, businesses can reduce costs by automating processes such as receiving, storing, and shipping goods, but cannot receive the other types of supply chain benefits. Case-level tagging allows for more of the benefits because businesses have a more detailed view of the goods being handled. Case-level tagging allows for all the same benefits realized with pallet tagging, as well as some additional benefits. First, in terms of automating processes, case-level tagging allows for quicker packing of mixed pallets, which are pallets that contain different types of cases. By reducing picking errors in mixed pallets, businesses can reduce errors in delivery to retail stores, thereby eliminating unsaleables or returns to the manufacturer or distribution center. Case-level tagging can also automate inventory counts when the inventory is held in cases.

In the retail store, case-level tagging can reduce out of stocks by detecting the movement of cases around the retailer's backroom or store floor. It can also improve visibility in the supply chain, providing retailers and manufacturers with more accurate inventory information, reducing the inventory on hand that retailers need to keep. Reducing this inventory level saves retailers money in carrying costs and items that become obsolete or expire. To reduce theft, case-level RFID can be used to track shipments in the supply chain and monitor cases held in the distribution center or in the stockroom at the retail store.

Just as upgrading from pallet tagging to case tagging vastly improves the types of benefits RFID can provide, upgrading further to item-level tagging upgrades the degree to which retailers and manufacturers can attain these benefits. Businesses can get all the same types of benefits with item-level RFID, but to a higher degree since they have an even more granular tracking capability. Retailers can track items throughout the retail store, vastly reducing theft by knowing when the item leaves the store. Items are also less likely to be lost or misplaced throughout the store. By retaining an accurate inventory count using RFID, stores will know more accurately when they need to reorder items, reducing the likelihood an item will become out of stock. Finally, item-level tagging can improve the return process by allowing customers to return products to the store without a receipt and facilitating restocking.

Though items level tagging costs retailers and manufacturers more, because it necessitates far more RFID tags as well as more readers placed in the store, the benefits of item-level tagging are also increased over case and pallet-level tagging. In one case study performed by Accenture, where item and case-level tagging were examined for a retailer, they found that the benefit from automation was 55% higher with item-level tagging, almost 275% higher in reducing shrinkage, and about 230% higher in reducing out of stocks.[25] In a different case study, IBM Business Consulting found that using item-level tagging as opposed to case-level tagging increased the benefit from reducing out of stocks by 72%, increased the benefit from automation by about 100%, and increased the benefit from reducing inventory by about 100%.[26] Though these numbers were early calculations, and not actual measurements of RFID in action, they illustrate the potential benefit from using item-level tagging, and therefore suggest a likely eventual shift to item-level tagging.

Consumer Benefits from RFID

In addition to supply chain benefits to manufacturers and retailers, RFID may also provide benefits to consumers. While some supply chain applications involving case and pallet-level RFID are already in use, many of the consumer applications necessitate item-level RFID and are therefore only proposed or in testing.

Consumers can benefit directly from some of the supply chain applications described above. Reducing out of stocks ensures that items are on the shelves when consumers look for them, eliminating the need to choose another product or go to another store. There is evidence that some of the cost reductions that stores obtain may be passed on to consumers, resulting in lower product prices. In fact, this occurred with the introduction of the Universal Product Code.[27]

There are other potential applications more directed towards consumers. The Metro Group RFID Innovation Center is testing RFID applications in the warehouse, department store, supermarket, and private household.[28] One idea is that RFID can be used in shopping carts, to keep track of the total price of all items at any point during shopping. This feature can aid consumers in controlling spending while shopping. RFID can also provide access to more information about a

product, such as ingredients or recipes in which it can be used. RFID tagged items may also prompt targeted ads or discounts in a supermarket, which may be more useful to shoppers than generic promotions. Finally, RFID can aid a smart checkout system whereby each item does not have to be scanned individually, but rather the whole shopping cart can be scanned at once.[29]

In the department store, RFID can be used to create Smart Dressing Rooms, which may supply additional information about garments, including available sizes, or product accessories. Similar displays may be placed on the sales floor, triggered when shoppers remove clothing from the sales rack. Sales staff may be alerted when certain goods run low, so they can restock before goods become out of stock.[30]

Lastly, in the private home, Smart home appliances, such as medicine cabinets, washing machines, or refrigerators can be designed to operate autonomously by reading the tags on items they contain. A Smart fridge could detect if products contained inside were running low and alert the owner.[31] A Smart washing machine could read the tags of clothing, ensuring the proper cycle or temperature is being used on the garments.

RFID is also being used for applications outside of retail. Active RFID tags are currently being used in highway toll systems so that drivers don't have to stop or pay cash at the toll. ExxonMobil Speedpass also makes use of RFID to allow for automatic payment. There are several other uses of RFID projected for the future. Some of these include:

- Tagging patients, staff, and equipment in hospitals to reduce costs and increase patient safety by reducing medical errors
- Tracking and tracing pharmaceuticals to prevent counterfeit drugs
- Using Smartcards or RFID in cell phones for automatic payment (e.g. public transportation)
- Tracking library books
- Tracking airline baggage
- Tagging livestock and pets
- Preventing passport fraud

RFID benefits are more easily quantified for businesses than for the consumer, since businesses gain efficiency or higher sales, while consumer may only gain time or added features in shopping. Despite the difficulty in quantifying benefits for consumers, they must be considered along side the costs of privacy loss in formulating adequate regulations.

CHAPTER 3: PRIVACY IN LAW

The encroachment on privacy that is discussed in Chapter 4 is likely because of the absence of laws pertaining to RFID use. To understand how best to regulate RFID practices, we must first understand any current privacy laws as well as some of the past attempts at regulating RFID to protect privacy.

The United States, Canada, and Europe

While there is no direct mention of privacy in the U.S. Constitution, some Courts and scholars have construed the 14th Amendment to include such a right. "No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law," has been deemed to imply the right to the liberty of personal autonomy.[32] There is also some international precedent for the right to privacy. The United Nations, in the Universal Declaration of Human Rights,[33] states in Article 3, "Everyone has the right to life, liberty and security of person," and in Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

In the United States, it is the duty of the Federal Trade Commission to enforce the statutory right to privacy, limiting access to personal information. However, many of the statutory rights relate to specific aspects of privacy and would therefore not cover information privacy intrusions from RFID. The Privacy Act of 1974[34] regulates the disclosure of personal information by the federal government but does not apply to private entities. The Gramm-Leach-Bliley Act[35] only applies to financial institutions. The act mandates that financial institutions must respect the privacy of its customers and protect the security of their personal information. It also mandates that financial institutions provide a privacy policy to customers explaining what information is collected and how it will be used.

The Fair Credit Reporting Act[36] regulates the collection and use of consumer credit information by consumer reporting agencies. The act covers consumer reporting agencies, defined as those people or entities that assemble or evaluate consumer credit information. Like the Gramm-Leach-Bliley Act, this act only regulates personal information for a specific use, which is credit reporting in this case. Lastly, the Children's Online Privacy Protection Act of 1998[37] regulates the online collection of personal information from children under 13 years of age. Websites that may collect information from children must post privacy policies and obtain parental consent before collecting information from children.

While these four statutes regulate certain aspects of privacy and are all enforceable by the FTC, there are still many aspects of information privacy which are not covered, namely collection of personal information by private entities which are not financial institutions, or online collection of personal information of adults. When it comes to other practices, the FTC only has the authority to prevent "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practice in or affecting commerce."[38] However, the privacy implications discussed in Chapter 4 do not fall under the umbrella of unfair methods or deception.

The FTC is currently administering the policy of voluntary self-regulation for other areas of the market which are not legislated. The FTC suggests five fair information practice principles that businesses should adhere to when collecting or using personal information: notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Each of these principles describes a guideline for entities accessing or obtaining personal information. (Chapter 7 elaborates further on each of these principles and their specific application to RFID). This current policy would apply to information collected with RFID technology in consumer products. Any information collected with RFID technology, such as names, addresses, credit card numbers, or store purchases, is not legally protected by any federal privacy legislation.

Other nations have stricter privacy laws than the United States. The Canadian "Personal Information Protection and Electronic Documents Act"[39] mandates that businesses must obtain consent in the collection, use, and disclosure of personal information. The act also gives consumers a method of reprieve, whereby individuals can bring up complaints to the Privacy

Commissioner for further investigation. The act was rooted around fair information principles, dictating that entities can only collect information specific to a transaction. Further, they must explain the purpose of collection and to whom they wish to disclose the information. Individuals may also request information about themselves to correct and verify the data. Overall, the act resembles the five fair information principles recommended by the FTC,[i] though in Canada they are part of the law. The legal situation in Canada is an interesting comparison to that of the U.S. since this particular act is recent, going into full implementation in 2004, and designed with input from businesses, governments, and consumer associations.

The European Union, under Data Protection Directive 95/46/EC,[40] also regulates the use of personal information by private entities. The directive[ii] mandates that data must be fairly and lawfully processed for limited purposes and kept no longer than necessary. Data collection requires the explicit consent of the individual and the data must be relevant and non-excessive to the purpose of collection. Furthermore, since the E.U. has strict personal data laws, information can only be transferred to countries outside the European Union if those countries maintain an adequate level of protection, a criterion which the United States currently does not meet.

In addition to the original data protection initiative, the directive gives latitude for creating commissions to consider amending the regulation. In 2005, the E.U. released a Working Document[41] issuing guidelines for the private sector for the use of RFID. The document sets out principles for the collection and use of information collected using RFID. The document requires businesses to give notice of the presence of RFID tags and readers to consumers as well as explain the purpose of use. The fact that European law is ahead of American law in legislating RFID is consistent with the pattern of the E.U. relying more on government enforcement and the U.S. relying more on self-regulation.

---

[i] The FTC advocates five fair information practice principles: notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Each of these principles sets a different guideline for entities accessing or obtaining personal information. Chapter 7 elaborates on each of these principles and relates them to RFID use.

[ii] A directive is a legislative act of the E.U. which is not in of itself legally binding, but requires member states to achieve its rules through its own legislation.

As opposed to the current U.S. policy of self-regulation, H.J. Smith of Wake Forest University noted that European countries follow an "omnibus fashion [of law-making] by passing sweeping privacy bills that address, in general terms, all the instances of data collection, use and sharing throughout the society."[42] This is in contrast to the U.S.'s approach of segmented legislation pertaining to certain applications of privacy, such as the financial institutions and credit reporting acts. There are many reasons for this variance, primarily a difference in politics and governance, but it may also be due to the manner in which various countries view privacy as a right. While Europe sees privacy as a fundamental human right, the U.S. seems to regard it, at least in the commercial arena, as a negotiation between businesses and consumers and as a cost/benefit conciliation.

Though the three sovereign entities—the United States, Canada, and the European Union—maintain differing privacy laws, they share a common reliance on fair information principles. Canada and the E.U. both have different versions set into law, while in the United States the FTC recommends compliance with the principles by business organizations. In an international marketplace, it is important that businesses are able to operate across borders without many roadblocks from the law. With the introduction of mass quantities of data collected with RFID technology, sharing data across country lines may be inhibited by differing privacy regulations between the countries. Businesses must acknowledge the need to become familiar with these laws, and perhaps meet the highest restrictions in order to conduct business in all necessary countries.

The FTC and RFID

The FTC held a public workshop in 2004 called "Radio Frequency Identification: Application and Implications for Consumers."[43] The FTC used the workshop to obtain both industry and public opinion with respect to RFID applications and privacy and security concerns. The committee staff published a report of the workshop's proceedings and the FTC's decision to regulate RFID at the time. Ultimately, the workshop found that while some participants were concerned about item-level RFID, due to their conspicuous size and the ability to monitor consumers surreptitiously, other participants believed that the privacy concerns are exaggerated.

The FTC stood behind self-regulatory models for addressing privacy concerns, noting there was also a need for transparency in labeling the presence of tags or readers. They also cited the importance of meaningful accountability to ensure compliance with self-regulatory measures. The FTC left it to companies to address privacy concerns raised by RFID applications, noting, however, that it would not disregard the possibility of issuing guidelines in the future.

Though the FTC chose not to issue strict regulations at the time, many factors may have influenced the decision. RFID was still a new technology and many of the applications which people are most concerned about are not yet a reality. While regulation may have been premature then, future regulation may be necessary as RFID becomes a ubiquitous technology. The analysis takes into account future applications of RFID and tries to anticipate the optimal regulatory path for the future, not only present day.

Proposed U.S. Laws

Only one federal law dealing specifically with RFID has made it to a Congressional committee thus far. U.S. HR 4673, 2004, would require businesses to place warning labels on consumer products containing RFID tags. The bill would also require giving consumers the option to remove the tag from the product or permanently disable it at the time of purchase.[44] However, this bill never made it out of committee. Several state bills have also been introduced, though the majority of those also failed in committee or on the floor.[45] Table 1 lists several which have been introduced as well as the purpose of each. Only the bill from New Hampshire was successfully passed into law.

The majority of state bills are similar to the federal bill in that they require that notice be given to consumers when purchasing a product containing an RFID tag. Missouri, Utah, Nevada, and Tennessee State governments all introduced bills requiring that labels be attached to consumer products bearing an RFID tag.[46] A Massachusetts bill[47] requires, in addition to labeling on products with RFID tags, that a sign to be a placed in an area with RFID readers, identifying the presence of the technology and the purpose of the readers. The bill mandates giving consumers the option to remove the tags after purchase if not essential to the items' operation. New Mexico

also proposed a bill[48] requiring the removal of RFID tags on consumer goods at the point of purchase and limiting release of personal information collected with the tags. South Dakota incorporated the principles of consent into a proposed bill,[49] mandating that consent must be given by a person before another person or entity can gather personal information and link it with data collected by an RFID system. The bill also discussed other fair information principles including access to the data and security.

Bill Number	State	Purpose
U.S. HB 203-FN, 2006	NH	Establishes a commission on the use of radio frequency technology with a report by November 1, 2008.
U.S. HB 1136, 2005	SD	Requires written consent, as well as fair access and security practices.
U.S. H.B. 314, 2004 Gen. Sess.	UT	Mandates labeling for products with RFID tags.
U.S. HB 251, 2004 Gen. Sess.	UT	Mandates labeling for products with RFID tags.
U.S. SB 128, 2005, replaced by U.S. SB 13, 2007	MO	Mandates labeling for products with RFID tags.
U.S. SB 181, 2005 and U.S. SB 159, 2007	MA	Requires notice of RFID tags and readers, an explanation for the purpose of the readers, and an option to disable or remove the tags after purchase.
U.S. SB 699, 2005	TN	Mandates labeling for products with RFID tags.
U.S. AB 264, 2005	NV	Mandates labeling for products with RFID tags.
U.S. HB 5929, 2005	RI	Restricts state agencies from using RFID to track the movement or identity of employees, students, or clients.
U.S. HB 215, 2005	NM	Requires the removal of RFID tags on consumer goods at the point of purchase and limits release of personal information collected with the tags.
U.S. HB 2953, 2005 and U.S. HB 1925, 2007	TX	Prohibits a school district from requiring a student to use RFID or a similar technology which may be used to identify, transmit information regarding, or track the location of the student.
U.S. SB 30, 2007	CA	Restricts the use of RFID created or issued by public entities in identification documents.

Table 1: U.S. state laws pertaining to RFID use.
Note: This table is not an exhaustive list of all state legislation regarding RFID use.

In addition to these bills legislating commercial use of RFID, several states have proposed bills legislating public use of RFID. Rhode Island proposed a bill restricting state agencies from using RFID to track the movement or identity of employees, students, or clients.[50] A Texas proposal[51] prohibits school districts from using RFID devices to identify or track students.

A California bill from the current legislative session, which was recently passed overwhelmingly by the Senate, aims to restrict the use of RFID in publicly issued identification documents.[52] A similar bill was introduced in 2006 but was vetoed by the governor. California has been especially eager to pass an RFID bill as they recognize special privacy protections unique to the state. California considers the right to privacy as "a personal and fundamental right protected by Section 1 of Article I of the California Constitution and by the Unites States Constitution. All individuals have a right of privacy in information pertaining to them."[53]

The only state bill that has been passed thus far was in New Hampshire, which established a commission on the use of RFID with a report due by November 2008.[54] While the overwhelming majority of these bills have been refused, states may continue introducing new legislation until appropriate federal legislation is passed.

An RFID Bill of Rights

As a response to some of the lingering privacy concerns, several interest groups have developed recommendations for self-regulation. EPCglobal developed four guidelines for RFID use for consumer products pertaining to consumer notice, consumer choice, consumer education, and retention and security.[55] As EPCglobal notes, "They are based, and will continue to be based, on industry responsibility, providing accurate information to consumers and ensuring consumer choice." EPCglobal has not ignored privacy concerns, but instead has tried to set an example by outlining principles to be followed.

Several privacy advocacy groups, including CASPIAN, Privacy Rights Clearinghouse, the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC) drafted a position statement on the use of RFID on

consumer products in 2003.[56] This statement identified RFID as a threat to privacy and civil liberties by enabling individual tracking and profiling, hidden readers and tags, and large data aggregation. It endorsed principles of fair information practice when using RFID, specifically openness, purpose specification, collection limitation, accountability, and security safeguards. The statement even went so far to say as RFID should be prohibited in certain instances, such as when merchants force customers to accept RFID tags in products, tracking individuals without their consent, or using RFID to eliminate or reduce anonymity.

CASPIAN even went as far as drafting proposed legislation, entitled the "RFID Right to Know Act of 2003"[57] requiring products bearing RFID tags to be labeled as such. The act also limited any businesses' use of RFID information linked to personal information.

While these recommendations addressed the privacy issue in different ways, there is no consensus between them. Both EPCglobal and the group position statement outline principles for self-regulation, though the EPCglobal statement only recommends compliance with the principles of notice, choice, and security, while the group position statement also advocates for purpose specification, collection limitation, and accountability. EPCglobal and the CASPIAN act recognize the importance of consumer education, though the CAPSIAN act also includes limitations on RFID use and the requirement for labeling of products containing RFID tags. Self-regulation would be most effective if supported by both consumer and industry groups, though currently it seems as though there are discrepancies between the recommendations of the groups. Examining which principles and types of regulation are most important to consumers and businesses could help lead to consensus in developing guidelines for RFID use.

CHAPTER 4: PRIVACY IMPLICATIONS OF RFID

Privacy Susceptibility

Information privacy can be described as "The ability of individuals to control the terms under which their personal information is acquired and used."[58] This concept may be extended to controlling information about oneself for the purpose of confidentiality, keeping certain information secret, and anonymity, keeping actions only traceable by oneself.[59] Protecting privacy is not a new issue brought on by the advent of RFID, rather, privacy in general has been a concern since 1890 when Warren and Brandeis defined privacy as "The right to be let alone."[60] However, with the introduction and growing use of the internet, as well as technologies such as RFID which foster the large collection and use of personal information, protection of privacy has become a growing concern.

While some aspects of information privacy are protected by law, including those of financial privacy and children's online privacy, other aspects enabled by RFID, especially by the private sector, are not currently legislated. The most applicable guidelines are the Fair Information Practice Principles,[61] recommended by the Federal Trade Commission (FTC), which provide a suggestion for how companies should obtain and use personal information. These principles, however, are not enforceable by law, and the FTC can only regulate practices to prohibit unfair methods of competition and prevent deceptive acts in the marketplace.

Concerns about RFID

In order to illustrate the "Big Brother" aspect of RFID, many writers invoke a particular scene in the 2002 movie *Minority Report* as a possible application of the technology. In the film, which portrays a futuristic society lacking many of the individual privacies we now enjoy, characters receive personalized billboard advertisements as they pass by, made possible by scanning their eyes. One advertisement tells the character, played by Tom Cruise, "You could use a Guinness right about now."[62]

While that scene is purely fictional, RFID could enable a similar scenario. If an RFID tag was placed in a consumer item, say a running shoe, and a reader was able to detect the tag and identify the object by its unique EPC, it could trigger targeted advertisements that could be displayed, say for new running shoes from that brand, or complimentary products. This application does not necessitate the identification of the person wearing the product, but rather only the product itself. However, if the purchased running shoe was linked to personal information about the consumer, and the information was available publicly or to the owner of a particular RFID reader, advertisements may be directed to that person based on a profile of all his or her purchases, instead of just the one. Many consumer advocates have raised concerns about RFID uses and have illustrated future scenarios such as the one above, yet not all scenarios apply to retail RFID use and not all are equally plausible.

Non-Retail Threats

While there are many applications of RFID, those not pertaining to the private retail sector are not within the scope of this thesis. The public sector is considering RFID for passports and other government issued IDs and for IDs in schools. RFID is also being used in highway toll collection and public transportation. Each of these applications produces different scenarios in which an individual's privacy may be compromised.

Many countries are beginning to use RFID chips in passports. The U.S. State Department announced in August 2006 that they would begin issuing electronic passports which contain a contactless chip in the rear cover.[63] The chip contains all the personal information printed in the passport, as well as a digital picture of the passport holder. Future passports could contain other biometric data including fingerprints and iris patterns. U.S. passports will have a metallic anti-skimming material, a built-in security device, to try to prevent unauthorized reading of the passport when it is fully closed.[64] Other security measures are being included as well to prevent the passport holder from being tracked. Despite these security measures, many opponents are still unsure that surreptitious reading can be prevented. Prior to the release of the passports, one security consultant demonstrated how he could crack a similar passport and even replicate the

RFID chip inside.[65] Alternatively, if the RFID chip itself fails, travelers may face delays or disruptions in their flight plans.

RFID tags are also being used in student IDs in schools. In 2005, a northern California public school began issuing mandatory ID badges with RFID tags to track students, without informing the students or parents.[66] When a student passed by a scanner at school, the device transmitted information to a computer about the student and his or her whereabouts. Many civil liberties groups and parents were alarmed by the breach of privacy of their students and asked for the school to discontinue use. Other schools have also experimented with RFID badges; one used RFID to record when students got on and off school buses.[67] While badges may be used for beneficial applications, such as ensuring the safety of students to and from school and on campus, many believe mandatory use is still a breach of a person's civil liberties. Some states have even considered legislation to prevent RFID use in schools.

Though some public sector uses may be mandatory, others are not, giving a user the choice whether to use the RFID application. Many users, however, may not be completely educated about the privacy implications of a certain technology when they make that decision. Highway toll collection systems make use of active RFID tags for easy toll payment, allowing drivers through without having to stop at the booth. These tags are a substantial convenience for drivers by saving time on the road. Typically, users will register for the tag, which is linked to a credit card on file used for making the payment. Since the devices used are active RFID tags, they are always on, transmitting signals which can be picked up if a proper reader is nearby. Houston is using RFID for more than just toll collection, staging automated vehicle identification at several points along the toll road. The identification points can determine vehicles' speeds and travel routes.[68] While the system may be beneficial for traffic management and emergency response, drivers may not want to subject themselves to being "tracked" along the highway.

The Bay Area Toll Authority began issuing mylar bags to enclose the toll tags when not in use, blocking signals tags may be sending.[69] The Bay Area uses toll tags for toll payment and for providing traffic flow data to the Transportation Commission, though information collected is done anonymously through the use of encryption software. Even though having these toll tags is

not mandatory for drivers, many find the convenience outweighs the possible privacy implications of tracking. Other states may want to consider an opt-out approach similar to the Bay Area, to give users an option about which applications they would prefer to use the toll tag for.

In a similar vein, RFID-enabled transportation passes are used in subway systems in Boston, Washington, D.C., and other cities across the country. These credit card-sized passes act as entry and exit payment systems for public transportation. Though some passes can be purchased anonymously, others require registration or link to a credit card. When linked to personal information, data may be collected about a person's travel—when and where they enter stations and other travel habits. Again, users can often opt-out of these systems, but the alternative may be more inconvenient or more costly. Using these passes, like the toll passes, reduces anonymity, decreasing the user's personal privacy.

Unlikely Threats

The next set of threats is those which may be possible with RFID chips in individual consumer items, but are unlikely to occur. While unlikely, they are plausible threats, but because of the lack of current technology, widespread use of RFID, or high cost of implementation, these applications are not imminent, and therefore not as important as some of the more plausible applications which may encroach on personal privacy. In addition, since item-level tagging is not currently pervasive, many of these threats may not even be applicable for 10-15 years.

Surveillance is an oft overstated concern with RFID. While people-tracking using RFID tags embedded in consumer products, such as shoes, clothing, or wallets, is technologically feasible, surveillance is more likely to be at the level of FedEx tracking a package, than constantly monitoring people's whereabouts. This means that while readers could detect the tags at certain points—entrances to stores, doorways, etc.—they cannot be continuously tracked. Since tags for consumer products are passive, they do not emit their own signal, like tags used for toll collection. This means the tag must be within read range of a reader, maybe 10-30 feet,[iii] to be

[iii] The read range depends on the frequency of the reader and tag and the conditions, e.g. if there is line of sight between the tag and reader.

detected. Unless there is an extremely large network of readers, RFID tagged items are not likely to be monitored or tracked more often than when a person walks through a specifically chosen doorway or area. Furthermore, not every reader will be able to identify every tag, since the reader and tags must use the same radio frequency and operate on the same protocol, or standard. Since there are currently no hard-line standards for RFID tags, it is unlikely that all readers will be compatible with all tags. If RFID becomes pervasive enough, then there may be large reader networks and the likelihood of surveillance will increase, but until then, other privacy threats are more imminent.

Probable Threats

Though item-level RFID is not currently a pervasive technology, decreasing tag prices are likely to drive wider adoption. With an increase of tagged items and RFID readers, tagged items will be detectable in and out of stores. The inconspicuous nature of tags and readers means a consumer might not know even know which products are tagged and whether a store uses RFID.

Although the RFID tag itself will only store a number, that number will be linked to more product information in a private or online database. Stores may choose to link information about purchased goods to personal information collected about the individual. This information can then be used by the store and 3rd parties it divulges the information to for targeted consumer marketing. Since it is likely that the store will share the information with at least partners in the supply chain, such as product manufacturers and distributors, it is possible that many parties will have access to the information.

There are two distinct privacy exposures with RFID-tagged goods on consumer items—RFID readers used in the store and detection by readers outside the store. RFID readers in the store, on shelves, in aisles, or at checkout, can be used to monitor the movement of products throughout the store. In the store, readers can detect tags which are either embedded in consumer products or affixed to the disposable packaging. Readers will be able to signal to store computers when items are taken off the shelf, placed in an RFID-enabled cart, or taken to checkout. Stores may want to use this feature to track "lost" products, when products are in the store but on the wrong shelf. However, if used as a marketing ploy, the store can tell which products you remove and then

place back on the shelf, revealing shopping patterns.[70] The information may also be used to display targeted ads for products complimentary to those already in your cart. While some shoppers may find this helpful, others may feel that their privacy is being invaded, and they are being spied on in the store. If RFID tags are linked to loyalty cards, the store may be able to make shopping recommendations based on all past purchases, not only present behavior. All this information on consumption patterns allows marketers to develop a more complete profile of every shopper.

Profiling consumers is essentially the same methodology as what is now happening with customer loyalty cards. Stores link customer sales with personal information in a store's database or the customer's store card to keep track of all customers' purchases. Profiling is also used in online stores such as Amazon.com, which use purchase information to make recommendations for future purchases.[71] Though use of consumer loyalty cards is optional, as well as shopping online at stores like Amazon, if RFID becomes pervasive enough, shoppers may not have the choice to avoid stores which use RFID. These stores are unlikely to give users the option to purchase products either with or without RFID tags, since it would complicate the stores' practices.

While the applications of RFID described above may pose as an annoyance and a privacy invasion to some consumers, others may actually find it helpful. Personalization of marketing made possible by profiling can reduce unwanted or wasted ads. The grocery store already does this by providing personalized coupons at checkout, while online retailers use previous purchases to recommend new products. RFID will allow a similar application, though it may come in the form of coupons, advertisements on the shelf, or throughout the store. This customization decreases costs for businesses by providing targeted advertising that is likely to be more effective than generic advertising, and produces no additional cost to the consumer other than the increase in intrusiveness and loss of anonymity.

Outside the retail store, readers will only be able to detect tags permanently embedded in products or those on the packaging of recently purchased products. Tags on the packaging of other items will have been discarded in the trash. As mentioned above, not all readers are

compatible with all tags, so RFID applications outside the store may be rare. While surreptitious detection of tags is possible, it may also be a rare situation. If consumers, however, are worried about their privacy, they may not want to carry around live RFID tags on products.

A final fear about tagging consumer products is the large amount of information that will be amassed. If all products were somehow linked to the internet, or to some other networked database, those who gain access, either rightfully or maliciously, could obtain purchase information, consumer information, or anything else that may be available. Authorized users may use the information for advertising and marketing, while those with malicious intent could obtain demographic or credit card information which could be used for theft. Strict security measures would have to be devised to prevent unauthorized access, though consumers may even feel it a breach of privacy if their information is kept without their approval.

Technology Solutions

Several researchers have suggested technological solutions for dealing with privacy concerns. Since this thesis focuses mainly on policy solutions, it only briefly describes some of the technology solutions. Any policy solution that is chosen should keep in mind the available technology as well.

One major privacy concern is the threat that tags on items can be read after leaving the retail store, allowing strangers access to the information stored within the tag. A technology solution to combating this problem is using the "Kill Tag" approach by disarming the tag after item purchase.[72] While this approach does avoid the privacy concern, there are some negative aspects as well. If the tag is permanently disabled, the store can no longer benefit from a more efficient return process if the consumer chooses to return that item. Similarly, the consumer may not be able to benefit from returning the item without a receipt, or using the tag at home with a Smart appliance.

Another technology option is the Faraday cage, which is a container made of a metal mesh or foil used to enclose the tag and shield it from radio signals.[73] California is currently offering this

approach to users of its toll collection system to shield the transponder when not in use. However, for consumer products this may not be a viable option if tags are manufactured into products and cannot be easily contained within a mesh.

A third option uses a blocker to obstruct the scanning of tags. A blocker could disrupt the RFID scanning process by simulating billions of RFID tags, causing a reader to stall.[74] However, consumers would have to obtain and carry around a blocker, and it may interfere with legitimate scanning, instead of just malicious scanning.

A final alternative entails security built into RFID tags to create "smart" tags, which can contain a variety of cryptographic solutions. One option could be a "smart" tag which would contain a privacy bit.[75] This bit would be part of the tag memory and could be *on* or *off*, indicating whether it could be freely scanned or not. Though a user may be able to control whether an object is scannable, use of this feature would be dependent on it being manufactured into the tag, and manufacturers may be resistant to such a feature if it greatly increases the price of producing a tag. Furthermore, consumers may not want to deal with the burden of learning how to operate the tag if it is complicated to turn it on and off.

While each of the solutions is either presently or soon will be technologically feasible, each also has significant drawbacks. Since none of these approaches is currently in use, and the focus of this analysis is on policy solutions, technology options will not be analyzed in depth, though they should be considered along with policy options when addressing the privacy problem. Computer-security research Simson L. Garfinkel suggests that implementing only a technical solution, and not also a policy solution, would "mean that anybody who could convince people [to] give up their information would suddenly be entitled to it."[76]

CHAPTER 5: DATA COLLECTION

Past Surveys

At least two prior surveys have been conducted regarding consumer response to RFID and privacy concerns. One member of the Auto-ID Center interviewed consumer groups to understand how RFID and EPC are perceived and to educate them about the possible benefits and harmful elements of the technology.[77] The survey found that most consumers felt impartial about the technology, but, nevertheless, wanted a choice in being able to deactivate the RFID tag after leaving a store. The results concluded that the Auto-ID Center should address privacy concerns by giving consumers the choice to disable tags and further reassurance about the technology.

Another consumer survey about RFID use was performed by Cap Gemini Ernst & Young in 2004.[78] They found that 77% of consumers they surveyed had not heard of RFID technology. Furthermore, of consumers familiar with the technology, 42% had a favorable view, 10% had an unfavorable view, and 48% were unsure or neutral. While CGEY did provide more detailed results, such as what specific concerns users had and what factors may influence their decision to use RFID-tagged products, the survey did not fully address all types of policy solutions available.

This thesis expanded on the prior surveys by questioning consumers about not only their perception of RFID, but also which types of solutions, e.g. "kill tags" or regulation, they find the most comforting in protecting their privacy. Though consumers may have concerns other than privacy, the survey was limited to only privacy issues in order to address them more fully. Also, while most people were unfamiliar with RFID when the other surveys were conducted, this research wanted to ascertain the percentage of consumers now familiar with RFID, three years later, and whether their perception had changed.

Both of the other surveys are consumer-targeted in nature. While one of the surveys conducted was a consumer survey, this research went further and presented a similar survey to businesses experimenting with or making use of RFID technology in order to understand whether they had similar concerns to consumers. The business survey also posed questions to these firms to understand which applications of RFID they find the most promising and which concerns they think will inhibit their business the most. Unlike other research conducted, this research tried to find similarities in the responses between consumers and businesses to understand all stakeholders' views before recommending a feasible solution for the protection of privacy.

Consumer Survey Development and Distribution

In developing the questions for the survey, past research was used to get a feel for some basic topics to cover, such as use of current RFID applications, knowledge or awareness of RFID, and information sources about RFID.[79] In addition, the survey was structured such that it obtained an answer as to the participant's prior knowledge of and perception of RFID. Following those questions, the survey included a brief overview of RFID to give participants a primer on the technology and applications of RFID. Also included in the primer was a section pertaining to the possible privacy implications of RFID. To get an unbiased opinion, the primer tried to educate the reader about those RFID applications which may impact privacy, as well as explain that the technology and read ranges affect the extent of the privacy implications. After the primer, the participants were instructed to answer whether their perception of RFID had changed after becoming more knowledgeable on the subject. This question was designed to see if consumers have a more positive or negative view about RFID after they are educated about its possibilities as well as its privacy implications.

Following those five basic questions, the rest of the survey was tailored to identifying the most important applications of RFID as well as the privacy implications of greatest concern to consumers and how they would propose addressing them. The survey asked users to rank, on a scale from 1 to 5, how they value certain potential or real applications of RFID. This question informed which applications are most important to consumers. Then the survey asked participants to rank their various concerns about RFID, whether it is loss of privacy, health risks,

increased prices of consumer goods, etc. Finally, the survey asked consumers which options, including various types of regulation, self-regulation, or technology solutions, they would find most appealing in protecting their privacy, and which standards of information collection they find the most important for businesses to abide by. Using these two final questions, combining them with which applications users prefer and what their concerns are, the research ascertained how important certain aspects of privacy are, how they relate to the desired RFID uses, and how strictly consumers would like to see them regulated. Appendix A contains a copy of the survey questions as well as the primer given to participants.

The survey was administered first online and then in person. The online survey guaranteed participants anonymity if they wished, but also included a demographic section. Links to the online survey were posted in three areas: on Mechanical Turk, an Amazon.com website, on Facebook.com, a social networking site, and on Craigslist.org, a community bulletin board website. On Mechanical Turk, the survey link and description were posted and participants were offered a 4 cent reward for their participation. The small reward gave users incentive to fill out the survey, while still not essentially "paying" for participation. On Craigslist, the link was posted in the volunteer section for users who came across it and wished to fill it out on a volunteer basis. Finally, on the social networking site, friends were asked to participate in filling out the survey. For all three sites, responses were automatically emailed back to my computer when the participant was finished.

Paper-based surveys were also distributed around Boston, Massachusetts near subway stations and public parks for users to fill out, and then return. Paper surveys were used to reduce the bias from only including users with access to the internet, since the type of user on the internet may have a different perception of or level of knowledge about RFID. Overall, 409 responses were received for the consumer survey from all the internet sources and the paper surveys.

Bias Checking: T-test

Since the research obtained results from four different outlets, an analysis was performed on the data to determine if there were any differences in the responses based on where, online or in-

person, the surveys were accessed. There is a possibility that the source of response affected the survey data. Specifically, the analysis was to determine if there were any disparities for two situations: between all surveys from the internet and surveys done in person, and between voluntary responses and paid responses.

A two-sample t-test was chosen to compare the samples. The t-test is used to determine if the means of two populations, in this case survey responses, are equal. The test verified the hypothesis that the means of the two distributions from which the samples were obtained are equal. The alternative hypothesis is that the means are unequal.

The survey responses were divided into five groups: those responses coming from the social networking site, responses from Craigslist, responses from Mechanical Turk, online responses from which the origin could not be determined, and responses from paper surveys. For the purpose of simplicity, these data sets will be hereafter known as Sample 1, Sample 2, Sample 3, Sample 4, and Sample 5, respectively. Since it was not feasible to compare responses for each of the questions on the survey, three questions were chosen for the t-test. Those questions pertained to the participants' prior knowledge of RFID, their initial perception of RFID, and how valuable they consider RFID for the application of faster checkout in retail stores.

In order to apply the t-test to the data, the analysis assumed that the data came from a normal distribution with unknown mean and common unknown variance. Though the sample variances were not exactly the same, the range of values was small enough to warrant this assumption. Since the test compares two sets of data, 10 tests were performed for each of the three survey questions to compare the data sets.

Question A: How familiar are you with RFID technology?

The first survey question tested asked the reader how familiar he or she was with RFID technology, giving them a range of five answers from "Have never heard of" to "Extremely knowledgeable." The analysis assigned each response a value from 1 to 5, and then calculated the sample means and variances for each of the 5 sets of data. Those statistics were then used to perform the t-test.

The two-sided test statistic, T, was used as defined below:

$$T = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{\left(S_1^2 + S_2^2\right)}{\left(n_1 + n_2 - 2\right)} * \left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

where $S_x^2 = \sum_{i=1}^{n_x} \left(X_i - \overline{X_{n_x}}\right)^2$, $\overline{X}$ is the sample mean, and n is the sample size.[80]

The T-statistic was calculated to test the hypothesis that the means of each sample were statistically similar, that is, that $\mu_1 = \mu_2$ at a level of significance α_0, where α_0 is the probability of exceeding the critical value.

After calculating the T-statistic for each of the pairs of data, they were compared to the *t* critical value, which can be found using a lookup table. The t critical value depends on the level of significance, α_0 as well as the degrees of freedom, which is $n_1 + n_2$, the sum of the samples sizes, minus two. For the purposes of this calculation, the level of significance, α_0, was chosen to be 0.05. Essentially, this means that we can be sure the correct hypothesis is chosen with 95% confidence. Since each set of data has a different sample size, there was a different value for the degrees of freedom in each case, and therefore a different t critical value.

Table 2 below shows the calculated T values for each of the ten tests performed.

	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		0.35	0.86	0.81	0.27
Sample 2			2.90	2.68	0.14
Sample 3				0.10	1.73
Sample 4					1.63
Sample 5					

Table 2: Calculated T statistic for survey Question A.

In the table above, the black cells denote pairs of the same sample, e.g. Sample 1 and Sample 1, where no test was performed. Since the order of the samples does not matter for the test, the calculated values would be reflected across the diagonal into the blank cells.

The t critical values are shown in Table 3 below.

	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		2.001	1.972	1.976	2.064
Sample 2			1.970	1.972	1.995
Sample 3				1.967	1.972
Sample 4					1.975
Sample 5					

Table 3: Critical t-value for each data set for Question A.

For each of the ten statistics, the calculated T value in Table 2 was compared with the corresponding critical t value in Table 3. For each pair, if $T < t$, then the hypothesis that the two data sets have the same mean is true, with 95% confidence. Equivalently, this shows that the two data sets have statistically equal means, which infers that there is no inherent bias due to the source of the survey data.

The table below was populated by comparing $T < t$ for each of the 10 sets and determining if, in fact, the t-test showed that the means of the two data sets were statistically equivalent. We can see that this is true for 8 of the 10 sets compared, but not for the sets of Sample 2 vs. Sample 3 and Sample 2 vs. Sample 4. For the question tested, which was whether the survey participant was familiar with RFID technology, there were statistically different means of the responses from Craigslist and Mechanical Turk, and of the responses from Craigslist and the unknown data set.

Are the means of the two data sets equal?					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		yes	yes	yes	yes
Sample 2			*no*	*no*	yes
Sample 3				yes	yes
Sample 4					yes
Sample 5					

Table 4: Comparison of calculated T statistic to t critical value for Question A.

In fact, Craigslist respondents were less likely to be familiar with RFID than either Mechanical Turk respondents or respondents from the unknown set, and according to the performed t-test, this difference is statistically significant. Though this analysis alludes to the fact that there may be some difference in the data due to the collection method, similar statistical analysis on the other two survey questions can give more insight into whether this is an anomaly or whether there are similar findings from the other questions.

Question B: What is your current perception of or feeling about RFID?

Question 4 from the consumer survey asked the participant about his or her current perception of or feeling about RFID. The possible responses varied from "Very unfavorable" to "Very favorable." Again, the answers were transposed to a scale from 1 to 5 and the means were calculated for each of the five data sets. Ten tests were performed, calculating the T-statistic and t critical value in the same manner as described above. The resulting calculations are shown in the tables below.

	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		1.59	1.42	1.47	1.35
Sample 2			0.83	0.79	0.29
Sample 3				0.05	0.20
Sample 4					0.18
Sample 5					

Table 5: Calculated T statistic for survey Question B.

	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		2.008	1.973	1.977	2.074
Sample 2			1.971	1.973	2.000
Sample 3				1.968	1.972
Sample 4					1.976
Sample 5					

Table 6: Critical t-value for each data set for Question B.

Table 7 shows that for each statistic calculated, T is less that t. In other words, the means of each comparison are equal, showing that the data for that particular question does not vary by sample set.

Are the means of the two data sets equal?					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		yes	yes	yes	yes
Sample 2			yes	yes	yes
Sample 3				yes	yes
Sample 4					yes
Sample 5					

Table 7: Comparison of calculated T to critical value t for Question B.

Question C: How valuable do you consider RFID for faster checkout at retail stores?

For Question 6a, which asked the participant to rate the value of using RFID for faster checkout in retail stores, a similar conclusion was found. For this calculation, the entries in the three tables were combined into Table 8 below, showing the calculated T statistics, the t critical value, and the check if $T < t$.

T statistic, t critical value, Are the means of the two data set equal (T < t)?					
	Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
Sample 1		0.01, 2.002, yes	0.17, 1.973, yes	0.59, 1.976, yes	0.13, 2.064, yes
Sample 2			0.38,1.97, yes	1.23, 1.973, yes	0.20, 1.996, yes
Sample 3				1.20, 1.967, yes	0.48, 1.972, yes
Sample 4					1.07, 1.975, yes
Sample 5					

Table 8: T statistic, t critical value, and comparison for survey Question C.

For Question C, as in Question B, the comparisons all showed that the samples had statistically equivalent means. In fact, of the three survey questions tested, only two pairs of data from Question A resulted in a rejection of the hypothesis that the means are equal. Since 28 out of the 30 tests performed indicated that there was little or no bias in the data based on the source, whether it be from one of the internet sites or from surveys conducted in person, this thesis will conclude for the sake of further calculations that the method of survey collection did not significantly affect the outcome of the data. For the first situation of concern, between surveys conducted in-person and those done on the internet, there was no statistical difference. For the other situation, between paid users on Mechanical Turk and unpaid volunteers on Craigslist, there was a difference in their Question A responses, with Craigslist users being statistically less likely to be familiar with RFID than Mechanical Turk respondents. However, there is no difference between samples for Questions B or C. Since the propensity of the analysis infers a lack of bias, this thesis will treat all responses of the consumer survey in a similar manner, with no regard to the source of the data.

Business Survey

The business survey specifically targeted members of those industries involved in RFID, including manufacturers of RFID components as well as those business that may use RFID in their operations. One organization contacted for this research was the Association for Automatic

Identification and Mobility (AIM). The survey was administered online as with the consumer survey, except that the survey was provided only to members of that organization.

The survey questions were slightly altered from those in the consumer survey, asking what RFID concerns the participants had for their company, rather than for themselves. Other questions were revised in a similar manner. Also, the survey assumed that participants were already moderately knowledgeable about RFID, so it did not include the primer section. Overall, fewer responses were received for this survey than for the consumer survey, but this was predicted inasmuch as the survey was not able to reach as many people.

Through AIM, 20 responses were received from members in various parts of their organization, including managers, those from sales, marketing, and IT, and analysts. Participants also varied by organization, age, and education level, so there was a mixed field of respondents. Though there was an attempt at outreach to other organizations, data was more difficult to collect for the business survey than for the consumer survey since the population targeted was so specific. Therefore, the collection of 20 responses, though much smaller than the 409 received from consumers, was used as the basis for the industry view for the purpose of this analysis. Since all business responses originated from the same source, there was no need to perform any tests to determine bias.

CHAPTER 6: DATA ANALYSIS

Awareness and Perception of RFID

While previous surveys revealed that few consumers were knowledgeable about RFID, results from this consumer survey reveal a different outcome. Rather, the majority of respondents, 62%, reported to be at least somewhat familiar with RFID. This increase in consumer awareness may be due to the time elapsed since the last survey. Alternatively, it could be because the survey was administered on the internet whose users may be more familiar with technologies than others. Expectedly, most industry members reported to be familiar with RFID. Figure 3 illustrates the range of responses for both consumers and industry members.

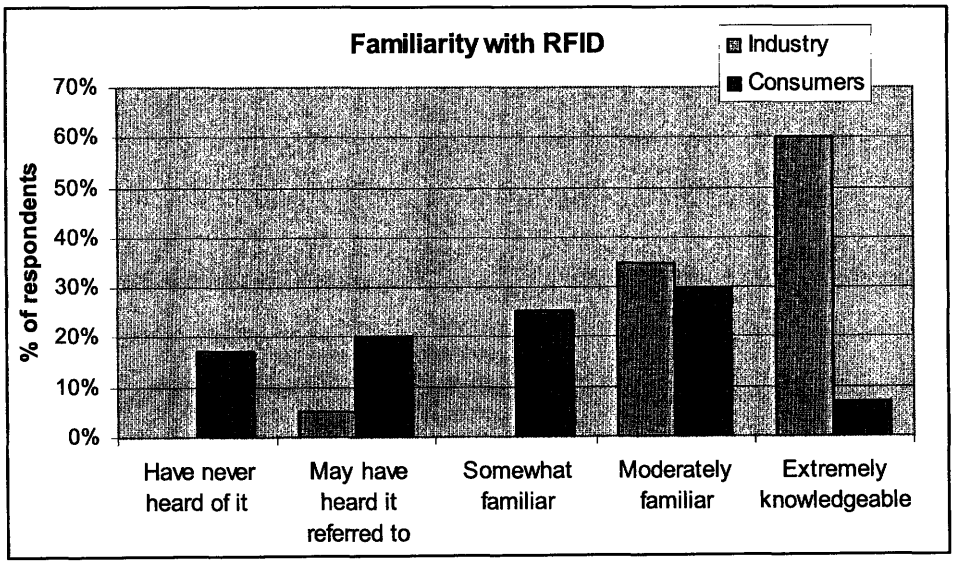

Figure 3: Survey respondents' familiarity with RFID.

Since the majority of respondents were familiar with RFID at the time of the survey, the analysis was able to gauge an accurate perception of their feelings about RFID. Figure 4 shows the distribution of responses as to perception of RFID for both consumers and industry members. Most consumers felt either neutral about the technology or had a somewhat favorable view. The industry members, however, held an overwhelmingly favorable view of RFID, though there were a few negative responses as well.

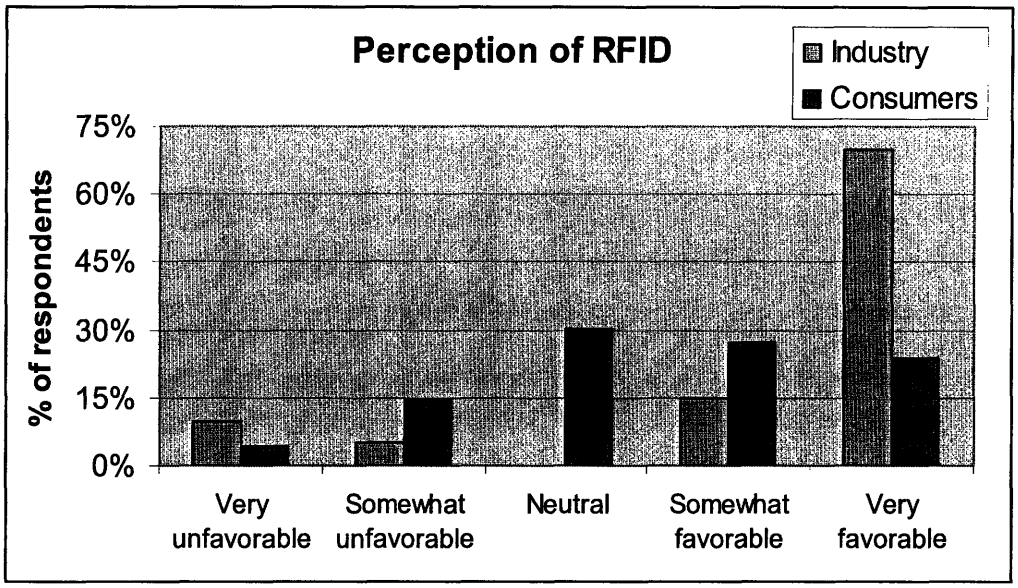

Figure 4: Consumer and industry perception of RFID.

Using the data from Figures 3 and 4, the analysis was able to determine if there was a pattern between knowledge and perception of RFID. Specifically, the data was used to see if those more knowledgeable were more likely to have a positive or negative outlook on the technology. Figure 5 shows the five categories of consumer respondents according to their knowledge of RFID, shown in the chart legend. These five divisions are plotted by the percentage of each group that holds a certain perception of RFID. The chart shows that the majority of those consumers who had never heard of RFID or may have heard of it, about 55%, had a neutral perception of RFID. This outcome is expected, since those respondents were not informed about the positive or negative aspects of the technology. Those who were somewhat familiar with RFID were more likely to hold a somewhat favorable view of RFID. Finally, those who were moderately familiar with or extremely knowledgeable about RFID were most likely to hold an extremely favorable view of the technology. Essentially, the data reveals that the more familiar a consumer is with RFID, the more likely he or she is to hold a favorable perception of it.

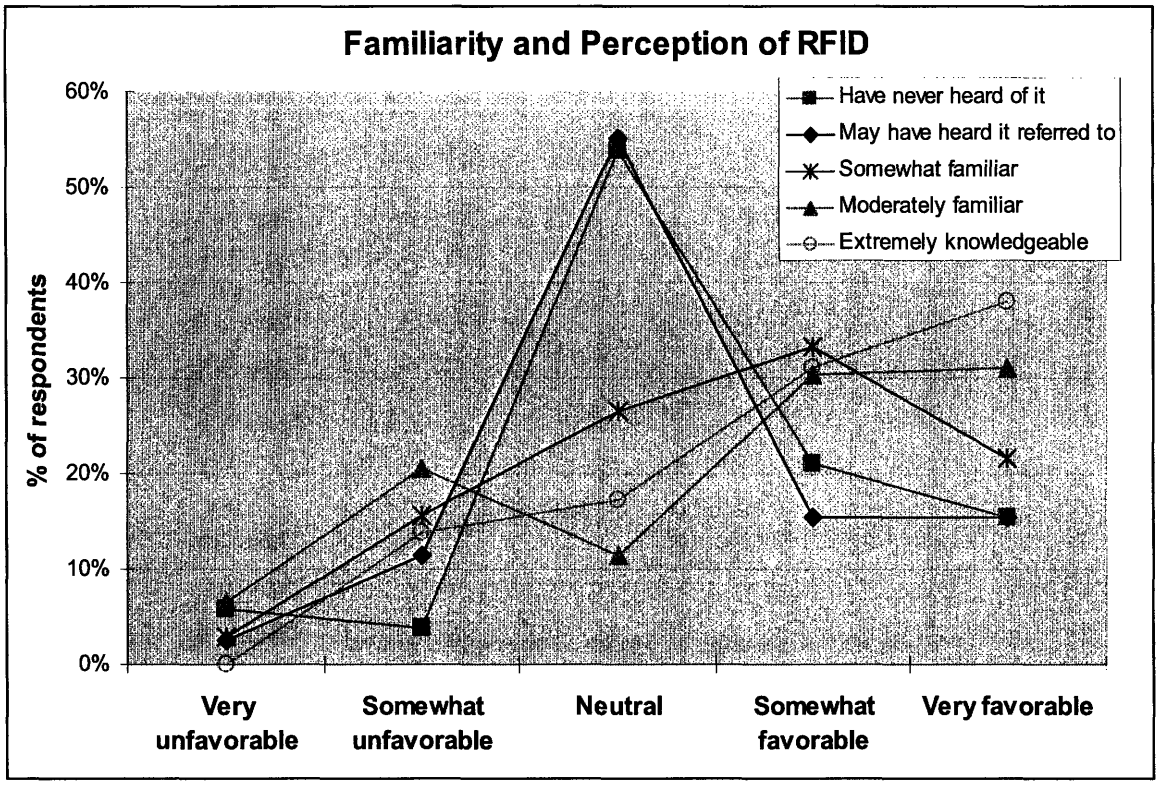

Figure 5: Consumer familiarity and perception of RFID.

Since the majority of the industry survey respondents, 95%, were moderately or extremely familiar with RFID, and 85% had a somewhat or very favorable view of it, the industry data seems to support the correlation between more knowledge and a more favorable perception of the technology. This conclusion will be discussed further, as it points to the solution of educating the public about RFID in order to gain more positive feedback and acceptance of the technology.

The industry survey omitted the RFID primer that was in the consumer survey, since it was expected that industry members be familiar with RFID beforehand. However, in the consumer survey, participants were asked about their perception of RFID before and after the primer to see if their view had changed. The survey wanted to ascertain directly if becoming more knowledgeable about RFID gave consumers a more positive, more negative, or the same view of the technology.

As Figure 6 shows, most respondents, regardless of their initial knowledge about RFID, held the same view of it before and after the primer. However, about 23% to 30% of those who were

familiar with RFID at the start of the survey reported to have gained a more positive view after reading the primer. It is possible that those who started off less educated about RFID learned less from the primer than did those who began with a greater understanding. Therefore, the primer had more of an impact on those who knew more about the technology. While a few respondents reported to feel more negatively about RFID after the primer, this was only a small minority of the respondents for each of the groups. In general, Figures 5 and 6 reveal that more knowledge about RFID is correlated to a more positive view of the technology.

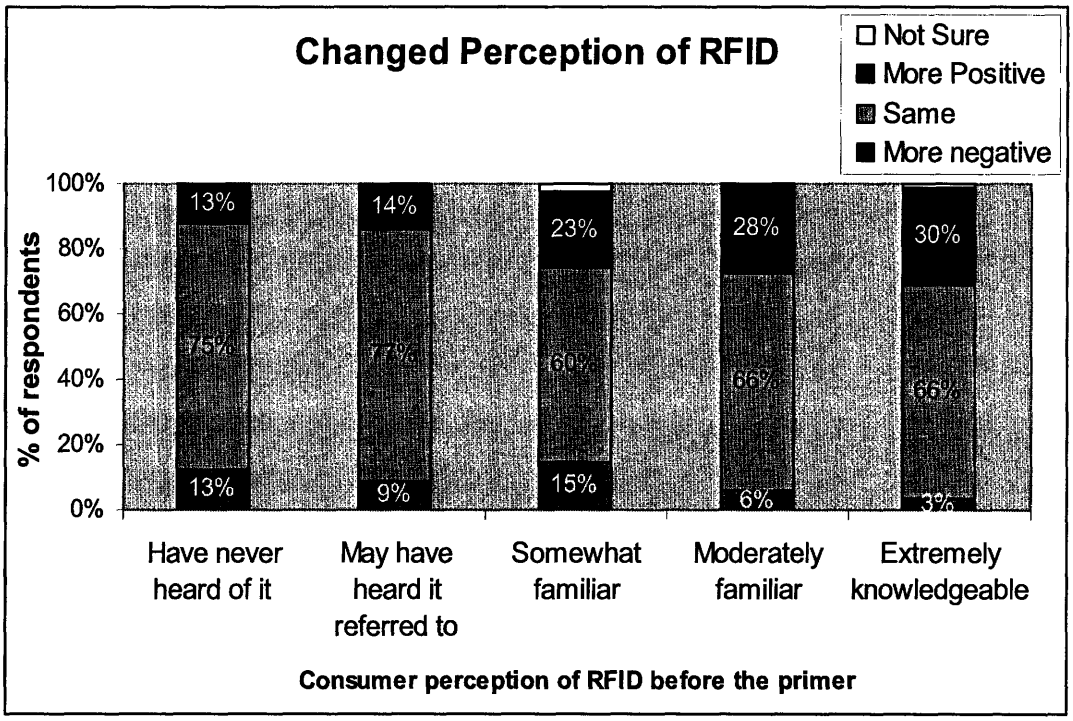

Figure 6: Changed perception of RFID before and after the RFID primer.

RFID Applications and Concerns

The second part of the survey dealt with how respondents valued certain applications of RFID or had concerns about RFID. Consumers were asked about their personal view while industry members were asked about how they value certain applications for their company or have concerns for their company. For the question concerning applications, participants were given ten possible applications of RFID, both retail and not, and asked to rate each on a scale from 1 to 5 from *not important* to *very important*. The number of responses were counted for each rating

and the average score was found. Figure 7 below shows the average score for each application for both consumers and industry, ordered by consumer preferences.

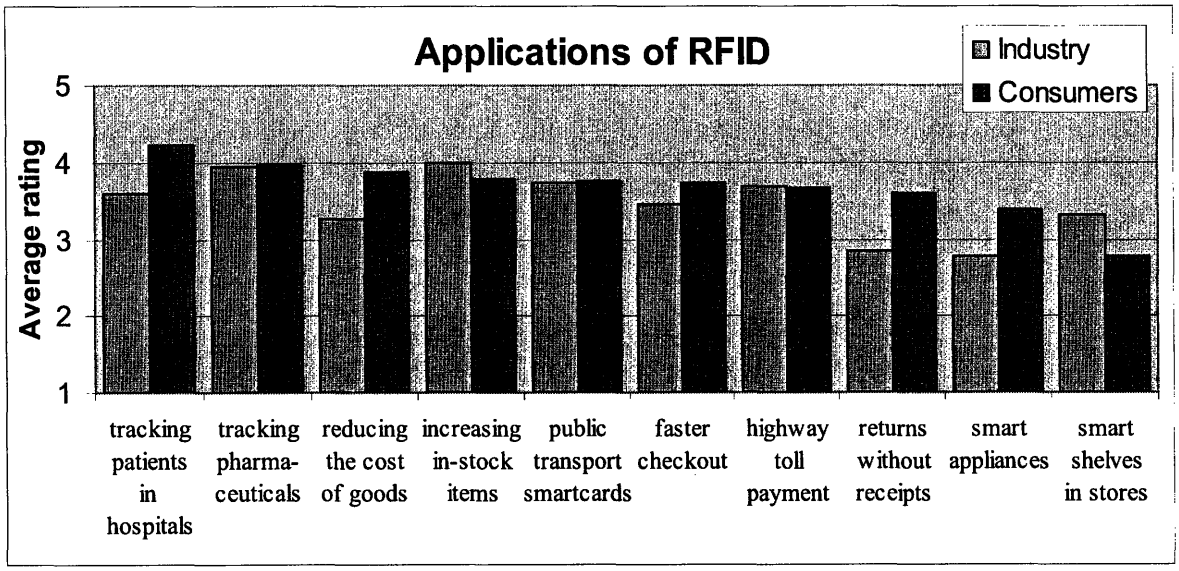

Figure 7: Average rating of each RFID application.

The chart indicates that consumers and those in the industry have different views about which RFID applications are most important. While ensuring items are in-stock is the most important application according to industry members, it ranks only fourth for consumers. This discrepancy may be due to the fact that businesses stand to gain sales from reducing out of stock items, while consumers will only gain convenience.

Both parties acknowledge the importance of tracking pharmaceuticals to reduce counterfeit drugs, though this rating may be inflated because of the recent reporting and political discussions of counterfeit drugs. Another interesting difference between consumers and industry members is how they view the importance of lowering the cost of consumer goods. While consumers obviously find this an enticing possibility of RFID, businesses may not be gaining anything from reducing the price of goods, and therefore do not rate it highly. Alternatively, they may find the cost of RFID prohibitive to reducing the cost of goods, and therefore, do not find it a likely outcome of using RFID in business operations.

The same averaging method was used to compare the concerns about RFID. Consumers and industry members were surveyed about six possible negative implications of the technology, listed in Figure 8 below.

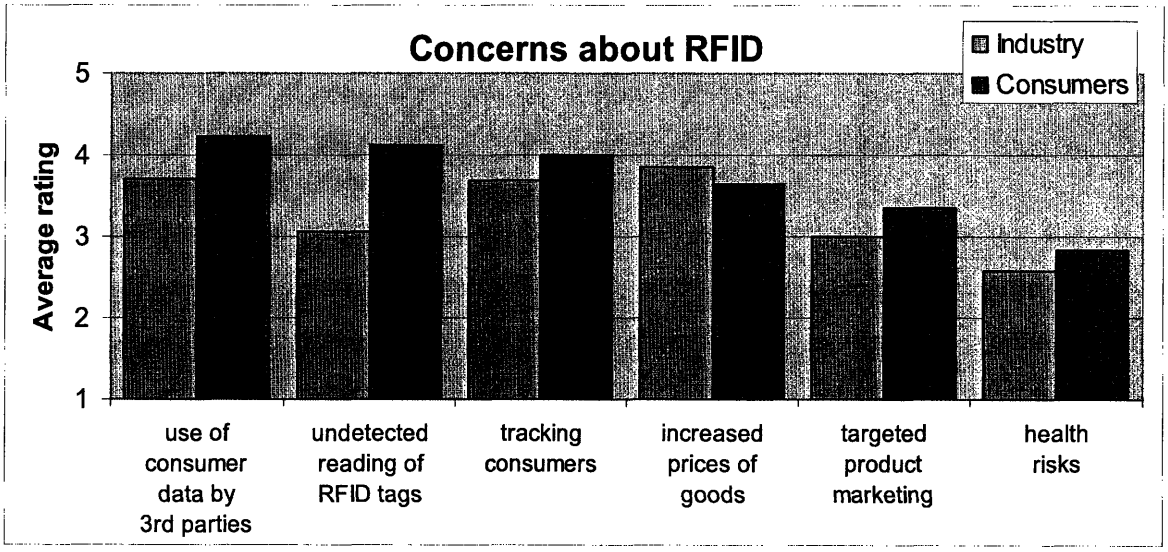

Figure 8: Average rating of concerns about RFID.

For this survey question, consumers were asked how concerned they were about these risks of RFID and industry participants were asked how concerned they were about these risks being damaging to consumer perception of their company. Industry members' top concern is increased prices of retail goods, which may hurt their business. Consumers, however, only rank this fourth among their relative concerns. Consumers are more worried about third party use of consumer data, undetected tag reading, and tracking. As described in Chapter 4, tracking is an unlikely application, though both third party use of data and undetected reading of tags are possible under certain conditions. Neither party was concerned about targeted product marketing or possible health risks. Targeted marketing is probably less of a concern than other worries since it is already happening in retail stores. As far as health risks, they were not mentioned in the RFID primer, and consumers may not be worried about them because they are not educated about the risks.

Regardless of the rankings of the privacy threats, both consumers and industry respondents ranked each as a high concern. Participants were asked to rank the risks on a scale from 1 to 5, as 5 being *very concerned* about the applications. For the top five concerns in Figure 8, each had an average ranking of between 3 and 5, for both consumers and industry members. While they may disagree on the relative importance of the risks, both groups seem to be in consensus that all of the privacy threats from RFID pose a considerable concern to either their personal privacy or to their businesses.

Results from these two survey questions reveal that consumers and industry members place importance on different applications and concerns of RFID, though they both recognize he positive uses of the technology as well as the threats. While consumers anticipate RFID use for medical applications and reducing the cost of retail goods, industry members place importance on reducing out of stock items and increasing their sales. As far as the risks, industry members are most worried about RFID increasing prices of their goods and possibly damaging their profits, while consumers are more concerned about other negative implications of the technology such as third party data use and undetected tag reading. It may be difficult for consumers and businesses to agree on a proper method of regulating RFID unless their concerns are aligned, or, in the least, shared with the other party. Since both parties recognize the concerns, they should be able to collaborate on solutions.

Regulating Privacy

The final two survey questions dealt with how respondents would like to see privacy regulated. Though they may not be aware of all the positive and negative aspects of each type of regulation, the analysis was used to see which mode of regulation participants would prefer and which principles of information collection they would find the most important.

Figure 9 shows the eight options survey respondents were given for protecting privacy. They were asked to choose which options they found the most appealing and to limit their choices to one to three options. The chart illustrates the percentage of all respondents who chose that particular option. Both consumers' and industry members' top response was the choice to disable

the RFID tag at the checkout register. However, most respondents who chose the option to disable the tag also chose another method of regulation.

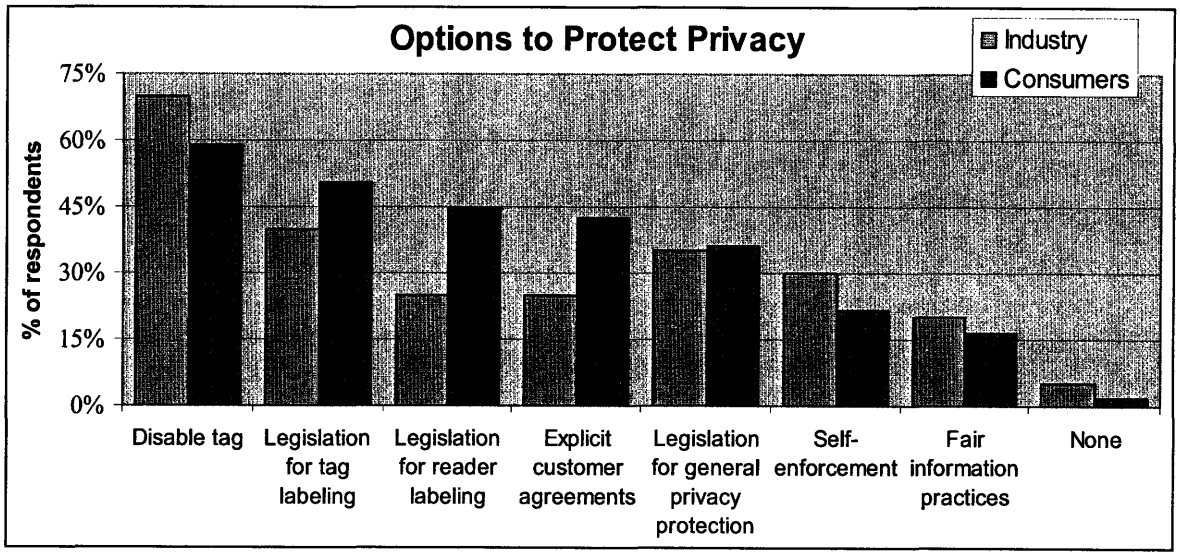

Figure 9: Percentage of respondents who support particular options to protect privacy.

The next most popular options for consumers involved legislation mandating tag or reader labeling. The more general privacy options, such as legislation of general privacy protection, self-enforcement by businesses, and the current practice of the FTC recommending fair information principles, were not ranked as highly. This may be due to the vagueness or broadness of these options as opposed to the specific requirement of tag or reader labeling. For the most part, industry's preferences were similar to those of consumers, though industry members elevated general legislation for privacy protection. Perhaps, the compliance costs of meeting such a regulation would be less than specific mandates such as consumer agreements or labeling the presence of readers.

The final survey question related to the fair information principles of data collection. Survey participants were asked to rate each of the nine principles, on a scale from 1 to 5, from *not important* to *very important*. Figure 10 displays the average rating given to each of the principles by consumers and industry members.

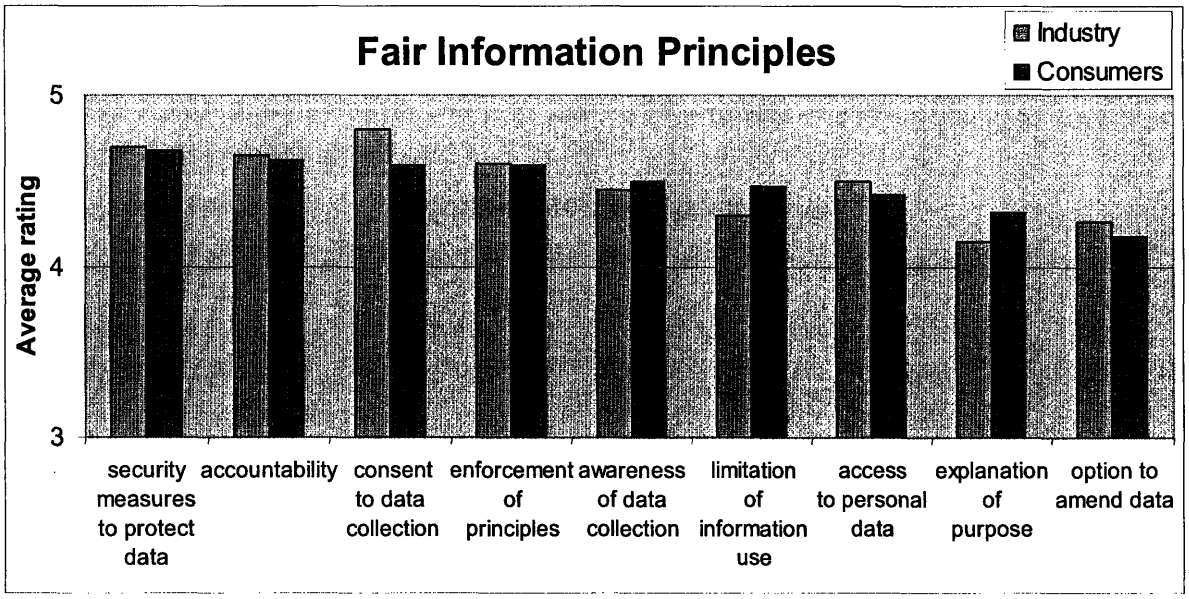

Figure 10: Average rating of importance of fair information principles.

While there are a few differences between the two groups of survey respondents, there is a general alignment on the principles. The three most important principles to each group are that of consent to data collection, security measures to protect data, and accountability of the information collecting entity to comply with the principles. Both groups put enforcement of principles and the awareness of data collection as fourth and fifth in importance, respectively. Sixth and seventh were the option to limit how the information is used and the ability to access the information that is collected. Finally, both groups thought the least important principles were explanation of the purpose of data collection and the option to amend the data that has been collected. Despite the difference in ratings between principles, overall, both groups of respondents had an average score of a 4 or 5 for each of the principles, confirming the importance of these principles to consumers and industry members alike.

These nine principles were taken from the U.S.'s fair information principles, as well as the Organisation for Economic Co-operation and Development's (OECD) data collection principles, devised in 1980, from which the others originated.[81] The U.S. fair information principles only include five from the above table: awareness, consent, access, security, and enforcement. The other four principles—accountability, use limitation, explanation of purpose, and option to

amend data are only present in the OECD principles. Accountability is assumed when there is strict enforcement, so it can be included in the enforcement principle. The other three, however, are not completely analogous to any of the five U.S. principles, though they are also among the least important to consumers. This suggests that the U.S. principles, as currently written, align with consumer and industry preferences concerning which principles are most important to enforce. Since both parties, however, acknowledged accountability as important, there may need to be a stricter method of enforcement instead of the FTC merely suggesting compliance with the principles.

CHAPTER 7: REGULATORY OPTIONS

There are three options for regulating privacy as affected by RFID use. These options are the market-based approach, self-regulation, and government regulation. Each of these approaches may be regarded as a different type of enforcement of the principles for information collection. First, this section includes an explanation of these principles, followed by a discussion of the three regulatory options, and concludes with an argument for the option which the survey data best substantiates.

Fair Information Practice Principles

The FTC advocates five fair information practice principles: notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. Each of these principles describes a guideline for entities accessing or obtaining personal information. Table 9 explains each principle and elaborates on its specific application to RFID.

The first principle pertains to giving consumers notice about an entity's information practices as well as information about the type of data being collection, the uses for the data, and any potential recipients of the data. The second principles, choice/consent, refers to giving consumers the choice whether to disclose personal information as well as consent to the different uses for the information. Correspondingly, consumers should be able to opt-in or opt-out from the collection of certain data or uses of the information. The third principle states that an individual should have the right to access information that has been collected about him or herself and check the information for accuracy and completeness. The fourth principles, security, states that the data that is kept should be secure and have reasonable measures to prevent unauthorized access of the data. Considering the potential for large amounts of data to be collected, technical measures should be used to prevent access in the transmission and storage of data. Finally, the fifth principle states that consumers should have a mechanism to enforce the first four principles. The method of enforcement can take the shape of any the different types of regulation, including both industry self-regulation and government regulation. Some form of redress, or remedy,

should be available to consumers to ensure that businesses comply with these principles. While the government could enforce civil penalties, if industry self-regulates, they must be sure to provide redress mechanisms to obtain the trust of consumers and to ensure compliance with the principles.

Principle	Explanation	Application to RFID
Notice/Awareness	Consumers should be given notice of an entity's information practices prior to the collection of personal information.	Consumers should be given notice of RFID tags placed on consumer products or of the presence of RFID readers in the vicinity.
Choice/Consent	Consumers should be given options as to how personal information collected from them may be used, including those uses beyond those necessary for the immediate transaction.	Consumers should be given the option not to purchase items with RFID tags or have the option to remove or disable tags at the time of purchase.
Access/Participation	Consumers should be given timely and inexpensive access to data about him or herself and the option to verify and update the data for accuracy and completeness.	Consumers should be given access to personal information collected via RFID and given the option to verify or amend the information.
Integrity/Security	Data collected from consumers should be accurate and secure.	Data collected with RFID should be held in a secure database.
Enforcement/Redress	There should be a mechanism in place to enforce the principles of privacy protection and a mechanism for redress.	There should be a mechanism for enforcement of the above principles, whether it is self- or government-enforced, which ensures compliance with the principles as applied to RFID use.

Table 9: Fair information practice principles and their application to RFID use.[82]

Applying these principles to RFID use is rather straightforward. Consumers should be given notice of the placement of RFID tags in or on products and should be aware if stores used RFID readers. If consumers are aware, then they can make the choice whether to shop at stores that use RFID or purchase products that contain RFID tags. Consumers should also be given the choice to

give their personal information to the store to be used in conjunction with information gathered with RFID. If data about a consumer is held by the store, consumers should have access to the data to verify its accuracy. The store should ensure that the private data is secure and not available publicly. Finally, a store should be responsible for enforcing these policies and action should be taken if a store is not in compliance.

Market approach

A market-based solution, though similar to self-regulation in that it does not involve legislation, is not identical to self-regulation. A market approach to regulating is really the absence of regulations, self- or legally-enforced. With a market approach, business incentive drives the enforcement of privacy protection; however, the only incentive for businesses to offer privacy protection is financial. The market approach is based on the assumption that consumers with privacy concerns would patronize stores with strong privacy policies, while consumers without privacy concerns would be able to frequent any store, including those without strong protections. A business would have incentive to offer privacy protection if it thought it would boost its public image and increase sales. The effectiveness of the market solution is determined by how much bargaining power consumers have. If more consumers are willing to make purchase decisions based on privacy protection, then they will have more power in the marketplace and companies will need to enforce protections to be more profitable. If few consumers are willing to make purchasing decisions based on privacy policies, however, then the businesses will not face as much pressure and will become ineffective at offering privacy protection.

Though some consumers may make decisions based on their privacy, more are sensitive to price differences and are therefore more likely to make decisions based on cost and not privacy. This can lead to a disparity between different groups of consumers. For example, many supermarkets now use customer savings cards. If consumers sign up for a card, disclosing their personal information, the supermarket will give them additional discounts on products when they use that card. If consumers feel uncomfortable giving their personal information, they can still shop at the grocery store without the cards; however, they will miss out on some of the discounts. Some shoppers may not be able to afford to give up these discounts in exchange for privacy protection.

To deal with this inequity between consumers, regulations may be needed to ensure all consumers receive equal treatment, regardless of their financial situation.

Though market solutions are generally thought to be the most efficient, some feel market failures, such as inequity, necessitate a regulatory solution. In addition to inequity, data collection can result in a market failure known as information asymmetry, when the company collecting information knows more about how data will be used and kept than the consumer.[83] In this situation, the customer will face costs in learning and understanding privacy policies or how their information is being used. In addition to learning about privacy policies, consumers will have to verify or trust that companies are complying with their own policy if there is no legal mechanism in place for enforcement. Consumers also have no power in bargaining for more privacy protection, since they are unlikely to band together to become forceful, and the costs of gaining bargaining power may outweigh the benefits. Companies also get the full benefit of using information they collect and of sharing or selling it to third parties, while they do not suffer the costs of privacy loss which consumers must entail. The information asymmetry creates an inequity between consumers and businesses and because of that, some observers believe that market forces alone may not be enough to protect consumers' privacy.

Self-regulation

Another regulatory option entails businesses developing their own regulations without government legislation. Self-regulation is often introduced with new technologies when businesses want to show consumers they are looking out for consumers' best interests. Self-regulation may also arise under the threat of legislation, when businesses choose to self-regulate to avoid the government doing it for them. EPCglobal, the organization responsible for developing and managing the Electronic Product Code, has developed a set of privacy policies they recommend for corporate members when using RFID.[84] Though these guidelines do advocate rights for consumers similar to the fair information principles, they are only suggestive, and therefore businesses are not required to follow these policies when using RFID.

Though self-regulation is not legally enforced, if offers benefits over government-mandated legislation. One benefit is that industry itself develops the rules, and they have the insight and knowledge about the technology and compliance costs. Industry may choose to self-regulate to avoid compliance costs with legislation. They may also do so to improve the reputation of the industry as a whole. Otherwise, one company could develop a privacy policy when the industry has not and have the advantage of differentiating itself and attracting consumers based on privacy protection.

At least one company is already taking the lead in self-regulation. Proctor & Gamble, a user of RFID in their supply chain, posts a public statement on their website regarding EPC use.[85] They state that they support certain principles for item-level EPC, including notice of when EPC is being used, the choice to disable or discard tags in products, and the choice as to whether personal information is linked to EPC numbers on products they purchase. Though several organizations have developed privacy policies similar to this one, with self-regulation it is difficult to ensure a complete regulatory system consisting of enforcement and adjudication with self-enforced rules if a company has violated those rules.

In 1999, the Georgetown Internet Privacy Policy Study[86] was undertaken to assess the privacy policy disclosures on various websites. The study was initiated by the private sector to report to the FTC whether self-regulation was effectively protecting consumer privacy on the internet. While posting privacy policies was, and still is, optional, most websites now post privacy policies giving consumers notice of their procedures. Of the 361 consumer-oriented websites chosen for the study, the researchers found that 67% had some type of policy disclosure, yet only 15% of those had a comprehensive privacy policy, defined as that which addressed notice, choice, access, and security of information.

When deciding whether to recommend to Congress to regulate privacy protection on the internet, the FTC looked to see if self-regulation was working. Since 67% of websites did have some type of privacy policy, industry argued that self-regulation was working. Consumer groups, however, argued that most websites were not effectively protecting privacy on their own and that there was a need for more meaningful, comprehensive privacy protection. The author noted that based on

this study, it was evident that "a full self-regulatory regime has not emerged." Since websites are not required to post any disclosures, and the FTC has no basis for acting under current authority to protect fair information principles, a comprehensive scheme may not emerge without the impetus of legislation.

Though this study was performed in 1999 and only assessed internet privacy practices, it is useful to compare internet privacy practices to the current situation with RFID. While a certain percentage of companies may elect to post and adhere to privacy practices, they are not required to, and it may take some time before many businesses adopt these privacy policies. With RFID, however, consumers may not have the option of opting out of certain practices as they do with giving out personal information online, so it is even more important to ensure privacy with the prospect of pervasive RFID use.

Government Regulation

Government-mandated regulation, whether federal or state, can have the effect of prohibiting certain types of activity or protecting certain rights. Government action consists of three distinct parts: legislation, referring to the process of rule-making; enforcement, referring to the initiation of an enforcement action if rules are broken; and adjudication, referring to the process of determining if a party has violated the rules. When considering the development of laws pertaining to RFID, lawmakers could choose to set standards for labeling, require mandatory labeling of RFID tags and/or readers, or limit the types of information obtained from RFID devices. Alternatively, instead of legislating RFID technology directly, lawmakers may choose to take a broader approach, developing and enforcing general information privacy guidelines, such as the fair information principles. Regardless of the type of legislation chosen, government-mandated regulation provides the strictest privacy protection since it gives consumers a legal recourse if their privacy rights are breached.

Though government action has the benefit of legally enforcing privacy principles, there are drawbacks to government action, as there are to the other regulatory options. As market failures can occur for market solutions, and self-regulation can be slow and incomplete, institutional

failures may inhibit government solutions. Legislation often entails a long, costly process, whereas market solutions and self-regulation can be less costly. The costs of law-making, including drafting, administering, and enforcing rules, falls on the government and taxpayers, while the industry is also likely to face compliance costs. The cost of compliance will vary based on the type of legislation and how greatly the industry needs to change its practices. The compliance costs will also depend on the degree of precision in the regulation.[87] If rules are broad, then the industry can choose the least costly path to compliance, while very strict rules may result in a higher compliance cost.

In addition to these institutional barriers, which occur when law-makers are acting in the best interest of all parties, government officials may sometimes not pursue the public good. Officials can be influenced by interest groups, representing either consumers or the industry, or may seek to pursue more selfish goals.

There are also costs to inhibiting use of RFID by businesses. Restricting information flow can generate indirect or direct costs for the consumer, as well as decrease the personalization of goods or services.[88] Each of those costs must be weighed against the benefits of ensuring privacy protection for consumers and creating equity in the marketplace.

Costs and Benefits of Regulatory Options

Table 10 summarizes the costs and benefits of the three regulatory options identified. Benefits of a certain type of regulation are denoted as (+), costs, or drawbacks, of certain regulations are denoted as (-), and factors that can either be positive, negative, or neutral, are denoted as (+/-). For each regulatory option, there are benefits and costs for both consumers and industry, as well as for society as a whole, which encompasses the costs and benefits of both interest groups. Since this thesis is interested in examining the optimal regulatory solution for all stakeholders, it will focus on the outcome of regulations for the combination of consumers and the industry, which is society as a whole.

	Market	Self-regulation	Government regulation
Consumers	(+) No tax payer money spent in law-making process (-) Inequity between consumers (-) Information asymmetry between consumers and businesses (-) Lack of accountability for privacy practices	(+) Little or no tax payer money spent in law-making process (-) Lack of legal accountability for privacy practices	(+) Legally-mandated privacy protection and enforcement (-) Tax payer money spent on law-making
Industry	(+) No compliance costs (+) Bargaining power over consumers (-) Lack of basic standards for privacy regulation may hurt public image	(+) Positive public image (+) Influence in regulations (-) Low compliance costs	(+) Positive public image (-) Compliance costs (-) Restrictive laws may prohibit certain practices or uses
Society	(+) No cost of law-making or compliance with laws (+/-) Consumer response and acceptance of technology (-) Lax accountability or enforcement of privacy protection	(+) Low law-making and compliance costs (+/-) Consumer response and acceptance of technology (-) Non-comprehensive privacy protection	(+) Strong protection of privacy (-) Law-making and compliance costs (-) Possible restriction on technology use and/or growth

Table 10: Costs and benefits of various regulatory solutions.

With a pure market solution, there is no requirement that businesses comply with privacy principles, and therefore no enforcement of privacy protection. As discussed, this lack of protection could lead to information asymmetry between consumers and the industry, giving the industry more market power. In addition, since businesses have no restrictions on how they practice and choose to use RFID, they do not have to face compliance costs. Likewise, there are no costs to consumers or businesses from the law-making process. The only unknown factor is how consumers will react to unregulated RFID use. Some consumers may accept it as it becomes

the norm, while others may choose not to shop at stores that use RFID. An anti-RFID consumer movement could hurt the public image of businesses and reduce the cost benefits of RFID. If industries self-regulate, businesses' public image may improve, since consumers are often reassured by the use of privacy policies. Better public image and handling of the technology may improve consumer acceptance, and thus, eliminate any backlash from consumer groups which could occur. Self-regulation, if in response to the threat of government regulation, will entail some cost in the time law-makers spend on considering regulation, but still less than would be accrued with passing and enforcing legislation. Businesses may have to face a low compliance cost in establishing privacy policies, though if there are costs, they will be lower than those of complying with government regulation. Though the costs are lower, and there is some incentive for privacy protection, self-regulation will probably not result in as comprehensive a policy as some consumers would like to see. As evidenced by internet privacy policies, while many companies have established some set of principles for consumers or users, these policies are not standardized across all businesses and many companies do not meet all recommendations in the fair information principles.

Finally, government regulation, whether of broad privacy principles or specific mandates to RFID, is the strictest type of regulation because of the guaranteed mechanisms for accountability, enforcement, and redress of the law. Businesses have a strong incentive to comply with these regulations to avoid civil penalties. However, there is a high cost to government regulation. This expense is made up of the cost to the legislative branch in developing these regulations, the cost of administration required to enforce the regulations, and any costs for adjudication in upholding these regulations. Companies may also face high compliance costs in meeting these government-mandated regulations. Despite the costs, government action may still be the best option if strict privacy protection is necessary to ensure businesses have the incentive to respect a consumer's privacy.

Recommended Regulatory Solution

Both consumers and industry members expressed a strong concern for various privacy threats. Survey analysis confirmed that most respondents were somewhat concerned about RFID use for

targeted product marketing, tracking, undetected reading of RFID tags, and third party use of data. Furthermore, when asked about fair information principles, both consumers and industry participants agreed in the importance of all five principles of notice, consent, access, accountability, and security, citing consent, accountability, and data security as the most important. There is a legitimate privacy threat from item-level RFID use, and while many respondents cited a neutral or positive perception of RFID, they maintained concerns about the technology.

The leading solution to privacy threats cited by survey respondents was the option to disable the RFID tag. 70% of industry respondents and 59% of consumers supported the choice to disable the RFID tag at the checkout register. While physically disabling the tag necessitates a technical solution, a regulatory option is necessary to enforce this policy. If there is not currently a sufficient technological solution for disabling the tag, consumers should be given another option which would sufficiently address their concerns. Giving consumers the choice to purchase a product with or without an RFID tag embedded in the product would also let those consumers who are not comfortable with the technology effectively opt-out of using it. Though it would be costly for businesses to manufacture and sell two types of products, those with and without tags, this option could be used to oblige businesses to affix tags to the outside of products instead of embedding them in products until there is a reliable mechanism for disabling embedded tags. Giving consumers either this opt-out choice or the possibility to remove or disable the RFID tag would meet the concerns of most survey participants.

Since a majority of both consumers and industry members focused on the option to disable tags, there is a high level of importance in meeting this concern with strict enforcement of privacy. Though government regulation involves costs to both consumers and businesses, their desire for privacy protection seems to outweigh these costs. For the specific purpose of disabling or removing RFID tags which are embedded in consumer products, government regulation should be considered as the most favorable solution to meeting these privacy concerns. If disabling tags is not possible, then businesses should give consumers either the option to purchase products that do not use RFID or purchase products that only contain RFID tags on their packaging and can be discarded. Since the use of RFID tags in consumer items is still rare, this policy does not have to

be enacted immediately, but rather in the next few years as RFID use grows. In developing the policy, both consumer groups and industry representatives should discuss with law-makers the best approach for enabling and enforcing this policy. Since disabling tags also involves a technological solution, RFID tag manufacturers should be involved in facilitating this innovation as well. Based on the strong desire for the option for tag removal, and the strictness of government regulation in protecting privacy, the survey data favors a legislative solution in requiring businesses to offer options to consumers of tag removal, disabling, or opting-out from purchase altogether. As stated by one of the respondents from the business survey, "A person's right to privacy should always be held at the highest level."

Despite the recommendation of a legislative option for enforcing the option to disable or remove RFID tags, other privacy concerns, while strong, were not as fervently pushed by consumers and industry representatives. Other concerns such as third party data use and targeted marketing could remain a threat to consumer privacy despite the ability to disable tags. Most survey participants responded that fair information principles were important to them, and that these principles should therefore be part of every privacy policy of a company using item-level RFID in its retail business. Since item-level tagging is not widely used yet, and implementation may not be widespread until the cost of tags drops, enforcing these principles is not an immediate concern, though it will be as RFID use grows. A policy of self-regulation should be used by businesses planning to use RFID to reassure consumers that they are abiding by the fair information principles. These businesses should develop a common privacy policy for self-regulating RFID use that encompasses all five of the fair information practice principles. An industry-led policy would entice more businesses to follow suit and give an incentive to the industry as a whole to strengthen its public image to consumers. Since the industry is best informed about the costs of implementation of such a policy, compliance costs are likely to be lower than if the policy is mandated by law-makers. Additionally, this lower cost of compliance ensures that businesses are still able to reap the efficiency benefits of using RFID, which means consumer goods prices are less likely to rise because of RFID use and may drop as efficiencies get passed on. While self-regulation does not promise strict accountability for all privacy principles, the current advances by EPCglobal and some individual businesses in establishing their own privacy policies suggests that more businesses will follow suit.

Though consumer support for self-regulation may not be as strong as for government regulation, this solution gives businesses the freedom to operate and establish their own policies while keeping the cost of RFID implementation down. Businesses should try to build awareness of their privacy principles as well as educate consumers about RFID use to get the most positive response. While RFID use in the retail sector is still in its infancy, it is highly likely to grow in the next five to ten years. After RFID acceptance becomes more widespread, the policy of self-regulation should be re-examined to ensure it is still providing consumers with adequate privacy protection. If law-makers find that consumer privacy is a strong concern even with self-regulation, they may want to consider legislative options to give incentive to businesses to strengthen their self-regulatory actions.

CHAPTER 8: CONCLUSIONS AND RECOMMENDATIONS

Conclusions

RFID can be positively accepted by consumers if privacy concerns are addressed first, before the technology has become ubiquitous. Previous technologies which have succeeded, including Caller ID and cell phones, have thrived partly because there was a clearly visible consumer benefit along with the profit for businesses.[89] Furthermore, consumers had the option to opt-out of using those technologies so they didn't feel forced into using them. These elements eased likely public fear and made introduction of the technology smoother. Businesses considering RFID can take these findings into account by giving consumers the option of whether to purchase RFID-tagged goods at first and educating consumers about RFID and the benefits available to them. Consumers may accept the risk of RFID if they feel it is worth the benefit. EZ-Pass toll collection and ExxonMobil Speedpass have avoided consumer backlash even though they both use RFID technology because they provide a direct benefit to users. Other applications of RFID may improve the overall shopping experience or enhance convenience, and these should be publicized to try to increase user acceptance of new RFID applications.

Furthermore, the U.S. government can take some preliminary action to regulate RFID use. A government must be seen implementing technologies to encourage use if it is to gain and keep the trust of its citizens. By enacting legislation to give consumers the option to disable or remove RFID tags from products, or to opt out of buying these products in the first place, consumers are likely to feel more at ease with the technology. This strict protection will reassure consumers that their privacy rights are not being breached and may be achieved at a low cost. To further assure consumers, businesses should consider enacting privacy principles that incorporate the guidelines of the FTC's fair information principles. A comprehensive privacy policy can maintain consumer privacy for those who are concerned without creating a high cost for businesses.

While this thesis tried to account for most consumer concerns, there are others which may be recognized in the future as RFID becomes more ubiquitous. Furthermore, other applications of RFID outside of the retail sector may be better suited to different policy options from those recommended in this thesis. For each of those, a similar analysis could be performed recognizing the desire for privacy protection as well as the benefits of using the technology. Government action may be necessary to address privacy threats, but should not impede the growth and usage of the technology if it provides adequate compensation benefits to society.

Recommendations

The following recommendations for the government, retail industry, and consumers provide guidance for ensuring a positive acceptance of RFID while acknowledging the privacy rights of consumers. These recommendations are based on the analysis in this thesis and take into account the opinions of both consumers and industry members surveyed. RFID is a promising technology and should be implemented with the utmost care. Following these recommendations is a first step in ensuring the growth and acceptance of the technology.

Recommendation 1: Educate consumers about RFID before widespread use of the technology to build trust in the industry.

Consumer survey data shows that those participants who are more familiar with RFID are also more likely to have a favorable perception of RFID. Those who are not as familiar with the technology are more likely to hold a neutral perception of the technology. Furthermore, the survey showed that about 15% to 30% of survey participants gained a more positive view of RFID after learning about the technology in the primer included in the survey. This significant correlation between knowledge and perception is rationale for educating consumers about RFID. Consumers who are more educated about both benefits of the technology as well as privacy threats are more likely to hold a positive perception of the technology than those who are less familiar with it. Members of the retail industry and other industries which plan on using RFID should educate consumers about their proposed use of the technology to encourage a positive perception of it.

Recommendation 2: Facilitate a discussion between consumers and industry representatives to share concerns and ideas about the technology.

Participants in the survey agreed that privacy threats posed by RFID were a concern to them. Both consumers and industry members acknowledged they were somewhat or very concerned about several possible uses, including targeted product marketing, third party use, tracking, surreptitious detection of tags, and increased prices of consumer goods. Consumers acknowledged they were concerned about these risks to their personal privacy, while businesses acknowledged that they worried about those uses of RFID as being damaging to consumer perception of their company.

Despite the consensus, businesses and consumers differed on their top concerns. Consumers identified use of the data by third parties and surreptitious tag reading as their top concern, while businesses identified increased prices of goods as theirs. A discussion between consumer groups and industry representatives could be facilitated to share mutual concerns about the technology. While businesses may worry about prices, they may also want to address concerns such as targeted product marketing if that is what consumers care about more. Consumers will be more accepting of the technology if their concerns are acknowledged by businesses, and businesses may be able to use RFID freely for certain applications if they know consumers are not as concerned about those particular uses.

Recommendation 3: Give consumers the option to disable or remove an RFID tag from a product after purchase.

70% of industry respondents and 59% of consumers advocated for the choice to disable the RFID tag at the checkout register. If the tag is on the product packaging, then consumers can simply remove and throw away the packaging. However, if the tag is actually embedded in the product, then there will need to be a method for either temporarily or permanently disabling it.

If there is not a sufficient technological solution for disabling the tag, consumers should be given another option which would sufficiently address their concerns. Businesses could give shoppers the choice whether to purchase a product with the tag embedded in it or not, instead of giving them the option to remove or disable tags. Those consumers who are not as concerned about the

technology may not care about the presence of RFID, however, those consumers with legitimate concerns about RFID must be given notice about products with RFID tags embedded in them so that they can choose to purchase the item or a similar item without the tag. Either the choice to purchase the item or the choice to disable the tag would meet the concerns of most of the consumers and industry members surveyed.

Recommendation 4: Encourage businesses to self-regulate their use of RFID by developing and enforcing comprehensive privacy policies.

The five fair information principles of notice, consent, access, security, and enforcement were of high importance to most survey participants. Businesses and industry leads can work together in creating comprehensive privacy policies which encompass these five principles. This industry-led policy would give businesses leeway in developing and enforcing their own policies, while still providing consumers the assurance that their privacy rights will not be breached. As RFID use grows in the next five to ten years, this policy of self-regulation can be re-examined later by the FTC, consumer groups, and industry members to analyze if the policy is working and, if necessary, be adapted later to meet the needs of consumers and businesses.

APPENDIX 1: SURVEY QUESTIONS

RFID Survey

For my research at the Massachusetts Institute of Technology, I am conducting a survey to better understand the public's current knowledge and concerns about Radio Frequency Identification (RFID). I welcome your participation, regardless of your current understanding of RFID or its applications. The survey is 10 questions long and should take you about 5 to 10 minutes to complete. The questions are designed to garner your individual knowledge about this topic, so I ask you to complete this survey on your own, and without the aid of additional resources.

This survey is entirely voluntary. You may answer as few or as many questions as you would like. Care will be taken to ensure confidentiality of the responses. I will be happy to provide anonymous results to those who indicate such on the last page.

I appreciate your cooperation. If you wish further clarification please provide me with your feedback at the end of the survey. This survey also appears on the web, at http://web.mit.edu/~deanna/www/rfid/start.htm.

Name: _____

Organization: _____

Position: _____

Age: Under 18 18-25 26-35 26-45 46-55 56-65 Over 65

Gender: Male Female

Highest Level of Education Completed: Some High School High School Graduate
Associate's Degree Bachelor's Degree Some Graduate Work Graduate Degree

1. Do you regularly use any of the following? (Select all that apply)

- ☐ Customer loyalty cards (CVS card, Shaws card, etc.)
- ☐ EZ-pass or other highway toll payment system
- ☐ ExxonMobil Speedpass
- ☐ Smartcard for public transportation (e.g. CharlieCard, SmarTrip)

2. Radio Frequency Identification (RFID) is a technology used to automatically identify objects. RFID readers use electromagnetic waves to power computer chips in RFID tags, which then send back their data to the reader using an internal antenna.

How familiar are you with RFID technology?

- ☐ Have never heard of it
- ☐ May have heard it referred to
- ☐ Somewhat familiar
- ☐ Moderately familiar
- ☐ Extremely knowledgeable

3. What is you main source of information about RFID? (Select all that apply)

- ☐ None
- ☐ TV
- ☐ Radio
- ☐ Newspaper
- ☐ Online newspaper/journal
- ☐ Educational setting
- ☐ Friends
- ☐ Colleagues
- ☐ Work setting
- ☐ Other:

4. What is your current perception of or feeling about RFID?

- ☐ Very unfavorable
- ☐ Somewhat unfavorable
- ☐ Neutral
- ☐ Somewhat favorable
- ☐ Very favorable
- ☐ Don't Know

A Quick Overview

In case you are unfamiliar with RFID, please read the information below before continuing with the questionnaire. When you are done, use the button at the bottom of the page to continue on with the rest of the survey.

What is RFID?
Radio Frequency Identification (RFID) is a method for automatically identifying tagged objects. RFID tags can be affixed to almost any object and store a unique identification code for the object. The information embedded in the tag is communicated to a reader using electromagnetic waves. When RFID readers are hooked up to computers, data from the tags can be read into an information system.

RFID is an improvement over barcodes because unlike UPC symbols, RFID allows for the capture of data without line of sight from the tag to reader, eliminating the need for manual scanning. RFID also allows for the reading of hundreds of tags simultaneously, whereas UPC symbols can only be read one at a time. The Electronic Product Code (EPC), which is currently being used in conjunction with RFID tags for retail applications, can store more information than the Universal Product Code (UPC), which means more objects can be uniquely identified.

Active and Passive Tags
There are two types of RFID tags: active and passive. Passive tags, which are smaller and cheaper than active tags, have no internal power source. They are powered by incoming radio waves transmitted by the reader, which are then reflected back and detected by the reader. Typical passive tags range in size between a postage stamp and a credit card, and can cost between 5 and 40 cents depending on the size and manufacturer.
Active RFID tags have an internal power source used to generate an outgoing signal. Active tags are more reliable than passive and can transmit at higher power levels, in more challenging environments and over longer distances. The downside of active tags is that their need for batteries gives them a finite shelf life and can be more costly than passive tags. RFID devices used to collect electronic highway tolls make use of active tags.

RFID Applications
RFID tags can be used for a wide range of applications. In retail supply chains, RFID tags are being used to track pallets, cases, and items from the warehouse to the distribution center, and then to the retail store. Using RFID tags instead of barcodes or other identification methods allows retailers and manufacturers to achieve efficiencies in the supply chain, including automating receiving and shipping processes, reducing inventory levels, and increasing the chance an item will be in-stock on the retail shelf. RFID can also automate the checkout process, shortening the time consumers will have to wait in line. Since RFID can cut costs for both the manufacturer and retailer, there are potential spillover effects for the consumer, resulting in lower prices.

Active RFID tags are currently being used in highway toll systems to automatically transmit data from the RFID tag. ExxonMobil Speedpass also makes use of RFID to allow for automatic payment. There are several other uses of RFID projected for the future. Some of these include:

- Tagging patients, staff, and equipment in hospitals to reduce costs and increase patient safety by reducing medical errors
- Tracking and tracing pharmaceuticals to prevent counterfeit drugs
- Using Smartcards for automatic payment (e.g. public transportation)
- Tagging library books
- "Smart" home appliances, such as medicine cabinets or washing machines

Implications of RFID

While there are many promising benefits of RFID, there are also some concerns about RFID security and privacy. Though RFID is not currently a pervasive technology, decreasing tag prices are likely to drive a wider adoption of RFID. With an increase of tagged items and RFID readers, tagged items can be read in and out of stores. Since the current range to read an RFID tag is about 10 to 20 feet, the chance of an unauthorized person reading a tagged item in your home is small, though read ranges may become larger in the future with improved technology.

Though the tag itself will only store a number, that number will be linked to product information in an online database. Stores may choose to link purchased goods to personal information about an individual for marketing purposes. There is the possibility of use of this information by the retailer for more targeted consumer marketing, or perhaps, abuse of the information by 3rd parties.

For example, tagged items in grocery stores can be used to identify shopping habits by keeping a record of consumer purchases, similar to a customer loyalty card. RFID readers on store shelves can track removal of products, identifying whether that item is placed back on the shelf, purchased at the register, or taken out of the store without payment. Since RFID tags used for retail applications are likely to be passive, they are not reliant on batteries, and information can be read whenever an acceptable reader is placed close enough to the tag. If tags are still activated after leaving a store, information from the tag can be read by others using an acceptable reader (of the proper frequency).

5. Given the information you just read, how has your perception of RFID changed?

☐ More negative
☐ Same
☐ More positive
☐ Don't know

6. How valuable do you consider these current or future application of RFID?
Please rank each application from 1 to 5, with 1 being *not important* and 5 being *very important.*

· Faster checkout in retail stores	1	2	3	4	5
· Returns at retail stores without receipts	1	2	3	4	5
· Reducing the cost of retail goods	1	2	3	4	5
· Increasing the chance retail items will be in stock when you look for them	1	2	3	4	5
· "Smart" shelves in grocery stores which present relevant advertisements and special offers when items are removed	1	2	3	4	5
· Tracking patients in hospitals to reduce medical errors	1	2	3	4	5
· Tracking pharmaceuticals to reduce counterfeit drugs	1	2	3	4	5
· Automated highway toll payment	1	2	3	4	5
· Smartcards for subways or other public transportation	1	2	3	4	5
· "Smart" home appliances (e.g. medicine cabinet to remind patients to take medication)	1	2	3	4	5
· Other: _____	1	2	3	4	5

7. How concerned are you about the following RFID applications?
Please rank each from 1 to 5, with 1 being *not concerned* and 5 being *very concerned.*

· Targeted product marketing by retailers	1	2	3	4	5
· Use of consumer data by 3rd parties	1	2	3	4	5
· Tracking of consumers using product purchase information	1	2	3	4	5
· Undetected reading of RFID tags from a distance	1	2	3	4	5
· Increased prices on retail goods	1	2	3	4	5
· Health risks from electromagnetic waves	1	2	3	4	5
· Other: _____	1	2	3	4	5

8. What options to protect your individual privacy do you find the most appealing? (Limit your selection to 1 to 3 choices)

- ☐ The choice to disable the RFID tag at the checkout register
- ☐ Self-enforcement of consumer privacy by companies (e.g. company privacy policies)
- ☐ Explicit customer agreements concerning the collection of personal information
- ☐ Legislation requiring labels on products to identify the presence of an RFID tag
- ☐ Legislation requiring labels to identify the presence of an RFID reader
- ☐ Legislation banning the use of personal information by 3rd parties
- ☐ Status Quo: Fair Information Practice Principles enforced by the Federal Trade Commission (FTC)
- ☐ Other: _____
- ☐ None

9. When giving out your personal information to a person/entity, which principles would you like to see enforced, and how important are they to you?
Please rank each from 1 to 5, with 1 being *not important* and 5 being *very important.*

· Awareness when a person/entity collects information	1	2	3	4	5
· Explanation of the purpose of data collection	1	2	3	4	5
· Consent to personal information being collected	1	2	3	4	5
· Option to limiting how the information can be used	1	2	3	4	5
· Access to your personal data which is being collected	1	2	3	4	5
· Option to amend the collected data for accuracy and/or completeness	1	2	3	4	5
· Reasonable security measures taken to protect the data	1	2	3	4	5
· Accountability of the person/entity to comply with the above principles	1	2	3	4	5
· Enforcement of the above principles with the opportunity for redress/compensation of wrongdoing	1	2	3	4	5

REFERENCES

[1] Landt, J. "Shrouds of Time: The History of RFID." The Association for Automatic Identification and Data Capture Technologies, Oct. 1, 2001. http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf (accessed July 10, 2007).

[2] Albrecht, K. and L. McIntyre. *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move.* New York: Plume, 2005.

[3] Albrecht, 2005.

[4] Thiesse, F. "RFID, Privacy and the Perception of Risk: A Strategic Framework." *Journal of Strategic Information Systems*, 2007.

[5] "Boycott Gillette." Consumers Against Supermarket Privacy Invasion and Numbering. http://www.boycottgillette.com (accessed July 10, 2007).

[6] Albrecht, 2005.

[7] Identity Information Protection Act of 2007, U.S. SB 30, CA, 2007. http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_30&sess=CUR&house=B&site=sen (accessed July 10, 2007).

[8] U.S. Senator Patrick Leahy. Remarks at the conference on "Video Surveillance: Legal and Technological Challenges." Georgetown University Law Center, Mar. 23, 2004. http://leahy.senate.gov/press/200403/032304.html (accessed July 10, 2007).

[9] "RFID: The State of Radio Frequency Identification, Implementation and Policy Implications." IEEE, Nov. 21, 2005.

[10] Leong, K. et al. "EPC Network Architecture." Auto-ID Labs White Paper Series, Sept. 2005. http://autoid.mit.edu/whitepapers/AUTOIDLABS-WP-SWNET-012.pdf (accessed July 11, 2007).

[11] Brock, D. "The Electronic Product Code." Auto-ID Center Which Paper, Jan. 1, 2001. http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-002.PDF (accessed July 7, 2007).

[12] Brock, 2001.

[13] Laubacher, R. et al. "What is RFID Worth to Your Company? Measuring Performance at the Activity Level." MIT Sloan Research Paper No. 4601-06, Mar. 2006.

[14] Laubacher, 2006.

[15] Rothfeder, J. "What's Wrong with RFID?" *PC Magazine*, Aug. 1, 2004.

[16] "RFID: Uncovering the Value." Metro AG, 2004. http://www.rfidc.com/pdfs_downloads/rfid_value.pdf (accessed July 11, 2007).

[17] Quimby, J. and R. Laubacher. "Technology-Process Value Mapping: Use of a Web-based Knowledge Management Tool to Assess the Impact of RFID." Presentation given at the MIT Center for Digital Business, April 4, 2007.

[18] Alexander, K. et al. "Applying Auto-ID to Reduce Losses Associated with Shrink." IBM Business Consulting and Auto-ID Center, Nov. 1, 2002. http://autoid.mit.edu/whitepapers/IBM-AUTOID-BC-003.PDF (accessed July 13, 2007).

[19] Alexander, Nov. 2002.

[20] Laubacher, 2006.

[21] Chappell, G. et al. "Auto-ID on Demand: The Value of Auto-ID Technology in Consumer Packaged Goods Demand Planning." Accenture and Auto-ID Center, Nov. 1, 2002. http://autoid.mit.edu/whitepapers/ACN-AUTOID-BC-002.PDF (accessed July 13, 2007).

[22] Alexander, K. et al. "Applying Auto-ID to Reduce Losses Associated with Product Obsolescence." IBM Business Consulting and Auto-ID Center, Nov. 1, 2002. http://autoid.mit.edu/whitepapers/IBM-AUTOID-BC-004.PDF (accessed July 13, 2007).

[23] Corsten, D. and T. Gruen. "Desperately seeking shelf availability: an examination of the extent, the causes, and the efforts to address retail out-of-stocks." *International Journal of Retail & Distribution Management*, Vol. 31, Iss. 12, 2003.

[24] Hardgrave, B. et al. "Does RFID Reduce Out of Stocks? A Preliminary Analysis." Information Technology Research Institute, University of Arkansas, Nov. 2005.

[25] Chappell, G. et al. "Auto-ID in the Box: The Value of Auto-ID Technology in Retail Stores." Accenture and Auto-ID Center, Feb. 1, 2003. http://www.autoidlabs.org/uploads/media/ACN-AUTOID-BC006.pdf (accessed July 10, 2007).

[26] Alexander, K. et al. "Focus on Retail: Applying Auto-ID to Improve Product Availability at the Retail Shelf." IBM Business Consulting and Auto-ID Center, Jun 1, 2002. http://autoid.mit.edu/whitepapers/IBM-AUTOID-BC-001.PDF (accessed July 10, 2007).

[27] Garg, V. et al. "17 Billion Reasons to Say Thanks: The 25th Anniversary of the U.P.C. and It's Impact on the Grocery Industry." PriceWaterhouseCoopers, Mar. 1999.

[28] Metro Group Future Store Initiative. "Test Areas." 2007. http://www.future-store.org/servlet/PB/menu/1007134_l2_yno/index.html (accessed July 11, 2007).

[29] Roussos, G. "Building Consumer Trust in Pervasive Retail." International Workshop, Information Sharing and Privacy, Tokyo, 2004. http://www.slrc.kyushu-u.ac.jp/rfid-workshop/roussos-paper.pdf (accessed Apr. 18, 2007).

[30] Metro Group Future Store Initiative, 2007.

[31] Metro Group Future Store Initiative, 2007.

[32] "Privacy." Legal Information Institute, Cornell University Law School. http://www.law.cornell.edu/wex/index.php/Privacy (accessed July 11, 2007).

[33] The United Nations. "Universal Declaration of Human Rights." *General Assembly Resolution*, 217 A(III), Dec. 10, 1948. http://www.un.org/Overview/rights.html (accessed July 11, 2007).

[34] U.S. Code Title 5 Section 552a. Legal Information Institute, Cornell University Law School. http://uscode.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html (accessed July 11, 2007).

[35] U.S. Code Title 15 Section 6801-6809. Legal Information Institute, Cornell University Law School. http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_94_20_I.html (accessed July 11, 2007).

[36] U.S. Code Title 15 Section 1681. Legal Information Institute, Cornell University Law School. http://www.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_41_20_III.html (accessed July 11, 2007).

[37] U.S. Code Title 15 Section 6501-6506. Legal Information Institute, Cornell University Law School. http://uscode.law.cornell.edu/uscode/html/uscode15/usc_sup_01_15_10_91.html (accessed July 11, 2007).

[38] U.S. Code Title 15 Section 45. Legal Information Institute, Cornell University Law School. http://uscode.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000045----000-.html (accessed July 11, 2007).

[39] "Privacy Legislation." Office of the Privacy Commissioner of Canada, Dec. 2000. http://www.privcom.gc.ca/legislation/02_06_07_e.asp (accessed July 11, 2007).

[40] European Council Data Protection Directive 95/46/EC, Oct. 24, 1995. Center for Democracy and Technology, 1995. http://www.cdt.org/privacy/eudirective/E.U._Directive_.html (accessed July 11, 2007).

[41] "Working document on data protection issues related to RFID technology." European Council, Jan. 19, 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf (accessed July 11, 2007).

[42] Smith, H.J. "Information Privacy and Marketing: What the US should (and shouldn't) learn from Europe." *California Management Review*, Vol. 43, Iss. 2, 2001.

[43] Federal Trade Commission. "Radio Frequency Identification: Applications and Implications for Consumers." 2005. http://www.ftc.gov/bcp/workshops/rfid/ (accessed July 11, 2007).

[44] U.S. H.R. No. 4673, 108th Congress 2nd Session.

[45] Scassa, T. et al. "An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies." Office of the Privacy Commissioner of Canada, Apr. 28, 2005. http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf (accessed July 11, 2007).

[46] U.S. SB 128, 2005 and SB 13 2007, Mo.; U.S. HB 314 and HB 251, 2004, Utah; U.S. AB 264, 2005, NV; U.S. SB 699, 2005, TN.

[47] U.S. SB 181, 2005, and SB 159, 2007, MA.

[48] U.S. HB 215, 2005, NM.

[49] U.S. HB 1136, 2005, SD.

[50] U.S. HB 5929, 2005, RI.

[51] U.S. HB 2953, 2005 and HB 1925, 2007, TX.

[52] U.S. SB 30, 2007, CA.

[53] U.S. SB 30, 2007, CA.

[54] U.S. HB 203-FN, NH, 2006.

[55] EPCglobal. "Guidelines on EPC for Consumer Products." Sept. 2005. http://www.epcglobalinc.org/public/ppsc_guide/ (accessed July 11, 2007).

[56] Electronic Frontier Foundation. "Position Statement on the use of RFID on Consumer Products." Nov. 14, 2003. http://www.eff.org/Privacy/Surveillance/RFID/rfid_position_statement.php (accessed July 11, 2007).

[57] Consumers Against Supermarket Privacy Invasion and Numbering. "RFID Right to Know Act of 2003." http://www.nocards.org/rfid/rfidbill.shtml (accessed July 11, 2007).

[58] Westin, A. *Privacy and Freedom.* New York: Atheneum, 1967.

[59] "Dilemmas of Privacy and Surveillance." The Royal Academy of Engineering, Mar. 2007. http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf (accessed July 12, 2007).

[60] Warren, S. and L. Brandeis. "The Right to Privacy." *Harvard Law Review*, pp. 193-220, 1890.

[61] Federal Trade Commission, "Fair Information Practice Principles." http://www.ftc.gov/reports/privacy3/fairinfo.htm (accessed March 29, 2007).

[62] Minority Report Script. http://www.script-o-rama.com/movie_scripts/m/minority-report-script-transcript-spielberg.html (accessed July 11, 2007).

[63] "Department of State Begins Issuing Electronic Passports to the Public." Office of the Spokesman, U.S. Department of State, Aug. 14, 2006. http://www.state.gov/r/pa/prs/ps/2006/70433.htm (accessed July 12, 2007).

[64] U.S. Department of State, 2006.

[65] Lyman, J. "Hacker Cracks, Clones RFID Passport." TechNewsWorld, Aug. 7, 2006. http://www.technewsworld.com/story/52270.html (accessed July 12, 2007).

[66] "Mandatory Student ID Cards Contain RFIDs." Electronic Frontier Foundation, Feb. 7, 2005. http://www.eff.org/news/archives/2005_02.php#002371 (accessed July 12, 2007).

[67] Zetter, K. "School RFID Plan Gets an F." *Wired*, Feb. 10, 2005. http://www.wired.com/politics/security/news/2005/02/66554 (accessed July 12, 2007).

[68] "Automated Vehicle Identification." Houston TransStar. http://www.houstontranstar.org/about_transtar/docs/2003_fact_sheet_2.pdf (accessed July 12, 2007).

[69] "FAQ." FasTrak, 2006. http://www.bayareafastrak.org/static/about/faq_using.shtml#8 (accessed July 12, 2007).

[70] Albrecht, 2005.

[71] Brito, J. "Relax, Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature." http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf (accessed Mar. 28, 2007).

[72] Kumar, R. "Interaction of RFID Technology and Public Policy." Wipro Technologies, 2003. http://www.rfidprivacy.us/2003/papers/kumar-interaction.pdf (accessed Mar. 23, 2007).

[73] Juels, A. "RFID Privacy: A Technical Primer for the Non-Technical Reader." RSA Laboratories, draft Feb. 23, 2005. http://www.astalavista.com/media/directory06/uploads/098e8eb7a860bbb913f0cb835354d13b.pdf (accessed Mar. 29, 2007).

[74] Juels, 2005.

[75] Juels, 2005.

[76] Claburn, T. "RFID-Privacy Law Debated." *InformationWeek*, Feb. 3, 2004. http://www.thomasclaburn.com/2004/02/rfidprivacy_law_debated.html (accessed June 17, 2007).

[77] Duce, H. "Public Policy: Understanding Public Opinion." Auto-ID Centre, Feb. 1, 2003. http://www.autoidlabs.org/uploads/media/CAM-AUTOID-EB002.pdf (accessed Mar. 27, 2007).

[78] Cap Gemini Ernst & Young. "RFID and Consumers: Understanding Their Mindset." Jan. 13, 2004. http://www.us.capgemini.com/DownloadLibrary/requestfile.asp?ID=400 (accessed Mar. 26, 2007).

[79] Duce, 2003 and Cap Gemini, 2004.

[80] See DeGroot, M. and Schervish, M. *Probability and Statistics.* Boston: Addison Wesley, 2002, Chapter 8 for more information on the t-test.

[81] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." OECD, Directorate for Science, Technology and Industry, Sept. 23, 1980. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed July 18, 2007).

[82] FTC, "Fair Information Practice Principles."

[83] Swire, P. "Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information." Privacy and Self-Regulation in the Information Age, U.S. Dept of Commerce, 1997. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472#PaperDownload, (accessed June 19, 2007).

[84] "Guidelines on EPC for Consumer Products." EPCglobal, Sept. 2005. http://www.epcglobalinc.org/public/ppsc_guide/ (accessed July 13, 2007).

[85] "P&G Position on Electronic Product Coding (EPC)." Proctor & Gamble, 2007. http://www.pg.com/company/our_commitment/privacy_epc/epc_position.jhtml (accessed July 13, 2007).

[86] Culnan, M. "Protecting Privacy Online: Is Self-Regulation Working?" *Journal of Public Policy & Marketing*, Vol. 19, Iss. 1, Spring 2000.

[87] Swire, 1997.

[88] Walker, K. "The Costs of Privacy." *Harvard Journal of Law & Public Policy*, Sept. 22, 2001.

[89] Cantwell, B. "Why Technical Breakthroughs Fail: A History of Public Concern with Emerging Technologies." Auto-ID Center, Nov. 1, 2002. http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-016.PDF (accessed July 13, 2007).