8-2006

Personal Privacy Protection within Pervasive RFID Environments

Eeva Kaarina Hedefine

PERSONAL PRIVACY PROTECTION WITHIN PERVASIVE RFID ENVIRONMENTS

By

Eeva Kaarina Hedefine

A.S., Legal Technology, University of Maine - Augusta, 1998

B.S. University of Maine - Orono, 2002

A THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

(in Spatial Information Science and Engineering)

The Graduate School

The University of Maine

August, 2006

Advisory Committee:

Harlan J. Onsrud, Professor of Spatial Information Science and Engineering, Advisor

M. Kate Beard-Tisdale, Professor of Spatial Information Science and Engineering

Peggy Agouris, Associate Professor of Spatial Information Science and Engineering

LIBRARY RIGHTS STATEMENT

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at The University of Maine, I agree that the Library shall make it freely available for inspection. I further agree that permission for "fair use" copying of this thesis for scholarly purposes may be granted by the Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature: Erica K. Hedgpeth

Date: 8/21/06

PERSONAL PRIVACY PROTECTION WITHIN PERVASIVE RFID ENVIRONMENTS

By Eeva Kaarina Hedefine

Thesis Advisor: Dr. Harlan J. Onsrud

An Abstract of the Thesis Presented
in Partial Fulfillment of the Requirements for the
Degree of Master of Science
(in Spatial Information Science and Engineering)
August, 2006

Recent advancements in location tracking technologies have increased the threat to an individual's personal privacy. Radio frequency identification (RFID) technology allows for the identification and potentially continuous tracking of an object or individual, without obtaining the individual's consent or even awareness that the tracking is taking place. Although many positive applications for RFID technology exist, for example in the commercial sector and law enforcement, the potential for abuse in the collection and use of personal information through this technology also exists. Location data linked to other types of personal information allows not only the detection of past spatial travel and activity patterns, but also inferences regarding past and future behavior and preferences. Legislative and technological solutions to deal with the increased privacy threat raised by this and similar tracking technologies have been proposed. Such approaches in isolation have significant limitations. This thesis hypothesizes that an approach may be developed with high potential for sufficiently protecting individual

privacy in the use of RFID technologies while also strongly supporting marketplace uses of such tags. The research develops and investigates the limits of approaches that might be used to protect privacy in pervasive RFID surveillance environments. The conclusion is ultimately reached that an approach facilitating individual control over the linking of unique RFID tag ID numbers to personal identity implemented though a combination of legal controls and technological capabilities would be a highly desirable option in balancing the interests of both the commercial sector and the information privacy interests of individuals. The specific model developed is responsive to the core ethical principle of autonomy of the individual and as such is also intended to be more responsive to the needs of individual consumers. The technological approach proposed integrated with enabling privacy legislation and private contract law to enable interactive alteration of privacy preferences should result in marketplace solutions acceptable to both potential commercial users and those being tracked.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

This chapter introduces the problem of privacy loss and provides motivation for privacy protection in the use of location tracking technologies within RFID environments. It states the goal of the research, which is to provide an alternative approach to privacy protection that better comports with foundational ethical principles, and provides an outline of the remaining thesis chapters.

1.1 Motivation

Technology is creeping into every aspect of our lives. There is a feeling that we are losing control over our personal space, which was formerly considered private. Surveillance technologies are watching and recording our every move – ATM machines, traffic light cameras, security cameras at the office, mall, health club, supermarket, parking garage, hotel, apartment building, street-scapes in business districts and many other locations as we move through the day. Advancing technology lowers our expectation of privacy and therefore as new technology is introduced we are less shocked or surprised by its capabilities. Individuals are slowly becoming immune or desensitized to privacy loss.

Radio frequency identification (RFID) technologies are likely to raise the surveillance level to a new high, with the capability to reach into homes or other personal spaces to share details of private activities. Comprehensive records of an individual's movements could be generated through capture of the globally unique ID numbers from

RFID tags embedded in consumer goods worn by, carried by, or in close vicinity to the individual throughout the day. The exploding RFID market will likely lead to the embedding of RFID tags into most consumer goods (e.g., clothing, electronics, food packaging and automobile parts), and implementation has already begun. RFID readers are capable of capturing massive amounts of data from RFID tags, and with the soaring demand for consumer data by private corporations, and the desire to access that data by government entities for purposes such as national security, threats to personal privacy continue to rise. In addition, RFID technology can be combined with other technologies such as surveillance cameras, creating a potentially pervasive surveillance network that enables personal identification and continuous tracking. This in turn could result in enhanced detection of spatial and temporal patterns linked to specific individuals.

Linking tag ID numbers to an individual at the point of sale will facilitate the capture of personally identifiable data by readers dispersed throughout the individual's daily environment. Announcements regarding implementation of this technology by government agencies and corporations such as Wal-Mart have led to growing controversy and fear of personal tracking. Proposals to limit collection of tag data include an outright ban on the technology or disabling RFID tags at the point of sale. However, many recognize the multitude of beneficial applications offered by RFID technology to consumers and businesses alike. This has led to recommendations of various methods to ameliorate privacy protection, while promoting the utilization of RFID technology. Researchers have explored both technological and legislative approaches to privacy protection, but neither approach alone appears to provide a realistic or practical solution. Technological approaches many times are germane only to certain applications areas and

may not be appropriate for others. The slow legislative process often does not keep pace with rapid technological advancements, and therefore legislation may already be outdated as it reaches adoption, while attempting passage of any type of privacy law may be a challenge in itself. In addition, U.S. privacy legislation is often reactionary, created in response to a specific privacy threat or violation, and applied on an ad hoc basis. Further, when laws are passed they typically are applied in a one-size-fits-all approach. Since technological and legislative approaches applied separately are limited in their success, a solution incorporating both approaches may prove more effectual (Taipale 2004) and may be more efficient in responding to the privacy and service needs of each user.

Although some RFID systems may have security measures blocking access to tag data by unauthorized readers, currently many do not, and the assumption is that this will hold true for the future as well. For item level tagging to be achieved, the cost of tags would need to drop into the five to ten cent range. Currently, cheap tags do not possess much computational capability, and cannot support many proposed security measures. Therefore, at least initially, RFID may be a fairly open system, so that anyone with a reader will be able to access data from most RFID-tagged consumer products, absent security measures. Further, tags that can be universally read regardless of where or from whom the item was purchased or borrowed will be of greatest utility to consumers and thus to a mature marketplace.

1.2 Research Goal and Hypothesis

The goal of this thesis is to develop and describe a model that protects personal privacy by facilitating individual control over personal information collection and use within RFID observation environments, while affording substantial support to marketplace uses of RFID technology. To accomplish this goal, specific questions need to be addressed, including the following:

- What is the minimum standard of privacy protection that would prove acceptable to the general populace and how could technology be used to enforce that level of protection?
- How might purchasers of RFID-tagged items be afforded control over the amount and nature of personal or location information that may be obtained through the recording and tracking of their tags by RFID readers?
- How could unauthorized linking of RFID tag data to individual identities be prevented?
- Since a multitude of consumer RFID applications are envisioned for the future, how might privacy be enabled in a way that permits continued tag usability after the purchase of RFID-tagged goods?
- How might consumer privacy protection be facilitated, while at the same time not hindering the growth of useful RFID applications and the RFID market?

The hypothesis of this thesis is as follows:

> *A combined legal and technological approach may be developed with high potential for sufficiently protecting individual privacy in the use of RFID technologies while also strongly supporting marketplace uses of such tags.*

1.3 Scope of Thesis and Methods Employed

This thesis explores various legal and technological approaches to privacy protection within pervasive RFID environments. It presents a conceptual model that attempts to balance personal information privacy and marketplace needs and analyzes

issues that are likely to arise during the design and implementation phases. This thesis does not include an actual implementation of the model since such would require legislative and institutional actions, as well as technological development.

Research began with an examination of past and current proposals for technological and legislative solutions to personal information and location privacy protection, in order to determine whether any of these proposals could be applied in a RFID environment. Proposals for RFID-specific legislation, guidelines and technology to protect privacy were then considered. So as to gain a global perspective, rather than merely a United States perspective on privacy and RFID technology, minimum legal standards and RFID technology deployment in various countries were considered. After investigation of other proposed solutions and reflection on the questions outlined in section 1.2, the results were incorporated into a design that appears to provide consumers with an acceptable level of privacy enabling individual choice and that supports marketplace applications and growth.

Since it is impossible to know for certain how RFID technology will develop and what future RFID environments will be like, it is necessary to make some assumptions in these regards. This research assumes that:

- Passive RFID tags (i.e. lacking their own power source) will be embedded in most, if not all, consumer products or packaging;
- RFID readers will be dispersed throughout the daily environment;
- Linking of RFID tag data to individual identity will be possible;
- RFID systems will be interoperable, functioning under common standards, so that a tag could be tracked continuously, even from one country to another; and

- RFID technology will continue to be a fairly open system, so that any RFID reader can access data from most passive RFID tags.

1.4 Thesis Outline

The remainder of this thesis is organized in the following manner: Chapter 2 defines privacy and discusses general privacy principles and issues, and then focuses on issues relating to location-based privacy. This chapter covers past and current approaches to personal information privacy protection, both in the legal and technological aspects, as well as the key differences between U.S. and European approaches to privacy and privacy protection. Chapter 3 introduces RFID technology – the components of an RFID system, the operation of an RFID system, and current user applications for RFID technology. Additionally, Chapter 3 examines future predicted and conceivable applications of RFID. Chapter 4 outlines privacy issues arising from the use of RFID technology and discusses what makes RFID-related privacy issues different from those of other technologies. Specific privacy concerns raised through current uses of RFID technology and potential future applications are also addressed in Chapter 4. Chapter 5 specifically focuses on proposed or attempted legal and technological approaches to protecting location privacy. The benefits and shortcomings of the alternatives are analyzed. This chapter also discusses why a combined approach incorporating into its design a contractual relationship between data collectors and data subjects, along with technology to enforce the agreed upon contract, may offer the best solution. Chapter 6 presents a model that allows consumers to "opt-out" of the linking of tags in purchased items to other personally identifiable information through registration on a centralized list, supported by privacy legislation. An individual's ability to "opt-in" at specific times

enabled through private contract law is also discussed, along with the technology required to implement the model. Legal and technological issues arising from the implementation of this model are also addressed. Lastly, Chapter 7 provides a summary and conclusions of the research conducted. A final section in Chapter 7 suggests areas for future work.

Chapter 2

PRIVACY

Before the modern technological era of surveillance cameras and the constant recording of an individual's transactions, communications and movements, events witnessed or statements overheard many times remained only as long as the memory of the individuals involved. Now with the advent of email, communications can be sent instantaneously and recorded indefinitely. An item posted on a website is available for the whole world to see and may be archived long into the future. Video clips can be played over and over again. The lives of even average people are now subject to constant scrutiny. The future promises even more scrutiny, as it is estimated that "by 2023 large organizations will be able to devote the equivalent of a contemporary PC to monitoring every single one of the 330 million people who will then be living in the United States (Farmer and Mann 2003)." With the potential for advances of this caliber in surveillance technology and other technologies that allows the extraction and analyzing of personal data, developing methods of protecting privacy becomes not only urgent, but paramount as well.

2.1 Privacy: Principles and Issues

Privacy is a difficult concept to define, with views on privacy varying greatly. Some view the loss of privacy and public anonymity as a potential form of social control and that "if current trends in technology development continue, then everyone in the country soon might find themselves back in the equivalent of a small town," where

everyone is constantly aware of everyone else's actions (Morgan and Newton 2004). Others maintain we are more likely to see a "big brother" or "panopticon" information environment where the many are observed in great detail by a corporate and law enforcement elite. In order to feel secure there must be protections from potential physical or monetary threats and criminal activities. To provide that security, the argument is made that law enforcement must collect information on its citizens, which in turn threatens the privacy of those citizens (Solove and Rotenberg 2003). Although total privacy or anonymity is not possible in today's world, a balance between these and other "legitimate social objectives" is important, with legal oversight provided (Morgan and Newton 2004). Regardless of the many viewpoints held on the degree of privacy or surveillance that should be allowed, prior to an individual's decision to relinquish some degree of privacy, there is a need to understand the potential consequences of that decision.

2.1.1 Privacy as a Right

Although privacy as a concept may differ from one country to another, people generally hold privacy as a right. Europeans tend to look at privacy as a basic human right and a matter of human dignity, enacting legislation setting minimum standards to protect the privacy of individuals. The United States holds privacy as a right under the Fourth Amendment of the U.S. Constitution. While the plain language of the Fourth Amendment restricts only government invasions of privacy, "unreasonable searches and seizures" without "probable cause," this constitutional right has been expanded by the courts over time in the context of other constitutional language (Onsrud et al. 1994). By

example, the constitutional right of privacy also prevents intrusions by private individuals or corporations, "...into one's private activities, in such a manner as to cause mental suffering, shame or humiliation to a person of ordinary sensibilities" (Shorter v. Retail Credit Co.). When determining whether the Fourth Amendment applies to a particular situation, consideration is given to the 'reasonable expectation of privacy test' articulated by Justice Harlan (Katz v. United States 1967). Both requirements of the test must be satisfied for application – 1) that an individual "exhibited an actual (subjective) expectation of privacy" and that 2) "the expectation be one that society is prepared to recognize as 'reasonable' (Solove and Rotenberg 2003)." Rosen (2004) suggests this test is of a circular nature, in that, "people's subjective expectations of privacy reflect the privacy they subjectively experience, and as electronic surveillance in public became more intrusive and more pervasive, it lowered people's objective expectation of privacy as well, with a corresponding diminution of constitutional protections."

Warren and Brandeis (1890) argued for the establishment of privacy as a general right to be defended in the courts, defining privacy as "the right to be let alone." Others have defined privacy "as a right of personhood, intimacy, secrecy, limited access to the self, and control over information (Solove and Rotenberg 2003)." Philosophers such as Kant have argued that a major aspect of personhood is the ability of an individual to be "autonomous" or "self-determining (Spinello 2003)." Unless individuals have the ability to control the amount and type of personal information being collected, stored and released, they cannot be considered autonomous. A person has autonomy in shaping his own life when he is able to make informed decisions based on his own preferences and desires rather than being forced to choose from within the confines of explicit or implied

parameters, constructed by others who define what is considered acceptable behavior. The ability to readily determine what information is being collected, when this is occurring, how it is being accomplished, and for what purpose, is a prerequisite for each individual in making informed decisions relating to the control and flow of their personal information.

2.1.2 Differing Perspectives

Views on privacy, whether in the U.S. or other countries, vary between or even within groups - whether governmental, business, or private citizen - as these entities have differing opinions on the value of or need for privacy. For instance, a U.S. business that wants to obtain records of an individual's buying habits for marketing purposes does not have much incentive to protect that individual's personal information except to the extent that its own privacy practices harm its potential market. If the business can better target a consumer's needs and desires, their profit potentially increases. The government trying to protect its citizens from threats of terrorism may feel the need and right to collect personal information. A citizen, however, if given a choice in the matter, may be reluctant to provide personal information for any of these purposes, concerned about future uses of the information that has been collected. The initial purpose for collection may be agreeable to the citizen, such as transaction data recorded at the time of a credit card purchase. However, once that information is stored within a database and merged with other data, the potential exists for additional unintended uses. The now defunct Total Information Awareness (TIA) data mining program would have allowed the federal government to collect, merge, and analyze vast amounts of personal data on citizens of

the United States. Another recently terminated (ACLU 2005) database surveillance program, the Multistate Anti-Terrorism Information eXchange (MATRIX), had been operating in a number of states with funding and oversight by the Department of Homeland Security. This program created profiles through data merged from government and private databases, allowing law enforcement searches for terrorist activities or other crimes (ACLU 2003). These government data mining activities to search through all citizens' personal information "run the risk of becoming the 21st-century equivalent of general searches, which the authors of the Bill of Rights were so concerned to protect against (Kumagai and Cherry 2004)."

The problem, according to Sobel of the Electronic Privacy Information Center, is that "once information exists, it's virtually impossible to limit its use." (Kumagai and Cherry 2004) The amount of personal information available is huge as illustrated by ChoicePoint, one current private data warehouse that contains more than 10 billion records gathered by marketers, credit card bureaus, and private detectives (Rosen 2004). In a recent visible case, tens of thousands of individuals in California had their credit information transferred by ChoicePoint to illicit companies. Until recently, California was the only state to require companies like ChoicePoint to divulge when they know such activities have occurred. Further, the accuracy of large customer databases has been called into question; with one estimate claiming 20-35 percent of records in many of those large databases contain one or more major errors or omissions (Farmer and Mann 2003).

2.1.3 Assessing the Risks and Benefits

Schilit et al. (2003) describe privacy as "a malleable concept based on societal perceptions of risk and benefit." Immediately following 9/11, perceptions of risk from potential terrorist acts increased immensely and therefore individuals were more willing to exchange some of their privacy for a perception of greater security. This was attested to by passage of the USA PATRIOT Act a mere six weeks after the attacks of 9/11, following little debate or revision within the House or Senate (EPIC 2004d). In the post 9/11 world, "citizens also face increasing pressure to expose personal information, in order to prove that they have nothing to hide (Rosen 2004)."

In order to weigh the risks and benefits associated with a given situation or a technology being employed, one must understand the issues involved. In a study conducted by Beckwith and Lederer (Beckwith 2003) at an eldercare facility supporting a "sensor-rich environment," residents, their family members, and the staff and managers were interviewed and observed to determine their views and perceptions of the sensor technology in their surrounding environment. Sensor technology included in the study were motion detectors, load cells on beds, sensors to determine if doors were open or closed, and electronic badges worn by staff and residents that allowed their location to be constantly tracked and recorded. Beckwith (2003) found that the individuals involved often were not aware of the technology's capabilities or the extent of the data being collected, and often forgot any monitoring was occurring. Although some of the data collected could be considered "sensitive," the study "found that people's lack of understanding of the technology rendered them unable to judge (Beckwith 2003)."

Without a clear understanding of what potential issues may arise as the result of a particular decision, informed consent to relinquishment of privacy is not possible.

2.2 Past and Current Approaches to Personal Information Privacy Protection

Differing perspectives on privacy make it difficult to come to any sort of consensus as to how best to protect personal information privacy. Privacy International, a watchdog group, suggests four current models of privacy protection, with countries often implementing combinations of these models (White 2003):

1. *Comprehensive laws* that regulate the "collection, use, and dissemination of personal information, by both the government and private sector," such as the European Union (EU) Data Directives;
2. *Sectoral laws* that provide regulations for specific areas like videocassette rentals and medical privacy, such as those found in the U.S.;
3. *Self-regulation*, encouraging companies or industry groups to adopt their own guidelines on "self-regulation" and engage in "self-policing", an approach used in the U.S.; and
4. *Technology*, making use of techniques such as encryption, anonymous remailers, proxy servers, and digital payment methods.

This section outlines the implementation of some of these methods in both the past and present.

2.2.1 Legal Approaches

Article 12 of the UN Declaration on Human Rights (1943) provided the first international recognition of privacy as a basic human right. Over the years, this agreement "has acquired the force of law through its incorporation into national laws, and because its language and ideas have been included in subsequent, binding treaties on human rights (Rotenberg 2003)." The need for privacy protection was also recognized in the U.S. Department of Housing, Education, and Welfare (HEW) Report (1973), which highlighted concerns relating to governmental use of personal information. The report recommended establishment of the Code of Fair Information Practices, to apply to government records contained in computer databases. Recommendations included principles like notice, access, use limitation, accuracy, and security, principles similar to those recommended in the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines of 1980, which promoted the setting of minimum standards (Solove and Rotenberg 2003; Onsrud et al. 1994).

A general privacy law approach has been followed by the European Union, with implementation of the European Union Data Protection Directives of 1995, 1997, and 2002. EU Directive 95/46/EC regulates the processing of personal data and the movement of that data, limiting data transfer to EU countries or those with equal levels of privacy. The 1997 and 2002 directives are seen as "add-ons", developed to keep pace with new technology. The EU Directive 97/66/EC additionally protects personal privacy within the telecommunications sector, and EU Directive 2002/58/EC specifically covers privacy protection within the electronic communications sector. These EU Directives follow an "opt-in" requirement, in which the user must give explicit consent to have his

information collected (Zevenbergen 2004; Myles et al. 2003). Many of the post-Communist countries follow the European lead and explicitly grant data protection within their constitutions. The European approach to privacy law places the emphasis on protecting personal information from third-party users, with the EU Directives applying in the business arena, as well as to government (White 2003). While often advocated in the U.S., one should note that an "opt-in" approach has been held by the federal judiciary to-date as a violation of corporate "free speech" under the U.S. Constitution (U.S. West, Inc. v. FCC 1999). This suggests that alternatives to blanket laws need to be considered in the U.S. context.

Privacy law in the United States focuses mainly on protecting individuals from governmental abuses of privacy. There is a tendency to steer clear of regulating privacy within the marketplace. Rather than general across-the-board privacy regulations, U.S. law instead provides "scattershot" protection of information privacy, applying to specific areas (White 2003). Examples of major privacy laws in the U.S. include: the Fair Credit Reporting Act (1970), protecting individuals against misuse of personal information by credit reporting agencies; the Privacy Act (1974), which provides guidelines for federal agencies regarding the use and disclosure of personal information of citizens and provides citizens with access to their own files; and the Financial Services Modernization Act (1999), requiring financial institutions to provide consumers with a notice of the institutions' privacy practices and the right to "opt-out" of the sale of their personal information to third parties (Rotenberg 2003). According to Monmonier (2002), the Financial Services Modernization Act provides "...consumers and investors limited rights to control their data," however, "its opt-out procedures are arcane, inconsistent, and

unable to guarantee the confidentiality most of us crave," and he supports instead "...an opt-in requirement whereby no one can sell or trade our records without our explicit permission."

2.2.2 Technological Approaches

Various methods have been employed to protect the confidentiality of individuals while performing analysis of database records to extract useful information. One such area of concern is dealing with health records, especially when performing geographically-based analysis. Past approaches have involved aggregating all records for a geographical area of a specified population, which restricts the usefulness of analysis results. Armstrong et al. (1999) proposed instead to apply geographical masks to individual health events, allowing valuable analyses to be performed, while protecting the privacy and confidentiality of the individual records. Another approach for protecting information in databases is proposed by Latanya Sweeney of Carnegie Mellon University, who is developing privacy enhancing software using a "k-anonymity" model, in which "each individual record is minimally generalized so that it indistinctly maps to at least k individuals (Morgan and Newton 2004)." Sweeney's privacy-enhancing software might return query results of only the first three digits of a zip code or just the birth year, rather than the exact date (Kumagai and Cherry 2004).

Other researchers have endeavored to design filters for databases that protect the confidentiality of contained records. Teresa Lunt is designing a "privacy appliance" to restrict the in flow and out flow of database information that would permit identification,

short of a court order. The device also generates log files and audit trails to trace intruders (Kumagai and Cherry 2004).

A number of Privacy-Enhancing Technologies (PETs) have also been developed to protect personal information by controlling the amount of information released during on-line transactions or communications. Encryption is one type of PET in which data is scrambled or transformed into an unreadable format, and can only be unscrambled with a decryption key available to authorized users. Two common types of key encryption systems are symmetric-key and public-key systems. With the symmetric-key system the same key is used for both encryption and decryption. Public-key cryptography makes use of two separate keys – a public-key and a private-key. Data encryption is accomplished through use of the data recipient's public-key, which may be published in an online directory. Only the private-key can decrypt the message. Steganography can be used along with encryption to hide encrypted identifiers or other data in bits within the message (National Research Council 2000; Senicar et al. 2003). Using a key generator like public-key cryptography, and then adding a signing and verification function, a digital signature can be created. When a key pair is generated, a user can input the secret key and a digital object into the signing function. This produces a signature, or set of bits, as output. The object, the signature, and the signer's public key are then fed into the verification function to access the data (National Research Council 2000).

Anonymization is another example of PET. Anonymization involves assigning a pseudonym or alias, creating a unique ID, so that a user is not identified, during web browsing for example (Senicar et al. 2003).

2.2.3 Policy Approach

The Platform for Privacy Preferences Project (P3P), developed by the World Wide Web Consortium (W3C), follows more of a policy approach to privacy protection, relying "on social and legal pressures to compel organizations to comply with their stated policies (Myles et al. 2003)." P3P allows Web users to designate their own privacy preferences and then compares those preferences to the privacy policies of websites they visit. This comparison is carried out automatically through a web browser. (P3P 2003) If policies of a website do not match the privacy preferences of the user, then the browser will inform the user, who can then decide whether or not to enter that website. While a huge amount of time and effort by industry and others have gone into developing this approach, its widespread adoption and use has yet to occur.

2.3 Location-Based Privacy

Recent advances in technology have greatly enhanced surveillance capabilities. With the proliferation of surveillance cameras, an estimated 26 million in use worldwide and 11 million of those within the U.S., along with other technologies allowing electronic toll payments and ATM or credit card transaction recording, it is nearly impossible to move throughout the day without being picked up by one or more of these sensors. As an example, it is estimated that in London an average individual's image is captured by more than 300 cameras every day (Farmer and Mann 2003). By 2005, an FCC mandate requires wireless carriers to provide the location of cellular phone users in the U.S. to within a few hundred feet (White 2003). While current technology in the commercial sector is not yet coordinated sufficiently to allow for the automated tracking of

individuals, this could easily change with the ever-evolving and newly emerging technologies. This expanding ability to track the movements of average citizens has led to increasing concern over protecting information that relates to an individual's specific location and the desire to obtain more control over release of such information.

2.3.1 Defining Location Privacy

In order to understand the issues involved in location privacy, it is necessary to understand exactly what location privacy is and how it varies from other types of privacy issues. Beresford and Stajano (2003) define location privacy as "the ability to prevent other parties from learning one's current or past location." White (2003) lists a series of three processes that distinguish location privacy issues from other types of privacy issues – *location identification*, *data processing*, and *value-added use*. In the first process, location technologies provide identification of an individual and the determination of her location. In the second process, the location information collected is stored so as to allow processing. In the third process, there is a current or potential "value-added" use for the collected location information, although these "value-added" uses are often not foreseen.

2.3.2 Concerns Relating to Location Privacy

The importance of location privacy increases as location-tracking technologies gain greater accuracy in their locating capabilities. For example, an individual may not be concerned if he can be tracked and located to within 1000 meters, but once his location can be determined to within 10 meters his concern may grow. As of May of 2000 when the U.S. government turned off selective availability, even the most inexpensive GPS

receivers can determine location coordinates to within a range of 3-10 meters, provided the signal is not blocked by obstacles such as buildings or hilly terrain. As GPS technology and other location-tracking technologies continue to progress, pinpointing locations will become more and more accurate.

Along with advances in locating technologies, computing capabilities are constantly expanding. According to Moore's law, processor speed roughly doubles every 18 months. Hard drive capacity has doubled each year over the last decade (Farmer and Mann 2003). As computing capabilities improve, the potential severity of the consequences resulting from privacy abuse by means of location-tracking technologies also grows. Greater storage capacity allows for retention of more data and greater processing capabilities can provide faster and more in-depth data analysis.

In addition to concerns relating to the collection of very accurate location data are the concerns raised through the potential linking of that location data with other types of personal information. One location-based service (LBS) user may find the advertisement for a discount on leather jackets received as she passes a clothing store to be an annoyance, while others may be glad to receive discount offers reflecting their purchasing preferences. Although in this instance the linking of personal location and purchase profile data has resulted in an annoyance at most, the linking of other types of personal information to location data could prove more harmful. If an individual were continuously tracked, that individual's location could be determined at any given time. Additionally, if this data was collected over time, it might be fairly easy to infer where an individual would be located at a given time on a specific day. An unauthorized person gaining access to the data or an unscrupulous person having access may decide to misuse

the data to cause harm to the individual being tracked, linking the location data to other personal data such as home address and recent purchases.

As is often the case, there are costs involved in the use of new technologies. The use of wireless communication devices involves tradeoffs. Users are generally free to communicate from whatever location they choose. However, "that freedom from a *particular* location has a cost – the possibility that one must give up the ability to communicate from *any* location without disclosing that location to the wireless provider, allowing processing of that location information and further downstream uses (White 2003)." With that disclosure of location may come another cost – vulnerability to stalkers or others wishing to cause harm.

Chapter 3

RFID TECHNOLOGY

Although Radio Frequency Identification technology has become a hot topic of late, with current use becoming more widespread not only within industry but many other fields as well, it is not a new technology. RFID has been in use since World War II at least, when in 1940 the Royal Air Force implemented the "Identification Friend or Foe" system in which transponders placed on their aircraft would respond to signals, differentiating RAF from enemy aircraft (Royal Air Force 2003; Weis 2003). Since that time utilization of RFID technology has expanded to include numerous applications, from identifying and tracking lost pets to preventing theft of retail store goods and library books. Many novel uses of the technology are also being envisioned for the future.

3.1 Components

An RFID system generally includes three main components: an RFID tag, or transponder; an RFID reader or transceiver; and a "back-end" database. The RFID tag may contain "object identifying data," such as the brand, manufacturer, and model, along with a unique ID or serial number in the case of a product tag. The reader communicates with or interrogates the tag, having the ability to read and write tag data, depending upon the type and existence of a microchip within the tag. The database stores information received through the tag and related to the tag ID number (Weis 2003).

3.1.1 RFID Tags

Most RFID tags are made up of two basic parts - a microchip, permitting an ID number and possibly other data to be stored within the tag, and a means of communication such as an antenna coil or another type of coupling element (Weis 2003). The unique ID number of a tag has the ability to differentiate the tagged item from any other item, even one of the same brand and style.

Tags may be classified by their power source or by the types of functions they are able to perform. The three classifications by power source are passive, semi-passive and active tags. Passive tags do not contain their own power source and therefore must rely on the reader for activation and power. Power is supplied to the semi-passive tags through a battery, but the tag can only respond to signals received from the reader. Active tags also contain a battery as a power source, but in addition to receiving signals, the tags are able to trigger communication with the reader as well (Weis 2003).

Weis (2003) groups tags into five classifications by the functions performed, those classifications being similar to ones outlined by the MIT Auto-ID Center. Weis' five classes are ranked from 0 to 4 with Class 0 being the simplest tag. No unique identifier is found within Class 0 tags and these tags provide only *electronic article surveillance* (EAS), making their presence known to a reader. Class 1 tags, generally passive tags, contain a unique identifier. Tag memory is read-only or write-once read-many. Class 2 tags have data logging capability, with read-write memory. Typically these are semi-passive or active tags. Tags within Class 3 integrate environmental sensors that may record a feature such as temperature or monitor motion. These tags are semi-passive or active. Class 4 tags are active tags and able to communicate with other tags by creating

"ad hoc wireless networks." The main focus of this thesis is on Class 1 tags, passive tags containing a unique identifier.

3.1.2 RFID Readers

Normally a reader will initiate communication with a tag by transmitting a signal that is received by the tag when it comes within read range, the distance within which a reader is able to communicate with the tag. Read range of passive tags is typically up to 3 m, depending on such variables as the tag frequency and the RFID system being used (Psion Teklogix Inc. 2004), and newer technology is enabling longer read ranges. For passive tags the reader must supply power to the tag. This is accomplished either by "far-field energy harvesting" of a reader's signal or inductive coupling. For the latter, the magnetic field created by the reader causes an electric current to pass through a coupling element that powers the capacitor (Weis 2003).

Communication between a passive tag and a reader can be accomplished by one of two methods. In the 'reader talks first' method, tags are activated by the reader, but do not reply without a specific request from the reader. By applying 'tree walking' algorithms, for instance, the reader is able to specify a certain tag, rather than interrogating every tag within range. With the 'tag talks first' method of communication, transmission of data by the tags begins upon crossing the read range threshold, facilitating the tracking of swiftly paced objects (Asif and Mandviwalla 2005).

3.1.3 Databases

The real usefulness of a tag derives from the ability to store its related data, such as product or location information. A database contains information only as current as its last entry, generally the "moment of last human intervention (Weis 2003)." When RFID readers are linked to a database, that database can provide more than just a "snapshot" regarding a tag's last location, for example. It can supply an automated and continuously updated record of details associated with the tag, replacing the snapshot with "live video (Weis 2003)."

3.2 Enhanced Capabilities of RFID over Barcodes

RFID technology provides a number of advantages over optical barcode technology, leading to increased benefits for users of RFID systems. For instance, although the Universal Product Code (UPC), adopted as the standard industry barcode, contains the manufacture and product codes of an item, unlike RFID tags, it is unable to provide a unique identifier. Therefore, that particular item cannot be distinguished from another item of the same brand and style.

Additionally, when using optical barcodes is the necessary for proper alignment with the barcode scanner in order for the code to be read. If the barcode becomes distorted, or is covered in plastic wrapping, there is more potential for limited functioning of the scanner (Weis 2003). RFID readers, on the other hand, do not require line of sight to communicate with the tags and are able to automatically read up to several hundred tags per second at a distance of 3m or more for many systems (Weis 2003; Psion Teklogix 2004). Tags can be read through packaging such as cardboard, plastic, or paint,

allowing more flexibility in tag placement, and greater protection from harsh conditions or tampering (Psion Teklogix 2004). A RFID reader could easily determine the number of product packages located on a pallet, rather than having to scan the packages individually, thus providing greater efficiency and lowering labor costs (Weis 2003; Psion Teklogix 2004).

Currently there is the capability for RFID tags to be read by the various independently operating parties within the supply chain, perhaps using incompatible RFID systems. However, if a standardized RFID system were to exist, with each party in a product's lifespan – from manufacturer to waste disposal or recycling company – providing data to a comprehensive database as the product moved through each phase, then a complete history of the product could be logged. This would allow greater oversight by regulatory agencies such as the U.S. Food and Drug Administration, providing protections relating to prescription drugs or perishable food products (Weis 2003; Psion Teklogix 2004). In addition, cost savings for managing supply chains and retailer inventories could lead to substantial savings for consumers (Weis 2003). ROI-Watch estimates initial savings to Wal-Mart for RFID implementation of: $6.7 billion in decreased labor costs; $600 million in reduced costs relating to out-of-stock supply chain; $575 million in decreased theft; $300 million through improved tracking within warehouses and distribution centers; and $180 million relating to inventory holding and carrying costs (Asif and Mandviwalla 2005).

3.3 Current Applications

Applications of RFID technology can generally be placed into one of three categories – point-of-sale, closed loop, or open system. Point-of-sale applications are those involving automatic fast payment for goods such as gasoline or electronic toll collection systems. Closed loop applications are "standalone" solutions, overseen by only one owner. These could include applications in healthcare, animal tracking, or manufacturing processes, for example. Open systems would allow different entities, such as the manufacturer, the transportation provider, and the retailer of a particular product to make use of the same system. Open systems have been slower in arrival, since there is no universal standard for RFID technology at this time (Psion Teklogix 2004). However, widespread access to the data on many passive RFID tags may still be possible, since the tags are often not encrypted (Newitz 2006).

3.3.1 Point-of-Sale Applications

These applications have become increasingly popular as individuals strive to speed up transaction time and ease. ExxonMobil Speedpass allows customers to pay for gasoline with a wave of their ID encoded key fob over the RFID reader. More states are now implementing electronic toll collection systems, such as E-Zpass and FasTrak, allowing drivers whose vehicles are mounted with a transponder to simply drive through toll plazas (Psion Teklogix 2004; Dipert 2004).

3.3.2 Closed Loop Applications

The largest utilization of RFID technology within closed loop systems is in the tracking or locating of objects or individuals. Groups as diverse as librarians and nightclub owners are seeing the potential of RFID to increase profits and/or efficiency, while providing more consumer payment or checkout choices. RFID has been used within the commercial sector for years in the removable theft detection devices attached to clothing or other items in many retail stores. Now those clunky devices can be replaced with smaller, less conspicuous tags that will sound an alarm if an item is removed from the store before purchase. Manufacturers are using RFID to follow products through the manufacturing process and retailers are keeping a closer eye on their inventory, whether tires or shampoo bottles.

Hospitals and nursing homes are also joining the RFID bandwagon. Several Boston area hospitals are experimenting with RFID to track equipment as well as surgeons, so that both can be located quickly in an emergency. Patients at Massachusetts General Hospital are tagged, along with their medications. If a drug enters the room of an allergic patient, or a patient has waited more than an allotted time between tests, staff pagers will be alerted (Berdik 2005). Nursing homes are finding RFID tags helpful in locating wandering Alzheimer's patients.

Pet owners have been using embedded RFID tags for years to locate lost pets. Fifty million pets have been tagged worldwide. Livestock tagging has reached twenty million worldwide (Psion Teklogix 2004). This became more popular after the Mad Cow Disease scares, in order to trace the history of the animals. The newest in RFID cows tags are ruminary tags, which can be swallowed by a cow and then reside in its stomach

(Transponder News). Implantable RFID devices are no longer limited to pets – people are choosing to become "chipped" as well. Beach club patrons in Barcelona can pay for food and drinks electronically using their subdermally embedded tags. One hundred sixty government employees at the anticrime information center in Mexico City, along with the Attorney General, have been tagged with Verichip devices. Some individuals in South America have elected to go through the chipping process in response to increasing occurrences of "flash kidnapping." In addition, medical records can be linked to the ID number of a subdermal tag, allowing even unconscious individuals the ability to provide health information to medical personnel (Dipert 2004).

Many other individuals are being tracked in the course of everyday life. Businesses are tracing employee movements through use of RFID badges or cards, and limiting access to certain areas. Primary schools in Japan are placing RFID tags on clothing, bags, and nametags to locate students. In 2004 the shoes of Olympic Marathon and Boston Marathon runners were fitted with RFID tags, allowing readers along the racecourse to track the runners' locations, helping to prevent fraud (Dipert 2004).

Other items tracked through RFID include library books and airline luggage. Over 130 libraries in the U.S. are finding RFID technology useful in managing their collections. In addition to locating books, RFID could provide the ability for library patrons to checkout their own materials, not only speeding up the process for patrons, but also lessening librarian duties (Bender 2005). The Vatican Library has implemented RFID tags in the management of its extensive collection of 2 million books and other treasures. Delta Airlines is implementing a luggage-tracking pilot along one route, with plans to expand to other routes in the future (Dipert 2004).

These are but a few of the many applications currently being employed throughout industry, healthcare, government, entertainment, and various other arenas. The potential exists for much greater implementation of RFID in the future, with widespread adoption of current applications and those yet to come.

3.4 Predicted or Conceivable Applications

Future applications of RFID technology can be approached from two different perspectives. The first is a tag-based perspective in which consideration is given to the items to which a tag can be affixed, the information that will be linked to the tag and what opportunities that will provide. The second is to think about applications within a pervasive RFID reader environment - where the readers could be located and how this might change peoples' everyday lives.

3.4.1 Tag-based Perspective

The slant of current applications is more towards a tag-based perspective rather than a reader-based one. The majority of these current applications focus mainly on locating and tracking an object, animal or person, rather than focusing on the recording of large amounts of data about the subject of the tracking. This focus likely will shift somewhat in the future. Although locating and tracking will remain a large part of the RFID market, the growing amount of data that can be collected through and linked with the tags will become increasingly significant.

The general movement is towards the integration of RFID tags into every conceivable item and/or item packaging. Many consumer products could soon contain a

tag - home furnishings, food products, clothing, and accessories. Products could be tracked from creation to destruction, providing a wealth of information for marketing purposes, not to mention the ability to continuously track the individual wearing or using the products.

One predicted use of RFID tags is for authentication of products. With the proliferation of pricier brand name item "knock-offs", the ability to distinguish "knock-offs" from originals becomes more pertinent. Also, if a tag affixed to a purchased item had the capability of being linked to recorded purchase data, it would be simple for a retailer to determine purchase price and date, were the item to be returned for a refund. In another example, to ensure only approved engine and aircraft parts are used in aircraft construction, Boeing and Airbus are requiring their parts suppliers to attach tags to the parts, providing data on part numbers along with pricing information (Dipert 2004).

US Government plans for RFID technology include embedding RFID chips into e-passports. This would allow border agents to retrieve and then view the data on the tag - the bearer's name, place and date of birth, as well as a digital photograph. Using facial recognition software, a comparison between the traveler and the digital photograph could be made. Citizens of the 27 countries from whom the US does not require travel visas will need to carry e-passports as well. A prior deadline for compliance has not been met by most of these countries, leading to an extension of the deadline. Originally, no encryption techniques were to be employed to protect the data on e-passports. Security issues were to be addressed through use of write-once chips and digital signatures. (Singel 2005) The government is reconsidering security measures in light of tests showing that passport chips could be read from a distance of up to 30 feet, not the 10 cm

range they had previously held to. A solution under consideration involves the requirement of a reader password and encryption of the data transmitted between the chip and the reader (Zetter 2005). Presumably it would be feasible for the border crossing RFID reader to identify other items that contain RFID tags within a person's vehicle or on their person, items that are possibly illegal to bring into the country.

3.4.2 Pervasive RFID Reader Environments

With the proliferation of RFID tags comes the necessity of collecting data gathered through those tags. The more readers in place, the more data can be collected. Thus evolves a pervasive system of RFID readers, seeping into every aspect of life, whether in the home, office, vehicle, grocery store, or on the street corner.

The home of the future has great potential to draw on RFID technology. The vision is that homeowners won't be bothered with remembering such mundane details and tasks as making grocery lists, choosing washing machine settings, and adjusting light, temperature, and music to their personal preferences. RFID will do all of this for the homeowner. Readers dispersed throughout the home will detect which individual has entered the room through tags on their person and will adjust environmental settings accordingly. Washing machines will contain readers to scan the tags on clothing and microwaves will read food package tags so that the appropriate options will be chosen. Refrigerator readers will be alerted when supplies are low or the milk expiration date has passed and can reorder groceries to be delivered right to the door. Those same readers can determine which products are on the shelves of the refrigerator, in the kitchen cupboards, or within the medicine cabinet and send tailored commercials to the homeowner's

television. Medicine cabinet readers can not only determine the particular drugs on the shelf, but also track patient consumption and alert the patient and his/her doctor or pharmacist to any deviation from prescribed usage (Dipert 2004). Other readers in the home can be queried to locate misplaced eyeglasses or keys. Shelf readers can catalog the entire book or music collection in the home. If a product recall occurs on a purchased item, the networked reader at the front door that recorded the tagged item on its way into the home, and could then alert the homeowner to the recall (Garfinkel 2002).

Once leaving the home, individuals will face readers within and tags attached to their vehicles. The UK is considering the adoption of license plates containing RFID tags. These tags could be read from a distance of up to 300 feet, from stationary readers embedded within the environment or located within surveillance vehicles, recording vehicle locations wherever a reader was placed (Dipert 2004). Another potential use of RFID involves placing e-tags into windshield stickers. A system currently exists that allows for electronic toll collection and vehicle registration through windshield e-tags. If implemented by law enforcement, readers could automatically monitor traffic to locate uninsured vehicles, those with expired registration or outstanding violations, as well as those noncompliant with emissions regulations (Smith and Konsynski 2003).

Various theme parks within the United States and other countries are using RFID-embedded wristbands to allow parents to locate their children should they become separated, or family and friends to locate each other within the park through use of touch-screen kiosks (Gilbert 2004). Locating abducted children within a future pervasive RFID environment is another potential application of RFID technology. If the family of a child knew what clothing or other RFID-tagged items the child was wearing at the time of the

abduction, perhaps scanning the child with a personal RFID reader before the child left the house each morning, records from RFID readers could be searched for those particular tag ID numbers. Specific readers placed at bus stations, toll booths or other areas could be helpful in determining the route followed by the abductor and child.

If a trip to the grocery store is necessary, a person will find readers there as well. Pilot stores such as the METRO Extra Future Store in Rheinberg, Germany showcase RFID potential. Smart shelves determine when shelf inventories are getting low and restocking of tagged products is necessary. Product prices are adjusted on the shelf LCD labels as inventory increases or decreases. When an RFID-tagged DVD is scanned at the video kiosk, a movie trailer plays. Rather than waiting at the checkout, people will soon be able to push the cart right past a reader that instantly records all items within the cart and automatically deducts the amount from the person's checking account or charges a credit card (McHugh 2004). However, products are not the only objects containing RFID tags at the Future Store. Tags have also been embedded in loyalty cards, which when carried through the entrance RFID gates could potentially track which customers are entering or leaving the store, or the route of a customer while in the store (Albrecht 2004).

Like the home, office environments will be automatically regulated as to the preference of an individual entering a room. A person's desktop could appear on any computer she approaches for use. Surveillance of employees will no doubt expand as employee locations and activities can be continuously recorded. Surveillance will follow that employee out the door and down the street as readers record what she is wearing and carrying through the tags on her clothing and other portable items on her person. RFID

may facilitate time efficient crime for the thief located on the corner or in the parking lot, determining his next victim with a mobile reader in hand.

3.5 Issues and Challenges to Face in RFID Adoption

Many hurtles must be overcome before RFID technology is implemented on a wide scale basis. Changing from one type of system to another, in this case barcode to RFID technology, usually necessitates a major financial investment and companies first want to make sure they will receive a sufficient return on their investment. However, cost is not the only issue to face. This section outlines some of these issues, reserving a discussion of privacy related issues for Chapter 4.

3.5.1 Cost

A substantial investment, both in time and resources, is required for compliance with mandates such as Wal-Mart's requirement for its 100 top suppliers to tag cases and pallets by a January 2005 deadline. First year expenses for a large supplier (16 million cases and pallets) to meet this mandate might be as high as $9 million. An estimate for a consumer packaged goods manufacturer to implement RFID in shipping 50 million cases per year breaks down as follows: $5-10 million for tags and readers; $3-$5 million for system integration; $3-$5 million for modifications to existing supply chain applications; and $2-$3 million for storage and data analytics, altogether adding up to $13-$23 million (Asif and Mandviwalla 2005). Tagging of individual items, rather than just cases or pallets, will greatly increase these costs. However, it is the tagging on a per item basis that provides the capability for many proposed applications.

With the deployment of more tags comes the generation of greater quantities of data, leading to the necessity of more sophisticated software and IT design. According to Asif and Mandviwalla (2005), "...such data volumes will impose severe strains on existing data management and storage structures and strategies." One proposed method of dealing with the massive data generation is the Savant system (Sarma et al. 2002) developed by the Auto-ID Center at MIT. This software is designed to filter data received by the reader, to sort out errors such as duplicate tag reading or "phantom" or false reads sometimes occurring in manufacturing settings. Savant then sends the clean data to the back end system applications, reducing chances of overloading a system (Asif and Mandviwalla 2005).

Training of personnel represents another potentially large expense. In addition to training the workers who will be directly using the technology, there is also the need to find individuals that are skilled in implementing RFID technology and integrating it with current systems. According to Asif and Mandviwalla (2005), "...middleware has not advanced to a 'plug-and-play' stage, which means that initial adopters will have to spend considerable effort to integrate RFID into their existing business processes."

Another direction in which companies will have to focus attention is in discerning customer desires and developing marketing tactics relevant to RFID technology. "Speed and cost are the relatively easy and obvious goals of RFID enabling a supply chain; the more interesting and potentially strategic application may include integrating supply chain concepts with customer (marketing) strategies (Asif and Mandviwalla 2005)."

3.5.2 Lack of Standards

Standards are vital for interoperability and can reduce costs. Without large-scale adoption, equipment costs will not decrease, but without universal standards, this adoption is not as likely to occur. RFID users do not want to implement a RFID system based on current standards, then have to totally revamp the system later on when new standards are adopted, or face the issue of lack of interoperability between their system and others sectors in their supply chain, whether in this country or internationally (Asif and Mandviwalla 2005). A recently ratified standard may aid in dealing with this issue. EPCglobal, a standards body for retail supply, has ratified the Electronic Product Code (EPC) UHF Class 1 Generation 2 RFID protocol. The EPCglobal Network "provides the infrastructure for sharing RFID-enabled information about products in the supply chain (Hulme 2004)."

3.5.3 Security

Due to the restricted computational ability of tags, security measures such as cryptographic algorithms are difficult to apply. Theoretically any reader within range of a tag can gain access to data encoded on the tag's microchip, as RFID tags for the most part cannot authenticate readers (Asif and Mandviwalla 2005). However, within a Generation 2-compliant system, there is the capacity for the tag to require a password before it will communicate with the reader and allow the reader to access tag memory (Intermec 2005). Even though capabilities such as password protected access to tag memory and to initiate the kill command are included in the Gen 2 standard, use of these capabilities is optional

and they may not be employed in certain tags due to increased cost (Bailey and Juels 2006).

3.5.4 Accuracy

Although RFID technology is advancing, reader accuracy has fallen short of 90 percent in some cases. Performance of readers can be affected by conditions within a tag's environment, such as the proximity of tags to products or packaging containing metal or water that affect absorption of radio waves, or from electromagnetic interference. Changes to the 'physical infrastructure' may be necessary, for example, to deal with nylon conveyor belts producing static (Asif and Mandviwalla 2005).

With the move from pallet and case tagging to the tagging of individual items, the ability to read greater numbers of tags simultaneously becomes critical. If multiple tags enter a reader's vicinity there is the potential for tag collision, causing either misreads or no reads to occur. 'Singulation' techniques, such as the 'tree walking' technique mentioned in section 3.1.2, allow the request of data from only specified tags distinguished through their serial number (Asif and Mandviwalla 2005; Weis 2003). The Aloha is an anti-collision algorithm in which tag collision is evaded through random delay of tag responses (Weis 2003).

Through these and other methods, advancement towards a more accurate and secure design is being made. This is vital, because if issues such as accuracy or the others mentioned in this section are not addressed, supply chain management may not see the benefit of investing huge sums to adopt RFID technology over barcodes, absent mandates requiring the technology.

Chapter 4

RFID PRIVACY IMPLICATIONS AND ISSUES

Fear of new technology and its potential threat to personal privacy has caused some to call for an outright ban on RFID technology, while others simply wish to limit its use. Still other groups and individuals believe that RFID technology should be exploited to its full potential. "As a society, we typically overestimate the short-term impact of new technologies and underestimate their long-term impacts (Smith and Konsynski 2003)." Like many other technologies, it is only as RFID technology evolves and new applications are developed that certain societal implications from the use of this technology present themselves. It is often difficult to foresee or predict what may occur down the road.

4.1 Uniqueness of RFID Related Privacy Issues

In a statement on RFID technology given before the House Subcommittee on Commerce, Trade, and Consumer Protection, Bruening (2004) outlined three ways that data collection through RFID technology is distinctly different from other technologies. These differences include the invisibility or hidden nature of the technology, the passivity of the consumer in the data collection process, and the type or detail of the data collected.

Due to the small size in which RFID microchips can now be produced, RFID tags are in effect invisible to the eye. Recently Hitachi introduced the 0.4mm square μ-chip (Hitachi 2004). As RFID technology continues to develop, microchip dimensions will no doubt be reduced even farther, allowing for a decrease in tag dimensions as well. The

small size will allow the tags to be virtually undetectable when embedded within objects such as clothing, food or other product packaging, and even shipping labels or paper. Since consumers may be unaware of the tag's existence, or the existence of RFID readers in the surrounding environment, they most likely will also be unaware of the data collection taking place as they go about their daily routines. This is in contrast to the visibility of the data gathering process involving loyalty cards or bar codes (Bruening 2004).

The consumer plays a passive role in the RFID data collection process. When a consumer uses a credit card for purchasing, the consumer takes an "active step" to become involved in the transaction and the subsequent transfer of information relating to the transaction – credit card account number, type of goods or service purchased, as well as the location and time of the transaction. However, no active step is required to become involved in data transfer through RFID use, and so the transfer of data may be hidden from the consumer. Unlike credit card statements received on a monthly basis detailing purchases, RFID data gatherers do not inform individuals of what information was collected and by whom (Bruening 2004).

RFID allows the collection of data at a level of detail never before possible. The technology will allow data gatherers to go beyond the personal profiles amassed today. Rather than just knowing you bought a copy of a particular book, the "globally unique" ID number that can be stored within a RFID tag allows the determination of exactly which copy of the book you bought and where you went with the book after purchase (Bruening 2004). This scenario can be expanded to include the purchase and subsequent tracking of any item containing a tag in the future.

The result of these distinctions of RFID technology is that much more information can be collected and therefore the potential and the desirability of data sharing increase greatly. As with the use of cookies for online interest assessments, RFIDs would allow businesses to determine not only what consumers buy, but if a RFID tag were embedded within a loyalty card, which items consumers showed interest in as they moved through a store. According to Bruening (2004), "RFID transfers to the brick and mortar world the type of very specific tracking of interests that is possible online."

The uniqueness of RFID issues raises some questions for which there may be no easy answers. Harvard Law professor Jerry Kang, speaking at the RFID Privacy Workshop held at MIT in November 2003, posed several societal choices to be made regarding RFID technology and privacy (Weis 2004), including:

- Who controls the information that RFID systems generate?
- How do people make difficult decisions about using RFID in the presence of coercion or the lack of viable alternatives?
- When does society have the right to override individual privacy?

4.2 Privacy Issues Raised by Current Applications

One impetus for greater privacy protection stems from the increasing ability to link personal data collected from various sources. RFID technology takes this to another level by adding location data to those personal records, providing additional context for an individual's actions. According to Weinberg (2004), "RFID is important from a privacy standpoint even where it only facilitates the collection of information that could otherwise be collected by analog means, automating the information collection and

storage process." For example, the manual recording of license plate numbers of vehicles traveling on a highway, versus RFID readers automatically recording the unique ID number in RFID embedded tires or other vehicle parts, with that ID number linked to an automobile's VIN in another database (Weinberg 2004). Both approaches can reveal, if not who was driving each vehicle, at least who the vehicle was registered to. "RFID readers...collect the information in a format that makes its inclusion in networked databases trivial. That's important, because the cheaper it is to collect, store and analyze information, the more information will in fact be collected, stored and analyzed (Weinberg 2004)."

4.2.1 Tracking

A major thrust of RFID technology today is towards tracing the movements of objects or people. Provided an object itself isn't being transported by or linked somehow with the movements of a person, tracking the object may raise relatively few concerns. However, the idea of having one's movements tracked throughout various aspects of one's life would not appeal to most individuals. Employees, for example, are often under the microscope on their jobs. Using RFID technology, employers may be able to keep fairly constant tabs on their employees from the moment they arrive at work, through their breaks, and until they head out the door at the end of the day. Although active RFID tags are required to provide continuous monitoring of movements and for actual location determination, passive tags can still reveal a good deal of information about a person's behavior and travel. For example, if workers are required to carry RFID embedded ID cards on their person or to gain access to certain areas of a facility, using strategically

placed RFID readers would make it possible to record when an employee passed a certain reader or entered a restricted area. Inferences could then be made regarding behavior, whether or not those inferences were in fact true. If an employee had to pass a reader when traveling in or out of his/her office, it could be determined how long that employee was out of the office, whether on break or carrying out some task. Determination of which route a person travels through the office is also possible. An employer may want to find out why an employee always goes by a particular desk or office, even though it may be out of the way for the task being performed. In this way it may be possible to determine with whom a worker is associating or perhaps organizing (Plichta 2004). These types of monitoring are not indicative of a friendly workplace environment and may tend to cause anxiety and stress.

4.2.2 Data Aggregation

As previously stated, data collection and aggregation is a large issue to face in personal privacy protection. RFID tags and readers only compound the problem, as they allow linkage of even more intimate data to one's current location. Generally, the more information that is gathered and aggregated, the greater the incentive that exists to breach personal information records, and the greater the threat once those records are breached. A computer security class of 41 graduate students at Johns Hopkins University recently demonstrated how easy it is to obtain and aggregate personal records. They carried out a project in which they proved that "...all it takes to obtain reams of personal data is Internet access, a few dollars and some spare time (Zeller 2005)." The task was to "vacuum up" as many records and databases as they could through legal, public sources

of information, with a budget of no more than $50 per student group. Students were able to acquire such databases as those related to death records, property tax, and occupational licenses. Methods through which the records were obtained included filing FOIA requests with local government offices or merely asking for information, and writing computer scripts to "pick up" databases online, whether governmental or free commercial databases such as yellow page directories. Several groups were able to obtain over a million records, showing on a small scale what large data warehouses are able to accomplish. As Professor Rubin points out regarding his students, "Imagine what they could do if they had money and unlimited time (Zeller 2005)." Jason Brandeis, an A.C.L.U. lawyer, states that "a balance needs to be struck between the public interest in open access to government information, and the need to protect individual privacy (Zeller 2005)." However, as Zeller (2005) acknowledges, "whether such a balance can ever be achieved when so much information is already available is an open question."

Although disclosure of information such as the value of an individual's property, which political party one belongs to, or which occupation one practices may not in themselves seem particularly distressing, when numerous records are linked, the ability to make inferences regarding an individual becomes easier (Zeller 2005). Integration with location data adds substantially to inferencing possibilities.

4.2.3 Profiling

Once data has been collected and combined, this facilitates individual profiling. Through embedded RFID tags, product information can be linked to a particular

consumer, from which assumptions regarding the consumer's health, income, lifestyle, or location can be made (Cavoukian 2004).

Langheinrich (2002b) feels that profiles are a threat to "universal equality." Although in the case of frequent flyer miles one may receive special offers or rewards based on a high number of miles, the opposite is also true. As Langheinrich (2002b) points out, "...even though a thoroughly customized future (using ubiquitous computing) where I get only the information that is relevant to my (very comprehensive profile) holds great promise, the fact that at the same time a large amount of information might be deliberately *withheld* from me because I am not considered a valued recipient of such information, constitutes a severe privacy violation for many people."

An example of the profiling potential through RFID data collection is the SmarTrip fare card used by Washington DC's Metro system. The fare card contains an RFID chip, allowing storage of a cardholder's personal data, such as name, address, and phone number, as well as collection of data on his/her use of the Metro system. This data includes the location and time of arrival at and departure from the Metro system, as well as Metro parking lots. The type of information derived from the data allows for the profiling of cardholders, but unlike state agency records, the data is not protected by law, only an internal Metro privacy policy (EPIC 2005).

As discussed in section 4.2.1, RFID employee monitoring can lead to inferences being drawn regarding behavior. However, employees aren't the only ones who need to consider whether they are being monitored and profiled. Marc Rotenberg, executive director of the Electronic Privacy Information Center, points out that students carrying RFID embedded student cards may be watched as well, revealing with whom they

associate, thus promoting assignment to a certain group and possibly subjecting them to more intense scrutiny based on their associations (Zetter 2005). As Weinberg (2004) brings out, "...RFID signifiers travel *with* the subject in the physical world, conveying information to devices that otherwise wouldn't recognize her, and that can take actions based on that information."

4.3 Potential Privacy Issues Raised by Future Applications

Many of the privacy concerns relating to current RFID applications also apply to future applications, but on a grander scale. As the technology becomes more pervasive and ubiquitous, the ability to collect personal data will increase at a potentially alarming rate. Developing a means to regulate the collection and linking of personal data will become even more crucial with the movement towards creation of an infrastructure allowing mass data collection and processing.

4.3.1 Per Item Tagging

The commercial buzz about RFID is growing and more corporations are beginning to invest in this technology. However, before RFID is widely deployed on a per item basis, the cost will have to come down. A recent study by the ARC Advisory Group estimates that passive UHF RFID tags will only drop in price to an average of 16 cents by 2008, not the once proclaimed 5 cents. They do acknowledge that if purchased in large enough quantities, it may be possible for some manufacturers to offer 5-cent tags (Ward 2004). It is estimated that at this point, the availability of a 5-cent tag, wide scale adoption of RFID technology will occur. Since it is impossible to predict with any

certainty just how quickly technology will progress, possibly allowing a shorter than estimated time period for a drop in prices, a timeline for RFID adoption is not feasible at this time. There is generally consensus on one point, however. Once the floodgates of RFID technology open up, the potential exists for tagging just about every consumer product made. This includes all clothing, in which the tags could store size, brand, price, as well as purchase location and date, or any other portable item that could be worn or carried. Items such as vehicles may contain multiple tags in various vehicle parts, facilitating collection of many different types of data. In addition, individuals possessing their own RFID readers may desire to tag their belongings in order to inventory collections, locate an item, or simply to identify an item as their own.

4.3.2 Surveillance

With widespread deployment of RFID technology looming in the near future, the issue of location tracking becomes an issue of all out surveillance of almost every moment of life. Were there to be a pervasive network of RFID readers dispersed throughout the environment – the home, the store, the office, and on every street corner – with tags embedded in most if not all consumer products, the potential threat to retaining even a modicum of privacy becomes enormous. There is some question as to whether a pervasive network of RFID readers could ever be assembled, and there is the belief that without this network, continuous location tracking would not be possible. However, as Weinberg (2004) points out, "if RFID use becomes widespread, then various commercial and governmental users are likely to deploy a wide range of discrete reader networks. If there are economic and political incentives for the proprietors of those various networks

to share information (and there are likely to be), then we will face the functional equivalent of a single very large network. At that point, any particular set of readers need not be pervasive." Weinberg (2004) relates a reader network to a "Panopticon geolocator" due to its ability to link identities with RFID tags, while providing location data.

Densely populated reader networks with readers located every few feet would not necessarily be required to enable continuous tracking. Positioning readers at "strategic locations" – entrances to buildings or entrance and exit ramps on highways or at street corners – could potentially generate enough data to provide fairly detailed location logs of individuals, whether traveling on foot or in a vehicle (CASPIAN et al. 2003). In addition to the possibility of an individual's location records being stored in a database for anyone gaining access to see, CASPIAN et al. (2003) argue that RFID tag location and data could in fact be transmitted to satellites by means of readers enabled with satellite communication capabilities, allowing real-time tracking of movements. This type of technology is already being employed in the tracking of product shipments as they move across the country.

One rising fear is the possible use of a pervasive network for government surveillance purposes (EPIC 2004c). By placing readers at building entrances, it would in theory make possible the automatic compilation of the identity of attendees to any particular event. This could result in the inclusion of these individuals on a government watch list in the future, prompt further surveillance or perhaps even arrest (Weinberg 2004). Although it would be difficult not to be traced through RFID tags were they embedded in clothing and other objects carried on the person, if implantable RFID

devices became mandatory for certain individuals, perhaps even being put into drivers licenses (Weinberg 2004), there would be no escape from surveillance for these ones. The U.S. military has discussed implanting RFIDs into soldiers, to provide quick access to medical records linked to the unique ID number of the tag. Rotenberg claims there is a real possibility of 'chipping' other individuals as well – prisoners, parolees, and children (Zetter 2005). Even though identification of a particular driver may not be possible through the scanning of one RFID tag, such as on a vehicle's tire, by "cross referencing" other tags within the vehicle or on the person, such as a tag in a library book, a link to that person's identity may be possible (Plichta 2004).

Another arena for pervasive networks to operate within is the retail environment. Stores such as the METRO Extra Future Store in Rheinberg, Germany, discussed in section 3.4.2, are designed with the plan of fazing RFID into most facets of store operation. The problem is, "...if a person enters a store carrying several RFID tags...one reader can read the data emitted by all of the tags, and not simply the signal relayed by in-store products. This capacity enables retailers with RFID readers to compile a more complete profile of shoppers than would be possible by simply scanning the bar codes of products a consumer purchases (EPIC 2004c)."

The Extra Future Store claims protection of customer security through its "De-Activator," which is supposed to disable RFID tags on items before they are removed from the store, by overwriting the chip's number code with zeros. As Albrecht (2004) discovered, this device does not in fact de-activate the tag at all. The number that is overwritten is merely the product code, which is the same for every like item of a specific brand. The unique ID number assigned to the particular item is not destroyed. This point

becomes very important when considering the future potential for pervasive RFID reader networks.

4.3.3 Security Against Unauthorized Access

With the potential for massive data collection, ensuring the security of data stored on and linked to an RFID tag is imperative. As appalling as it might seem to many for anyone to be collecting this data, the idea of an unauthorized person or group obtaining this data and possibly using it to the harm of an individual is even worse. Access to tag data may be accomplished by "skimming" the data on the chip with an unauthorized reader (Zetter 2005). Interception of the communication between a tag and an authorized reader is also possible (Garfinkel 2002). Eavesdropping readers can identify the contents of a purse, bag, or pocket, providing data to whoever wants it, including market researchers and thieves (Weis et al. 2003). In addition, data may be "hijacked" as it travels from a reader to the data storage location (Hulme 2004).

Spoofing of tags is a potential security problem, especially in retail environments. A thief may be able to "fool automated checkout or security systems into thinking a product was still on a shelf" or exchange data from the tag of an expensive item with that of a cheaper item (Weis et al. 2003).

At the 2004 Black Hat security conference, Grunwald demonstrated a program he helped create, known as RFDump. The program can read, alter, delete, or destroy tag data. The program requires only "an inexpensive plug-in tag reader attached to a handheld, notebook, or desktop running Windows or Linux (Hulme 2004)." Although most EPCglobal passive tags were at one time write-only, those now being deployed have

multiple-write capability, allowing alteration of tag data or for tags to be written to several thousand times (Hulme 2004). Even tags with password protected memory might be susceptible to brute-force attacks initiated to obtain passwords, allowing access to and therefore alteration of tag data (Newitz 2006).

Finding new means of dealing with these threats to the security of personal information in the use of RFID technology is essential. Developing privacy protections and security measures for this technology before mass deployment occurs would tend to make its introduction less costly and more likely to be implemented.

Chapter 5

ALTERNATIVE APPROACHES TO LOCATION PRIVACY PROTECTION

A significant concern relative to location privacy is the potential for linking data regarding an individual's location with other personal information, promoting the discovery of spatial inferences or patterns. RFID technology facilitates that link between personal information and location. The location of a tag can be determined through the location of the reader recording its unique ID, which may be linked to ever increasing amounts of stored personal information. This chapter examines legal, technological, and combined approaches to protecting location privacy, from general concepts that could be applied to RFID technology, to RFID specific ideas.

5.1 Legal Approaches

This section outlines legislative approaches to protecting location privacy in general and also specifically as it relates to RFID technology, from both U.S. and international perspectives. In addition, proposed guidelines for the implementation and use of RFID technology, along with resolutions emulating similar principles and goals are considered. Evaluation of these types of approaches is also discussed.

5.1.1 General Location Privacy

As mentioned in section 2.2.1 the U.S. has been reluctant to enact privacy legislation applying to the commercial sector and it has been even less inclined to enact specific location privacy legislation. The proposed Location Privacy Act of 2001 would

have required location-based service providers to give their customers "clear and conspicuous notice" as to planned uses of their location data, as well as requiring an "opt-in" rule for use of that data. Prior to this proposed legislation the Cellular Telecommunications & Internet Association had suggested comparable rules for regulating its own industry to the FCC, recognizing the need for clarification in this arena. The FCC decided on an "opt-out" requirement instead, and did not provide clarification through adoption of location privacy rules, feeling that these might "constrain the still-developing market for location-based services (White 2003)."

European governments have been more sympathetic towards protection of personal data, supplying this protection through the EU Data Protection Directives - 95/46/EC, 97/66/EC, and 2002/58/EC. EU Directive 2002/58/EC provides privacy protection within the electronic communications sector, relating to the processing of personal data and requiring explicit user or subscriber consent through an "opt-in" policy. It relates to the location-based services industry in that it contains definitions of traffic data, location data, and value added services and gives rules on how "traffic data" and "location data other than traffic data" may be used. For instance, Article 6 specifies that traffic data should be either erased or made anonymous if no longer required for transmitting a communication (Zevenbergen 2004).

Recent U.S. legislative attempts at more general data privacy protection could supply a basis for guiding principles to be applied in the location privacy arena as well. The Personal Data Privacy and Security Act of 2005 (S. 1332), recently introduced in the U.S. Senate, attempts to provide standards to protect personally identifiable information. A similar failed attempt at data privacy protection was the California Data Broker Access

and Accuracy Act of 2005 (S.B. 550), which would have regulated the "disclosure of personally identifiable information by data brokers." The Act included requirements for disclosing to individuals what personally identifiable information was collected about them, investigating disputed items, specifying procedures to control access to information, and the potential for initiating civil actions if there were violations of the provisions of the Act. Although this legislation would have allowed the potential collection of damages if data abuse occurred, White (2003) suggests that perhaps a better approach might be to develop a "*culture* of privacy protection" by means of a "more pervasive regime" such as the EU Data Directives or the FTC Fair Information Practices, as the "prevention of data abuse is far preferable to consumers than the collection of damages after some particularly heinous data abuse (White 2003)."

It would be prudent to perform a cost/benefit analysis when considering which type of "regime" would work best in providing data privacy protection, looking at both tangible and intangible associated costs. According to Hahn and Layne-Farrar (White 2003), some of the estimated business costs associated with fair information practice compliance are: $2-$5 billion to financial institutions to provide notice by designing, printing, and mailing privacy notices to customers under the Gramm-Leach-Bliley bill; $11.8 billion for ten-year compliance by the health industry to provide choice – allowing individual information use with consent; and $100 million to correct errors in consumer credit reports when providing access. However, the costs to consumers for lack of privacy protections can be high as well. When weighing the benefits and costs of an "opt-in" versus an "opt-out" rule, Kang (White 2003) gives several reasons why an "opt-out" rule provides the higher cost to consumers. First, there is the cost of determining if an

individual's personal information has been shared, with whom, and who currently has access to the information. Secondly, those who want to 'flip' or contract around the default rule, might not have the power to bargain for it.

Though U.S. legislation regarding personal data protection has been somewhat lax so far, there may be opportunity for data protection within the realm of data mining. As White (2003) asks, "is there a point at which data that would not in itself receive privacy protection become protectable because the use of technology has altered the reasonable expectation of privacy." With the potential for continuous tracking and data gathering capabilities through mass implementation of RFID technology, a many fold increase in data abuse becomes a likely prospect without stronger data protection controls being put in place.

5.1.2 RFID Specific

A number of U.S. states including New Mexico, Missouri, Utah, and Massachusetts have recently considered RFID bills, but various attempts to pass RFID specific legislation have failed. For example, in 2004 California rejected a bill introduced by Senator Deborah Bowen that would have regulated the use of RFID tags for businesses and libraries and would only allow collection of information from tagged items that were bought, borrowed or rented, not those that may have just been picked up or handled by an individual. The bill would also have prohibited collection of information from tagged clothing or purse/wallet contents. Bowen argued that RFID specific legislation should be addressed before the technology is deployed in order to avoid costly or difficult modifications to bring the technology in line with future regulations.

Opponents felt that legislation was "inappropriate" prior to determination of potential uses of the technology (Swedberg 2004). California has considered another piece of legislation relating to RFID technology, specifically as used in identification documents. Under S.B. 682, the Identity Information Protection Act of 2005, it would be a misdemeanor for "...a person or entity that knowingly or willfully remotely reads or attempts to remotely read a person's identification document using radio waves, without the knowledge of that person..." One piece of federal legislation proposed by Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) was the RFID Right to Know Act of 2003, which mandated the "labeling of RFID-enabled products and consumer privacy protections (CASPIAN 2003)." A recent successful attempt at passage of RFID legislation is a law in Wisconsin (Assembly Bill 290) banning the forcible implantation of RFID chips in humans.

Bruening of the Center for Democracy & Technology agrees that addressing privacy "at the outset of the development process" rather than after deployment "is more effective and efficient (Bruening 2004)." However, Bruening argues that "to enact legislation specifically for RFID would risk technology mandates that are ill-suited to the future evolution of the technology." Therefore another legislative approach would be to consider "technologically-neutral baseline privacy legislation." According to Bruening (2004) this type of legislation "would ensure that retail and marketing uses of the technology in conjunction with personal information were bounded by fair information practices." Bruening (2004) outlines some of the common elements of fair information practices that would apply to RFID technology including:

- *Notice:* Information collection and use should be open and transparent.
- *Purpose specification:* Personal data should be relevant to the purposes for which it is collected.
- *Use limitation:* Data should be used for only the purpose for which it was collected.
- *Accuracy:* Personal data should be accurate, complete, and timely.
- *Security:* Personal data should be protected by reasonable security safeguards against risk of loss, unauthorized access, destruction, use, modification or disclosure.
- *Access:* Individuals should have a right to view all information that is collected about them to correct data that is not timely, accurate, relevant or complete.
- *Accountability:* Record keepers should be accountable for complying with fair information practices.

EPIC (2004a), among others, has addressed the application of similar OECD Guidelines to RFID technology. In addition to applying these guidelines, the RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (CASPIAN et al. 2003) also suggests the need for a technology assessment by a neutral party, a process that is "multidisciplinary, involving all stakeholders, including consumers," as well as a statement of what practices are to be barred, such as human tracking or using the technology so as to "eliminate or reduce anonymity."

When initially considering application of fair information practices to simple RFID data collection systems, there does not appear to be a good fit (Weinberg 2004). Data collection can be performed by anyone, whether or not the intended user, and absent reader detection devices, the individual with tagged items most probably would not be aware of the collection taking place. For fair information practices to work well there must be "clearly identified data collectors." However, for "systems in which devices blab information indiscriminately," it's hard to identify the collectors so as to enforce rules against them (Weinberg 2004). This leads to several ideas on how to approach RFID regulation. One idea is to apply Fair Information Practices specifically to the linkage of personal identifying information to the tag data. The other is to restrict readers from data collection by barring reader use unless a warning is provided, by example requiring readers to emit a tone, light or other such indicator of reader activity (Weinberg 2004; Garfinkel 2002).

Garfinkel (2002) proposes an "RFID Bill of Rights" which applies principles originally set out in the Code of Fair Information Practices (HEW 1973) to RFID technology. Garfinkel's Bill of Rights (2002) includes five guidelines for RFID systems:

"Users of RFID systems and purchasers of products containing RFID tags have:

1. The right to know if a product contains an RFID tag.
2. The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
3. The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to

travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's "kill" feature.

4. The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.

5. The right to know when, where, and why an RFID tag is being read."

EPCglobal, one of the two main groups setting RFID standards, has created "Guidelines on EPC for Consumer Products" (EPCglobal 2005) which reflect to some extent Garfinkel's RFID Bill of Rights recommendations. However, according to Garfinkel (2004), the "guidelines are significantly watered down" from those which he proposed. For instance, although the guidelines (EPCglobal 2005) state that consumers should be given notice as to which products or packaging contain an EPC tag, there is no mention of the consumer's right to be notified of the presence of a reader, when a tag is being read, or specifically why the tag data is being collected. Also, according to Guideline 2 (EPCglobal 2005), "...consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire..." It does not say that consumers have the right to discard, remove, or deactivate tags, only that consumers are to be informed of the available choices, whatever they may be (Garfinkel 2004).

International concern regarding the potential for linking RFID-tagged items with personal information led to adoption of the Resolution on Radio-Frequency Identification by the International Conference of Data Protection & Privacy Commissioners on 20

November 2003. This resolution (Rotenberg 2003) states that the "basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular

a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;

b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way;

c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as necessary to achieve (or carry out) this purpose, and

d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags."

Within the European arena, the EU Data Protection Directives 95/46/EC and 2002/58/EC should provide some protection of personal data collected through RFID technology. According to Cedric Laurant (2004), Policy Counsel for the Electronic Privacy Information Center, these directives apply to "...individual tracking and the association of data with personal identification. As a result, any use of RFID tags that involves the processing of personal data is likely to be subject to a number of data protection obligations." However, as concluded by the National Consumer Council's (Lace 2004) summit on the future of RFID technology in retail, "...some in-store uses of the technology may concern consumers, but not involve their personal data, so the Data

Protection Act would not provide protection." Another NCC summit finding related to the danger of marginalization of consumers from the RFID debate, so that they would not have a say in "whether and how RFID developed and was implemented (Lace 2004)."

The Working Document on Data Protection Issues Related to RFID Technology (WP105) was created by an EU advisory board, Article 29 Data Protection Working Party (2005), with two stated purposes: to provide guidance to those deploying RFID technology so as to apply the basic principles set out in EC Directives 95/46/EC and 2002/58/EC, and to provide guidance to manufacturers of RFID technology in addition to standardization bodies as to "their responsibility towards designing privacy compliant technology in order to enable deployers of the technology to carry out their obligations under the data protection Directive [95/46/EC]." In addition to the requirement under Article 10 of the Directive, that data controllers provide information to data subjects such as controller identity, processing purpose, data recipients, and a right to access data, the Working Party 29 suggests that, "depending on the specific use of RFID, the data controller will also have to inform individuals about: (v) how to discard, disable or remove tags from the products, thus preventing them from disclosing further information and (vi) how to exercise the right of access to information." The Working Party stated regarding RFID interoperability, that it may "have some negative side effects for data protection unless appropriate measures are taken. For example, the principle of purpose limitation may be more difficult to apply and to control. Moreover, the management of access rights regarding privacy might also become more critical as the number of actors manipulating the data will increase." Working Party 29 felt that in the future additional guidance "will be particularly necessary if RFID technology becomes, as expected, one

of the main "bricks" of the future ambient intelligence environment (Article 29 Data Protection Working Party 2005)."

The Trans Atlantic Consumer Dialogue (TACD 2005) issued the Resolution on Radio-Frequency Identification (RFID) in April 2005, providing recommendations to the EU and US governments. Some of these recommendations included funding research relating to RFID impact on consumers, consulting "with all RFID stakeholders, including consumer organizations and independent academic researchers," and monitoring "whether RFID is being used in anti-competitive ways (TACD 2005)."

In June of 2004, Japan's Ministry of Inner Affairs and Telecommunication and the Ministry of Economy, Trade and Industry issued the Guidelines for Privacy Protection on Electronic Tags (Natsui 2005). These guidelines include the right of consumers to de-activate tags and entrust businesses with the responsibility of notifying consumers of de-activation procedures through explanation, posting, or inclusion of the information on products or packaging containing a tag. Also, consent from the data subject must be obtained before a use of tag data other than the original stated purpose or before release of tag information to another entity. In addition the guidelines encourage the education of consumers on RFID technology through business and governmental agency efforts (Natsui 2005).

In the comments of the FTC Workshop on Radio Frequency Identification, EPIC (2004a) enumerated its recommendations regarding RFID technology to the FTC. These recommendations included: setting guidelines for the "private manufacturing and retail sector" and establishing standards for users; requiring a technology assessment and deciding whether specific legislation is called for; focusing attention on the Object Name

Service (ONS) RFID database system, since "abuse of data in the ONS could severely endanger the personal privacy of millions of American citizens"; and publishing and disseminating "documents that educate the general public about RFID technology and with the purpose of educating businesses about the importance of protecting consumers' privacy." Also provided by EPIC (2004b) was the Guidelines on Commercial Use of RFID Technology, with prohibitions against tracking individuals and snooping through the reading of tags on or with individuals, so as not to generate consumer profiles, even if they are assigned anonymously. Also prohibited is the coercion of consumers to leave the tags functioning in order to derive certain benefits otherwise not available including "...warranty tracking, loss recovery, or compliance with smart appliances (EPIC 2004b)."

Whatever guidelines or recommendations are followed, if the RFID industry does not voluntarily adopt standards that pacify the concerns of consumers and privacy advocates, it is likely these groups will demand regulations on this technology. Garfinkel (2004) feels there is the danger that "high-handed actions on the part of RFID-advocates will likely empower consumer activists and their legislative allies to pass some truly stifling legislation." This reaction could serve to greatly limit or postpone many potential applications of this technology in the near future. As Plichta (2004) says, "a balance must be struck between a laissez-faire approach that might let tracking information abuse run amuck and a government regulation approach that might stifle this economically and technologically beneficial technology." In his proposed guidelines prepared for the Electronic Privacy Information Center, Plichta (2004) specifies three areas to consider in meeting this balance: Duties of a User Employing RFID Systems That Do Not Gather Data About Individuals; Duties of a User Employing RFID Systems That Can Gather

Personal Data About Individuals; and Rights of an Individual When RFID Systems Are Used. Specifically relating to location privacy is the guideline that the user of an RFID system will not "track the movement of individuals via tagged items." That user should also not "record or store tag data from tags that do not belong to the user, or from tags that have been already purchased (Plichta 2004)," which would serve to limit somewhat the continuous acquisition of consumer data from tags and prevent an all-out invasive personal search by RFID readers every time one entered an RFID equipped grocery store for instance.

According to Plichta (2004), the "most sound approach to addressing privacy concerns will have to examine each kind of tracking within a specific context, and a context that is developed enough to provide concrete, substantive solutions to burgeoning privacy risks." His feeling is that general guidelines may work for now, as they "provide an approach that is at the same time not over-inclusive, because it does not brush over the unique issues within each context, and not under-inclusive, because it deals, on a general level, with issues that come up (to some extent) within each context." With advances from current "speculative" to future "concrete" scenarios of RFID use, however, the need to deal with privacy concerns arising within certain contexts through more specific regulations may be necessary (Plichta 2004).

5.1.3 Evaluating Legal Approaches

One major problem faced in the regulation of evolving technology is that laws often lag behind rapid advancements in the technology. Ideas that seemed unthinkable or "far-fetched" in the recent past may occur quickly. As Barry Steinhardt (2004) remarks,

"if we at the ACLU have learned anything over the past decade, it is that seemingly distant privacy invasions that sound right out of science fiction often become real far faster than anyone has anticipated." It is especially difficult to legislate for possibilities that may not even have been envisioned yet. However, if a technology is saddled with too much regulation early in its development, this may impede creativity and progress within the field.

The various legal approaches mentioned in the previous section have not worked so far in a U.S. context for related areas. U.S. privacy laws have tended to focus more "on industry-specific uses of information, like credit reports or medical data, rather than on protecting the privacy of the individuals in the databases" and therefore are unable to effectively deal with increasing data mining techniques (Zeller 2005). The U.S. has been reluctant to provide many controls within the location privacy arena or even regarding data mining, although recent data security breaches that put at risk the personal information of tens of millions of individuals have given rise to increasing proposals of personal information privacy legislation. Time will tell whether any real privacy protections will be enacted.

Business concerns tend to triumph over consumer privacy concerns within the U.S. Along with the possibility of little or no additional privacy legislation; there is also the danger that U.S. businesses may themselves some day insist on legislation for specific technology such as RFID, demanding legislative protections against disabling or deactivating tags for instance (Rotenberg 2003). As the full import of RFID technology becomes apparent and even more uses are discovered in the future, businesses likely will

fight hard to retain or regain control of the potential information gold mine associated with use of RFID technology.

"Opt-in" approaches to privacy protection are probably unworkable in the current pro-commercial speech legal climate existing in the U.S. The court held in US West Inc. v. FCC (1999) that the FCC's interpretation of 47 U.S.C. §222 as requiring explicit customer consent before third party disclosure of customers' personal information was a violation of the First Amendment right of free speech. Use of customer information in commercial transactions was considered commercial speech and therefore protected by the First Amendment (White 2003).

Previous sections have discussed the idea of applying fair information practices in the use of RFID technology. There was some question as to how well this would work. One problem arises in considering the initial purpose in collecting data and the subsequent use of that data, dealing with the practices of *purpose specification* and *use limitation*. A group or individual could be collecting data over an extended time period trying to find correlations between individuals and events, for example general surveillance data to facilitate the link between individuals and certain crimes. If this were the case, the initially stated purpose could last indefinitely, with no time limit on data collection, or on the use and retention of the collected data. In order to make inferences from the data and to include updates so as to allow new inferences, continuous data collection would be necessary.

In order to enforce the principle of *notice* it is essential to know who is collecting the data. The issue involves not only who ultimately owns the data, but also who has access to or control over it. Control over tag data may depend in part upon the context of

tag ownership. As ownership relates to RFID-embedded personal products, the user may have total control of all tag functions, whereas in the context of a rented item, the user might only have the right to read a tag (Weis 2003). If anyone can collect data, for instance through rogue readers either skimming tag data or eavesdropping on communications, then there seems little hope of enforcing the notice principle. Since readers could be hidden almost anywhere, there would be unlimited opportunity to collect data and no way of knowing if it is even being done, unless notice is provided or a device capable of detecting reader activity is possessed.

Also inherent in ownership uncertainty is the question of who will be responsible for following the fair information practices of *security*, *access*, *accuracy*, and *accountability*. This is important considering the staggering amount of data that may potentially be generated by RFID readers. According to one estimate Wal-Mart alone may generate over seven terabytes of RFID data each day once the technology has been deployed within its stores (Laurant 2004). For EPCglobal tags embedded within items such as consumer products and packaging, the plan is to store the tag data, data that perhaps spans the life of a tag, within the ONS, a database system accessible through the Internet. According to Cedric Laurant (2004) of the Electronic Privacy Information Center (EPIC), "if information in this database is associated with personally identifiable information, the potential for abuses of consumer data and individual privacy will dwarf any technology previously in use." This is especially of concern as security breaches relating to personal information are on the increase and become ever more lucrative.

Acceptance of "voluntary industry-approved privacy" standards has been proposed as one privacy solution. However, as Garfinkel (2004) says, the "problem is

they're voluntary, businesses don't have to comply with them." But if there were a strong enough incentive to do so, that might change industry thinking. According to Morgan and Newton (2004), one way to provide privacy and anonymity protections for technology systems is to "promote the growth of effective system design standards." After development of performance standards, if system designers were persuaded to follow these "as a matter of good professional practice," and certification was developed to identify businesses that were complying with the standards, then these standards for best professional practice and certification, which had proved their worth, might become law (Morgan and Newton 2004). According to Morgan and Newton (2004), "if laws were passed that limit the extent and circumstances under which persons and their actions could be identified via automated systems in public places, and this information shared with others, then this would provide a basis for parties to sue system operators, providers, and designers when abuses occurred. That, in turn, would create a strong incentive on the part of designers to design systems in which abuse was difficult or impossible."

Attempting to regulate the collection, processing, storage, and use of RFID data to prevent abuse of personal information is a formidable task. The preceding information has shown that as respects location privacy, and especially as relating to RFID technology, fair information practices may be hard to enforce, and other legislative, regulatory, or guideline approaches to protecting personal privacy do not wholly work.

Table 1. Summary of legal approaches to RFID-related privacy protection.

Legal Approach	Potential Problems	Current State of Implementation or Support
Industry guidelines	If voluntary, cannot force businesses to comply Without incentives to do so, businesses may not want to comply	RFID guidelines have been created in the U.S. and various other countries, but are not widely implemented
"Opt-in" policy	Unworkable within current U.S. pro-commercial speech climate	Past attempts were ruled as violating U.S. corporate free speech rights
Technologically-neutral baseline privacy legislation	Provides only a minimum level of protection One-size-fits-all approach	U.S. law focuses more on protecting specific privacy invasions and does not generally support baseline privacy legislation
RFID specific privacy legislation	Excessive early regulation can stifle creativity and growth in the field Laws often lag behind rapid advancements in technology Enforcement of a law may not be possible without enabling technology	Numerous U.S. states are considering or have attempted to pass RFID legislation (e.g., Wisconsin has banned the forcible implantation of RFID chips in humans), however, most attempted laws have failed to pass

5.2 Technological Approaches

Numerous solutions for providing location privacy through technological means have been proposed. This section provides an overview of some of these approaches, both as to location privacy in general and specifically relating to RFID technology. The section also evaluates the technological methods of protecting privacy, as well as discusses how to promote privacy considerations during the design stage.

5.2.1 General Location Privacy

Duckham and Kulik (2005) recommend obfuscation as a means of privacy protection. Obfuscation involves degrading information quality. Their framework attempts to balance "an individual's need for high-quality information services against that individual's need for location privacy," recognizing there is a tradeoff between the two. The "obfuscation architecture allows an individual to connect *directly* with a third-party location-based service provider, without the need to use a broker or other intermediary," for example a cell phone company (Duckham and Kulik 2005).

Gruteser et al. (2003) suggest an approach where data is anonymized within the sensor network before storage. Therefore, the opportunity for misuse of the data by service providers or others who may gain unauthorized access to the stored data is minimized. System design includes a hierarchy of sensor nodes, with anonymity by means of cloaking either the node ID or the data obtained from the node. So an individual's exact location could be known but not his identity, or his identity could be known but not his exact location.

The system proposed by Beresford and Stajano (2003) operates by changing user pseudonyms when entering into a *mix zone* from an *application zone*. A *mix zone* for a specific group of individuals is "a connected spatial region of maximum size in which none of these users has registered any application callback," whereas an *application zone* is "an area where a user has registered for a callback." The privacy level provided by a particular mix zone at any one time depends in part on the size of the *anonymity set*; the *anonymity set* being defined as "the group of people visiting the mix zone during the same time period." The smaller the *anonymity set*, the lower the privacy level that is available. Users are able to choose the minimum set size at which they will agree to release location updates.

One problem with user pseudonymity and anonymity is that even though an individual's identity may not be directly linked to location data, through data mining identity may be inferred (Duckham and Kulik 2005). If records are retained for extended time periods, allowing tracing of past routes – to home, work, etc. – patterns will become discernable and from these identification may be possible (Zevenbergen 2004). Although anonymity may be desirable, as Langheinrich (2002a) states, "unless we want to abandon our current social interactions completely and deal only behind digital pseudonyms in virtual reality with each other, we must realize that our real-world presence cannot be completely hidden, nor perfectly anonymized." In fact, applications that required authentication and personalization would be difficult in the face of anonymity (Duckham and Kulik 2005).

Langheinrich (2002a) offers the privacy awareness system (*pawS*), composed of a device, the *privacy assistant*, that can detect sensors operating and collecting data within

an area and a privacy-aware database (*pawDB*) that stores the collected data. This system is a "privacy-enabler" not a "privacy protector." It operates based upon a principle similar to one used by democratic societies: "to give people the ability to respect other people's safety, property, or privacy, and to rely on corresponding social norms, legal deterrence, and law enforcement to create a reasonable expectation that people will follow such rules." The system is "targeted at ubiquitous computing environments that allows data collectors to both announce and implement data usage policies, as well as providing data subjects with technical means to keep track of their personal information as it is stored, used, and possibly removed from the system." The privacy policies are based on a P3P set up. Users are able to set their own privacy preferences using a language such as APPEL, these preferences are automatically compared to the privacy policy of a service or data collector, so that acceptability can be determined or the user can be prompted for a decision if one cannot automatically be made (Langheinrich 2002a).

The system proposed by Myles et al. (2003) employs LocServ, a "middleware service that lies between location-based applications and location-tracking technologies" and which allows use of various positioning technologies. Their system uses policy language that extends the P3P language. Unlike P3P, the system "does not require policies to specify the data to be collected, because the system can determine it from the associated query." The system differs from Langhenrich's pawS system in that "pawS lets users protect their privacy at the moment of information capture, typically when they access a service or enter a new geographic space," whereas this system "attempts to provide privacy checks at the moment of information release – that is, when an

application makes a solicited or unsolicited request for location information (Myles et al. 2003)."

5.2.2 RFID Specific

Due to the limited computing ability of passive RFID tags, it is difficult to apply security protections like encryption. However, according to Juels (2006), the very simplicity of RFID tags is one reason that technological methods can be employed in protecting privacy with this type of technology. Unlike the vulnerability of a computer with Internet access and employing various software applications, "an RFID tag interacts with external devices in a constrained manner" and being without software "it draws on a small set of fixed protocols for communication (Juels 2006)." Some of the proposed technological approaches to RFID-related privacy protection are outlined below.

5.2.2.1 Tags with Pseudonyms

According to Juels (2006), to lessen the threat of tracking, rather than containing a single unique ID, tags could hold a few "unlinkable" IDs or pseudonyms, perhaps responding with a different pseudonym at each scan. So two scans, one at each end of a street or mall, would produce two different ID numbers, thereby limiting the ability to track an individual as she moves through her daily activities. Depending on the spacing of readers and the number of individuals within that specific area at one time, it may be fairly easy to infer that the pseudonyms are linked to the same tag. Also, if all the pseudonyms could be "harvested" through "repeated, rapid-fire scanning," this privacy protection technique would fail. One solution would be to put a delay circuit into the tag,

so as to delay the transmission of a new pseudonym for several minutes after the tag is scanned (Juels 2006).

5.2.2.2 Faraday Cage

Use of a Faraday cage to shield a tag from reader interrogation has been offered as a possible means of protecting tag data. This involves encasing a tag in material like metal foil or mesh, thus protecting the tag from the reader's radio signals (Juels et al. 2003; Bono et al. 2005). A problem with Faraday cages or shielding is the temporary nature of the device. A tag is only protected from a reader's interrogation as long as it's inside the shielding material. Shielding is also not practical for many applications. For instance, shielding material cannot be worn over clothing with embedded tags (Working Party 29 2005). It would also not prevent "passive eavesdropping (Bono et al. 2005)."

5.2.2.3 Hash Functions

One fairly low-cost approach to RFID tag security, and potential privacy protection, is the use of a one-way hash function for controlling access to tags. One-way hash functions are difficult to invert and therefore may prevent tag reading by unauthorized readers. The owner can lock a tag by choosing a random key, computing the key's hash value and storing it as the tag's metaID, which is then stored along with the key in a backend database (Sarma et al. 2002; Weis 2003; Weis et al. 2003). Though spoofing may not be avoided in this method, it may at least be detectable. Hijacking of tag data is possible when the tag is "unlocked." There is also a potential for tracking people since the metaID serves as a tag identifier (Weis 2003). Weis et al. (2003) suggest

the possibility of equipping tags with a "random number generator" along with a one-way hash function to provide additional protection of tag data.

5.2.2.4 Killing, Recoding, and Overwriting

In order to facilitate some of the privacy rights outlined in his RFID Bill of Rights, Garfinkel (2002) suggested incorporating a "password-protected 'kill' feature" into the tags, a feature now incorporated into EPCglobal's Class 1 Gen 2 tags. Since the use of a standardized password could lead to an attempted killing or erasing of the unique serial numbers of all RFID tags within a store, systems to sense such activity could be employed. Informing consumers of the use of a reader could be accomplished by a prominently displayed written notice, or by having the reader or tag emit a flashing light or tone (Garfinkel 2002; Weinberg 2004). In addition, if consumers possessed "reader detectors" that included real-time clocks and positioning technology like GPS, non-compliant RFID system users could be identified (Garfinkel 2002). Weis (2003) suggests that RFID-enabled cell phones and PDAs could be used to "monitor, log and filter all read attempts." Nokia has now developed a cell phone containing an RFID reader, which according to privacy advocates may provide a "check against RFID tag deployment," not to slow deployment, but to "give individuals the power to read tags, and to know exactly what information is being stored (Weiss 2004)."

The Electronic Frontier Foundation (2005) also advocates use of the kill feature, but goes further in suggesting it should be mandatory for consumer products at the point-of-sale. As the EFF (2005) states, "in the complete absence of a common pool of knowledge about RFID technology, the privacy-invasive practices it enables, and the

resources necessary to combat abuse, the only effective stopgap measure for protecting privacy is a "default setting," or architecture, that supports it," namely, mandatory tag killing.

A number of concerns arise regarding the use of a kill command with RFID tags. One is that it prevents any further use of the tag, either in a commercial sense or possibly even the functionality of the tagged item altogether. The RFID Position Statement (CASPIAN et al. 2003) articulates a number of other concerns, one being that consumers may be forced to choose between retaining privacy through the killing of tags and receiving certain benefits and discounts by keeping the tags operational. If it is inconvenient to kill tags, the consumer may effectually be prevented from disabling them, whether or not there is an option to do so. Even though tags may be killed at the time of sale, this still allows for in-store tracking. Also, it may appear that tags have been "killed," but they may in fact only be "asleep," and have the potential to be reactivated at a later time. In addition, governmental action based on security threats could lead to the removal of a "kill" option for tags all together (CASPIAN et al. 2003).

An additional issue related to the kill option arises in applications that involve borrowing or renting items containing a RFID tag, such as use by libraries or video stores (Molnar et al. 2005). The RFID tag is needed at the time of item return, so should not be killed at the time of borrow or rental. Customer records for video stores and libraries are legally protected since they admittedly pose a substantial privacy risk, but if the tags are not de-activated and reading of the tags is possible outside the library or store walls, "the spirit of these laws can be completely circumvented (Molnar et al. 2005)." Molnar et al.

(2005) propose "recoding" or overwriting a tag's ID with a new number "when it changes hands."

Another possible technique is to simply overwrite tag data with zeros (Working Party 29 2005.) However, while the tag will only reply to the reader with zeros, the fact that the tag replies at all to a reader may itself communicate more information than a consumer may wish to convey. Tags are being embedded into more expensive items to begin with, thus allowing potential thieves to easily locate more lucrative targets, in cloakrooms or parking garages for example. One other consequence of overwriting tags is that "as RFID tags become more numerous, shops may dislike all those tags that respond to queries, but return junk data (Working Party 29 2005)."

5.2.2.5 Signal-to-Noise Measurement

Fishkin and Roy (2003) propose that tag response to reader queries be dependent upon the distance a tag is from a reader. They have shown that the distance from a tag to a reader can be approximated by measuring the signal-to-noise ratio of a reader query. If the circuitry to measure signal-to-noise ratio were incorporated into the tag a distance threshold could be set beyond which the tag would not provide any response, it might transmit its ID number when within a specified distance, or it might require a shorter distance before reacting to a kill command. Spoofing may be possible if a reader varies its broadcast power, simulating shorter or longer read distances (Juels 2006).

5.2.2.6 Blocker Tags

Another approach to privacy protection is "active jamming" through a mobile device that constantly broadcasts signals to disrupt reader operation. One major drawback is the potential to disrupt all reader activity within the locale of the jammer device, including those for applications not of concern to a user (Juels et al. 2003). Instead, Juels et al. (2003) suggest "passive jamming" through use of a *blocker tag*. The blocker tag can simulate all possible tag serial numbers, called a *universal blocker*, or simulate only certain subsets of serial numbers, known as a *selective blocker*. Weis (2003) had previously discussed a device to "mimic" tags that might enable the attack of an inventory-control system.

Tag simulation is accomplished through interference with the singulation protocol that allows a reader to communicate with a single tag. Used in this case is the "tree-walking" singulation protocol which permits a reader "to identify the serial numbers of nearby tags individually by means of a bit-by-bit query process resembling a depth-first search of a binary tree (Juels et al. 2003)." A selective blocker seems more appropriate for consumer use, since a universal blocker would lead to "indiscriminately disrupting" all readers within an area. Each designated *privacy zone* "consists of a restricted range of tag serial numbers targeted for protection (i.e., simulation) by a selective blocker tag." Singulation, in this case accomplished through a tree-walking algorithm, is disrupted by the blocker tag once it enters an area designated as a privacy zone (Juels et al. 2003).

One good point about blocker tags is the fairly low implementation cost (Juels et al. 2003). Little modification would be required to the one or two standard RFID tags used to make a blocker tag. Once the manufacturing cost of standard RFID tags reaches

five cents, blocker tag cost may be no more than 10 cents. Blocker tags do not require expensive cryptography and the password to facilitate privacy zone changes is similar to the password already available for the "kill" command. According to Juels et al. (2003), blocker tags are effectively as inexpensive an approach as the "kill" command, yet "much more flexible and useful for protecting privacy."

However, there are some drawbacks relating to the use of blocker tags. One is the potential for denial-of-service attacks through "malicious blocker tags," attempted perhaps by shoplifters in a retail setting. Denial-of-service attacks could be detected simply by setting a threshold for tag ID numbers, which once passed would indicate a malicious intent. Or tag IDs could be checked against a set range of authentic IDs through connection of the reader to a database, and if the ID fell outside the range, it could be considered fraudulent (Juels et al. 2003).

Another drawback is that "blocker tags effectively implement an "opt-out" policy", as consumers must purchase blocker tags to benefit from the protection afforded by them (Juels 2006). *Soft blocking* (Juels and Brainard 2004; Juels 2006) could allow an "opt-in" approach instead through use of *unblocker* tags. This would involve programming readers to only scan the *private zone* if an *unblocker* tag was present. According to Juels (2006), "a soft blocker tag may be thought of as a physically embodied privacy policy of sorts," likened to P3P, as it would allow a user to set privacy preferences that can be compared against a server's privacy policy. A soft blocker could be composed of a standard RFID tag whose ID number is linked to a user's privacy policy. Although the "voluntary or internally auditable" nature of the soft blocker may "offer somewhat weaker privacy enforcement" as compared to an ordinary blocker, it is

also more "flexible" in that it allows "partial or scrubbed data" to be revealed rather than the "all-or-nothing policy enforced by a blocker (Juels and Brainard 2004)."

Other potential problems with blocker tags are outlined in the RFID Position Statement (CASPIAN et al. 2003). To begin with, blocker tags "might encourage the proliferation of RFID devices by giving consumers a false sense of security." Like the kill function, blocker tags could be banned by government mandate if deemed necessary for national security, or even by stores themselves to protect against shoplifting or loss of marketing data. The ban might be limited to particular areas, or certain types of buildings such as airports. Blocker tags also put the burden of privacy protection on consumers, to remember to carry the blocker tags with them, to activate them, and to make sure they are functioning properly (CASPIAN et al. 2003).

5.2.2.7 Blinded Tree-Walking

Use of a Binary Tree-Walking anti-collision algorithm may leave tag data transmitted on the stronger reader-to-tag or forward channel open to attack by eavesdroppers located 100 meters or more away. With Binary Tree-Walking, a reader broadcasts "every bit of every singulated tag" over the forward channel. To combat the "long-range eavesdropping" potential on the forward channel, Weis et al. (2003) propose "Silent Tree-Walking" or "Blinded Tree-Walking" (Weis 2003), useful with a group of tags sharing a common ID prefix, like a product code or a manufacturer ID. Since the backward channel has a much weaker signal it cannot be monitored from as great a distance, so the tag's response to the reader over the tag-to-reader backward channel would be protected from long-range eavesdroppers. The tag could send the common

prefix to the reader as a "shared secret" over the backward channel and that "shared secret prefix may be used to conceal the value of the unique portion of the IDs (Weis 2003; Weis et al. 2003)." Close-range eavesdropping of the backward channel would still be possible. Another possibility is Randomized Tree-Walking in which pseudo-ID bits are generated and broadcast over the forward channel, although this would involve more communication costs (Weis et al. 2003).

Table 2. Summary of technological approaches to RFID-related privacy protection.

RFID Privacy Protection	Potential Benefits	Potential Problems
Tags with pseudonyms	Produces alternative RFID identifiers to limit identification and tracking	Linking of identity to a tag is possible depending upon reader spacing and number of people in the area
Faraday cage	Physical barrier blocks reader signal, preventing tag reading	Impractical for shielding tags in clothing or large items
Hash function	Tag locked by private randomly generated key which is difficult to reverse	Default of many tags is for them to be 'unlocked'
Killing, recoding, & overwriting	Privacy protected by removing or changing unique tag ID	Killing prevents future tag use Overwriting with another ID may still allow tracking
Signal-to-noise measurement	Privacy protection based on S:N which is a function of reader's distance from tag	By altering reader broadcast power, varying reader distances can be simulated
Signal jamming	Disrupts signal so reader cannot communicate with tags	Most or all reader activity near jamming device is also disrupted May be banned in the future
Blocker tags	'Passive jamming' through simulating all/subset of tag serial numbers Low implementation cost	Denial-of-service attacks by shoplifters
Blinded tree-walking	Secret tag prefix to conceal unique part of ID could be sent over tag-to-reader backward channel with weaker signal more difficult to detect	Close-range eavesdropping on backward channel is possible

5.2.3 Evaluating Technological Approaches

One advantage of technological over legal approaches is technology's ability to automatically enforce privacy measures when integrated into system design. Laws are often very hard to enforce, and if unenforceable, will not be followed by some without an anticipated return on their moral investment in compliance. However, it may be difficult to design a system so that privacy can be enforced and individuals can choose the level of privacy they desire. Privacy is subjective and therefore may not hold the same degree of concern for system designers as for consumers. The challenge comes not only in designing a system to placate the privacy concerns of consumers, but also the demands of businesses deploying RFID systems, and convincing system designers to be concerned about these issues in the first place.

5.2.3.1 Privacy by Design

Before technological solutions to privacy can be developed and applied in system design, implications of system use must be considered to determine what protections are required. There is, however, some question as to whom the responsibility to contemplate these issues belongs.

Marc Langheinrich, currently a researcher from the Institute for Pervasive Computing at ETH Zurich, visited a few European labs that design sensor-based computing systems and asked designers about the privacy implications related to their systems. According to Langheinrich, "Most said either 'It's not my business, it's the lawmakers' or 'It's not my business, because it's not my field.' Others said that if they thought about privacy, it would get in the way of building their designs." (Kumagai and

Cherry 2004) However, as Langheinrich (2001) argues regarding ubiquitous computing, "We cannot rely on lawmakers and sociologists to be fully aware of the vast possibilities and implications that the technology so obviously presents to us." According to Langheinrich (2002b), to build "systems that will respect the privacy of the individual, it is crucial to understand when it is exactly that people feel their privacy has been invaded." Langheinrich applies to ubiquitous computing Marx's (2001) personal border crossings – natural, social, spatial or temporal, and borders due to ephemeral or transitory effects – to aid in the determination of potential privacy violations.

According to Morgan and Newton (2004) "if system designers think carefully about the social consequences of alternative designs before they make their choices, then the potential for negative social consequences often can be dramatically reduced or eliminated." They outline a list of principles to be considered in designing systems involving collection of information relating to individuals within public space.

In designing ubiquitous computing systems, Hong et al. (2004) propose the use of "privacy risk models as a way of refining privacy from an abstract concept into a set of concrete concerns for a specific domain and community of users." Their model is two-part. The first "is a *privacy risk analysis* that poses a series of questions to help designers refine their understanding of the problem space," considering particular issues that may arise in both the "social and organizational context in which an application is embedded and the technology used in implementing that application." "The second part looks at *privacy risk management*, and is a cost-benefit analysis intended to help designers prioritize privacy risks and develop architectures, interaction techniques, and strategies for managing those risks (Hong et al. 2004)."

As Beckwith (2003) states, "...successful design requires that we understand the desires, concerns, and awareness of the technology's users." One attempt to accomplish this was through a field study of the MyGrocer pervasive retail system (Kourouthanassis and Roussos 2003) that evaluated consumer perceptions and concerns relating to the RFID system during its design stage and before actual implementation, so that modifications could be applied.

5.2.3.2 Conclusions on Technological Approaches

As has been shown, no one technology or perhaps even combination of technologies, appears to be able to satisfy privacy concerns entirely, as different applications demand a variety of privacy solutions. Finding workable technological solutions may not be enough absent laws to enforce these technological approaches, as industry may not be inclined to make use of them. Generally businesses do what is in their best interests. If the clamor for privacy becomes loud enough, it may be in the best interest of businesses to include privacy protections, although it may take longer to implement if not required from the beginning of the design process.

Legal approaches on their own also fail to deal with the complexities of RFID technology and enforcement may be near impossible in some instances. Therefore, exploration of a combined approach to privacy protection seems appropriate.

5.3 Combined Approaches

This section discusses a proposed privacy protection approach that combines legal safeguards with technology to enforce them. The advantages of a contractual approach to

privacy will also be discussed, along with how this approach could be integrated with technology to provide autonomous control over personal information.

5.3.1 Application of Fair Information Principles in Design

Applying fair information principles to facilitate privacy protection in the use of RFID technology was discussed in earlier sections. Floerkemeier et al. (2004) have taken that a step farther and explain how some of these principles can be incorporated even at the reader-to-tag protocol level, the communication between the reader and the tag. Although many of the principles could be carried out through "non-technical means" (e.g., notice of collection through sign posting), "by incorporating such principles directly into the underlying protocol, both consumers and data collectors can more easily follow them, thus strengthening existing legal protection by providing the means to verify and thus enforce corresponding regulations (Floerkemeier et al. 2004)." Relying on technology to automatically enforce some of these principles helps to overcome consumer tendency to not take advantage of available privacy protections when it is burdensome to do so.

This approach attempts to provide transparency, so that consumers can determine not only when data collection occurs, but also identify who is collecting the data and why. To accomplish this, each reader would have a *reader policy ID* (RPID) to be included in the inventory command of the reader. This RPID would contain IDs for the data collector, the policy, and the reader. Providing information on the policy would assist in dispute resolution, allowing customers to identify which policy was used. Existing ONS architecture could be used to store and access the policy in question. The

reader's inventory command would also include fields for declaration of purpose, many of which are similar to the P3P purpose types, and collection types. Floerkemeier et al. (2004) outline fifteen purposes and four collection practices applicable in this system.

The system would work in a fashion similar to P3P. As a web browser compares personal preferences of a user against the privacy policies of a website and then automatically acts for the consumer, the reader-to-tag protocol would allow automatic decisions as to whether to release tag data when queried by a reader, based upon privacy preferences of the user. This should serve to ease consumer burden as well as providing the consumer with autonomous control over release of personal information (Floerkemeier et al. 2004).

Transparency or tag detection is facilitated through use of a *watchdog tag*, which is a standard tag including a battery, screen, and possibly a long-range communication channel. The possibility exists for incorporating this technology into a mobile phone, rather than necessitating a separate device. With incorporation of the fair information principles into the protocol, the *watchdog tag* can not only detect a reader, but can decode reader commands and display them on the screen so that a user is provided notice of collection specifics such as time and date of collection, data collector, applicable policy, reader ID and location, purpose, collection type, and target selection. The *watchdog tag* is also able to keep track of all transfers of data, enabling users to obtain summaries of the data collected on them. The data logs could be accessed through the ONS (Floerkemeier et al. 2004).

The above system provisions accomplish application of the principles of *purpose specification*, *openness*, and *accountability*. *Collection limitation* is provided through the

use of a selection mask, with the goal of targeting only the tags relevant to the current collection type. If readers were integrated into a privacy-aware database such as *pawS* (Langheinrich 2002a), the principles of *use limitation*, *data quality*, and *participation* would be implemented. Incorporating selective jamming or blocking capabilities into the *watchdog tag*, would allow a consumer to give or withhold explicit *consent*. By providing the capability to look up the reader's ID number online, a user can decide whether or not to jam the reader signals. It may also be possible to enforce the principle of *security* through incorporating measures such as cryptography into the tags, facilitating the creation of an ID certification system, and helping prevent the theft of a reader's identification string. Registration of a company's identification string would be required (Floerkemeier et al. 2004).

Several concerns arise in use of this approach. One is the cost as far as system performance. Extensions to the current protocol would have some effect on performance, but the potential time delay appears to be "within acceptable limits", varying with the data transfer rate of a system, and in some cases would be compensated for by shorter reply times due to the capability of selecting only tags of interest (Floerkemeier et al. 2004).

Another concern relates to future and unintended uses of the data collected. For instance, even though the original purpose for collection may not have included location tracking, there is still the potential for log files to be combined at a later time. Since this system allows for the identification, storage, and access to the privacy policies utilized in any one instance, this provides legal leverage for consumers to pursue non-compliance claims (Floerkemeier et al. 2004).

5.3.2 Advantages of a Contractual Approach

When attempting to provide data privacy protections Bibas (1994) suggests pursuit of the "golden mean: a solution tailored to individual preferences and values." In order to find that "golden mean" a cost/benefit analysis is important in order to balance the potential benefits to be derived from the information industry against the costs of privacy loss. The value of privacy, however, is subjective and hard to calculate. Therefore, according to Bibas (1994), "any solution should be sensitive to individual valuations of the tradeoffs involved instead of giving privacy to everybody or nobody."

A centralized approach to data privacy, whether through legislation, regulations, state constitutional rights or tort law involves a decision on potential tradeoffs made by one individual or a few, on behalf of many, providing a one-size-fits-all solution. For example, a tort approach "requires judges to balance the utility of dissemination against the value of privacy to a reasonable person...Any such uniform standard based on the preferences of a non-existent reasonable person would imperfectly assess and allocate the social costs of withholding information (Bibas 1994)."

Contracts, however, are the "branch of the common law most sensitive to individual preferences (Bibas 1994)." In the past, courts have not been overly receptive to claims of privacy invasion. Privacy is a somewhat intangible concept and very subjective. Contracts are able to provide a more concrete or tangible basis for cause of action relating to breach of privacy. Contracts are also more flexible, allowing respect for both majority and minority preferences. "Flexibility is the market's forte: the pricing mechanism is extremely sensitive to variations in valuations and quickly adjusts to them," and so "a

contractual approach, by pricing information, would thus more efficiently allocate data than would a centrally planned solution (Bibas 1994)."

"Classical" contract law does not provide a total privacy solution though, for people many times do not have the bargaining power or leverage to renegotiate standard form contracts. A single business cannot absorb all start-up costs relating to new standards and still realize "profit advantages." (Bibas 1994; Onsrud 2001) In addition, new standards may be opposed aggressively by other industry players with heavily vested interests, no matter how beneficial these standards may prove to be for society as a whole (Onsrud 2001).

Applying a contractual approach to privacy protections for location-based services, Onsrud (2001) proposes combining computer code with a uniform model contract. (Bhaduri and Onsrud 2002; Bhaduri 2003) Industry adherence to such a model contract might be gained through methods such as providing government funding for initial open source computer code by means of contracts or grants, as well as hinging eligibility for permits, tax incentives, or program funding on adherence to the model contract. This combined "standard contract/code approach" is beneficial for privacy as it would "encourage companies to collect only minimum information to perform services... otherwise many consumers would not sign up for the service (Onsrud 2001)."

5.3.3 Contractual Approach for Location-Based Services

Bhaduri (2003) believes that "it is possible to develop an approach for protecting privacy in the use of location-based services that supports the core ethical principle of autonomy of the individual." A combined technological and legal model would enable

consumers to assume control over their own location privacy, rather than leaving this responsibility to service providers (Bhaduri and Onsrud 2002). This type of approach would be preferable to laws that address specific standards, as these do not provide the flexibility necessary to allow individuals to choose their own privacy level, and "one-size-fits all privacy protection is both economically and socially inefficient since the ability to adapt to specific circumstances is non-existent (Bhaduri 2003)."

Using a model contract applied across industry, a dynamic based approach to privacy protection is possible, with consumer choice facilitated through use of a "personal communicator" (Onsrud 2001) device. This device would enable a "continuous contractual environment" (Bhaduri and Onsrud 2002) in which a consumer's personal preferences could be changed "on-the-fly", allowing her to "opt-in" or "opt-out" of these preferences at will.

Preferences may be set individually for each category relating to a particular group or entity, or even individually for each member of a group, whether a business associate, friend, family member, or other. Through menu options, users choose whom they will allow to track or communicate with them, when, and how. For example, choices can be made regarding the accuracy to which others can track the user in time and space, the acceptance of push or pull services from clients, or the granting of permission for servers to use or distribute personal information (Bhaduri 2003).

Bhaduri (2003) feels that "by providing a single contractual model for all LBS servers a level playing field is created for all users, whether rich or poor." He asserts that giving users control of their own privacy would create the desired market and therefore the desired profits required to entice the location based service industry to adopt this

model. Bhaduri envisions that many users would be willing to surrender some of their privacy in exchange for service price reductions. By including the ability to make instantaneous privacy level changes, this would facilitate dynamic pricing and billing, allowing charges to be based on time usage at a certain level or the extent of the marketing conducted at that level.

Bhaduri (2003) mentions several potential concerns relating to implementation of this model. One concern deals with the way database management systems are designed. These systems are modeled for static rather than dynamic data (Sistla et al. 1997) and therefore database system redesign may be required in order for this model to function effectively. Another concern relates to the costs associated with implementing this model, not only monetary cost, but also technical costs in terms of computational efficiency and communication. With continuous advances in the computing field, the feasibility of system implementation will increase.

Chapter 6

POTENTIAL SOLUTIONS FOR LOCATION PRIVACY PROTECTION WITHIN RFID ENVIRONMENTS IN A U.S. CONTEXT

After consideration of the current and likely near future pro-commercial speech legal climate in the United States, as well as the various proposed legal and technological approaches to location privacy protection outlined in chapter five, several potential avenues through which to pursue privacy protection in the use of RFID technology present themselves. One approach is to let technological systems that protect autonomy of the individual, by allowing individuals to continually reset their own privacy preferences, to compete in the marketplace against those systems that do not protect privacy. The problem with this approach is that the public is unlikely to become fully informed of the ramifications of their choices due to the complexity of the technologies and issues. As a result, the company that fails to protect autonomy of the individual in privacy decision-making may gain a substantial economic advantage in the marketplace. A second approach would be to pass legislation stating that companies may not link the RFID tags to any activity of the individual unless the concerned individual explicitly "opts-in" to being tracked. This approach by itself creates a very heavy corporate burden in incentivizing people to "opt-in" and is subject to constitutional validity challenges under corporate freedom of speech concepts. Further, in the past, after a party has "opted-in" the commercial sector has been loath to make it easy for the party to ever "opt-out." A third approach would be to pass legislation or create regulations that place limits on the collection of data and the use of that data by businesses or other entities. A general ban on the collection of RFID data would stifle the development of useful applications and ad

hoc legislative approaches have been problematic in providing reasonably comprehensive solutions. A fourth approach might be to develop a standard universal contract to be applied across industry, combining both legal and technological means of protecting privacy. A fifth approach might be to use a specific combination of two or more of the above options. Ultimately a recommendation is given for a legislative ban on the tying of RFID tags' unique ID numbers to individuals if they have explicitly expressed a desire not to be tracked and to ameliorate the negative impacts of this approach by developing technology to gain permission to track interactively in specific circumstances enabled through private contract law.

6.1 Legislation

Under current U.S. law, businesses and other data collectors are not prevented from reading RFID tags, enabling them to potentially link the tag's unique ID number with other personal information, as well as providing tag location and therefore personal location at that moment in time. Although numerous attempts at privacy legislation have been made at both federal and state levels, relating to data collection in general and RFID data collection specifically, passing any type of workable consumer privacy protection legislation has proven to be very difficult.

Laws specifically restricting data collection procedures are possible, but appear unlikely in the near future in the current legislative climate. By applying guidelines such as the Fair Information Principles (Federal Trade Commission) to the collection and use of RFID-derived data and including those guidelines within specific RFID legislation, location privacy protection could be enhanced. However, the Fair Information Principles

have never been imposed by legislative mandate against the commercial sector in the U.S., as contrasted for instance with European legislation. Proposed legislation such as the Location Privacy Act of 2001, discussed in section 5.1.1, would not only have required notice to customers of intended data uses of location data by location-based service providers, but would also have required an "opt-in" rule for use of the data. That is, the tracking of location of individuals would not have been allowed unless each individual expressly affirmed that he was allowing himself to be tracked. However, such an "opt-in" approach is unlikely to withstand close constitutional scrutiny, as past court rulings have supported corporate flexibility to choose among competing economic models under free speech principles.

Supreme Court decisions on First Amendment issues of free speech were not always favorable to corporations. In fact, the court reversed its original stance that the speech of corporations is not protected under the First Amendment (Valentine v. Chrestensen (1942)). Vibbert (1990) outlines the court's progression towards ever increasing corporate rights of free speech through six cases, beginning with Bigelow v. Virginia (1975) and ending with Pacific Gas and Electric Company v. Public Utilities Commission of California (1986). Based upon analysis of those six cases, Vibbert (1990) goes on to speculate that "the increasing perception of corporations as social agents with the speech rights attendant to actors (if not to individuals) seems likely." Since that time, courts have continued to rule in favor of corporate free speech, to the point of declaring in U.S. West Inc. v. FCC (1999) that all or nothing "opt-in" rules requiring consent from customers before disclosure of personal information to third parties are an infringement on free speech rights. The court found that customer information used in commercial

transactions is considered commercial speech and therefore afforded protection under the First Amendment. The strong position of the court on the issue of corporate free speech suggests that unless a constitutional amendment is created that provides a basis for "opt-in" rules or the court begins to develop a countervailing "human right" that could prevail over corporate free speech rights in the event of conflicts (Black 1997), these rules will continue to retain an unconstitutional status.

An all or nothing "opt-out" approach might be facilitated through legislation providing rights such as those outlined in Garfinkel's (2002) RFID Bill of Rights, discussed in section 5.1.2. These rights include, among others, the right of the purchaser of a RFID containing item to remove, deactivate, or destroy a tag, actions which would require knowledge that a RFID tag was present in the item to begin with. Technology could be used to enforce these rights and limit data collection without actually removing or destroying the tags. If a business can alter a tag at the point of sale to indicate that the item containing it has been sold, the technology obviously exists so that a tag could be altered to disallow tracking of the purchased item. Altering a tag might include the option of never being tracked, by "killing" the tag outright, or perhaps being able to set the tag to "sleep" mode, so that it can be reawakened for use by the individual when and if she so desires. There is also the possibility of designating the tag as allowing tracking or not allowing tracking, perhaps by overwriting a default number that is stored in the tag's memory. The number could be overwritten at the time of purchase through use of a device or machine located within the store or at any time by an individual if she possessed a device allowing her to alter the tag. Or, the device could simply overwrite the unique portion of the tag ID number so that only general (i.e. a jar of Acme strawberry

jam) and no specific identifying data (i.e. this unique jar of Acme strawberry jam) was stored in the tag. Industry itself could provide the means for deactivating tags without being forced through legislation. IBM has introduced the "clipped tag" designed so that the antenna can be scratched off, torn off along perforated edges, or peeled off (IBM 2005). The drawback of destroying tags is that consumers would thereby also lose the substantial benefits of RFID tags for their own personal use. All or nothing approaches seem very inefficient from both economic and technological perspectives.

6.2 Assumptions Regarding Future RFID Environments

Although RFID technology is currently being employed in numerous settings, particularly in supply chain management, full scale deployment into many commercial and noncommercial sectors is still a future event. At present there is no way to know exactly in what form or to what extent the implementation of RFID technology will occur in the future. Without this knowledge it is necessary to make some assumptions regarding a future RFID environment.

One assumption is that RFID tags will be embedded within most, if not all, consumer products in the near future. As the benefits of RFID technology become clearly apparent to businesses, no doubt more businesses will invest in RFID implementation. In some cases, a supplier's customer base may depend upon whether the supplier decides to employ RFID technology, such as suppliers to the U.S. Department of Defense or Wal-Mart. If the potential exists for massive data collection through myriad tags, the likelihood of increased attempts to collect, record, and aggregate the data is high, perhaps resulting in the installation of myriad RFID readers throughout our daily environment. If

this occurs, attempts to control the data collection are also likely. Were RFID technology implementation to unfold in this manner, it is not difficult to envision a world where RFID readers are located on every street corner and at every building entrance, and RFID signal jammers are carried by almost every person. If the demand for privacy protecting technology became great enough, the cost of such devices as jammers could become quite affordable to the general populace, and would likely be a very desirable acquisition and carried on key chains or included as features on cell phones. In turn, the proliferation of jamming devices would likely motivate the market to seek out a universal contract model solution in order to allow the collection of data not otherwise obtainable. Alternatively, companies might seek legislation banning the use of jamming devices. If data linking is limited through establishment of a Do Not Link Registry, an incentive is created for market acceptance of use of a standard contract model to allow users to "opt-in" and "opt-out" on-the-fly.

Another assumption, based on past experience and the current data collection frenzy, is that at some point the majority of RFID systems will become interoperable. Currently each business may implement their own RFID system, based on their particular needs. Many companies are merely trying to get a system up and running and may be more concerned with cost than ensuring their system is compatible with other systems. With the potential for massive amounts of data to be collected through RFID tags, it is in the interest of businesses to have access to as much data as possible. So although these systems may not initially be set up as interoperable, and the current focus of individual businesses may not be on interoperability, past lessons indicate that interoperability is a likely reality for the future.

This is exemplified through the rise of the Visa corporation from the midst of the "self-destructive" credit card industry of the late 1960s to an immensely successful member corporation today. In the 1960s banks began franchising credit cards to licensee banks around the country, and those licensees, in an effort to compete against each other, issued massive numbers of credit cards, with the result that "fraud was rampant, and the banks were hemorrhaging red ink (Waldrop 1996)." In an effort to stop the hemorrhaging, Dee Hock, the newly appointed CEO of National Bank Americard, Inc. (later Visa International), implemented his vision for a "chaordic" organization, one that encouraged "as much competition and initiative as possible throughout the organization – "chaos" – while building in mechanisms for cooperation – "order" (Waldrop 1996)." So while banks were competing for customers, they also had to cooperate on issues such as implementing a set of common operating standards and a standard card layout, enabling merchants to "be able to take any Visa card issued by any bank, anywhere." "This harmonious blend of cooperation and competition is what allowed the system to expand worldwide in the face of different currencies, languages, legal codes, customs, cultures, and political philosophies (Waldrop 1996)." Likewise, although RFID can provide undeniable benefits to a particular business even without interoperability, the potential increase in benefits to the commercial sector as a whole will push for compatible systems. To design RFID systems and tags for interoperability, common standards are required. This becomes an issue when comparing U.S., European, and other countries' RFID technology. Currently EPCglobal specifications are not compatible with ISO standards. However, work on integrating EPCglobal specifications into an ISO RFID standard has begun and is supported by the Department of Defense (DOD 2006), who

along with Wal-Mart is requiring suppliers to employ RFID technology. Movement towards global interoperability of RFID technology is under way through deployment of the new EPC Class 1 Gen 2 RFID technology, creating the potential for tracking tags from the U.S. throughout Europe (ByteandSwitch 2005).

While the EPC Class 1 Gen 2 standard does include access-controlled memory requiring a password or PIN to read and write to some memory locations, this is an optional feature. Due to the added expense of this feature, many businesses will no doubt opt not to include this capability on their RFID tags. Additionally, EPC tags "release their identifiers and product information - known as EPC codes – in a promiscuous manner. Any reader may scan any EPC tag; no access control exists on EPC codes (Bailey and Juels 2006)." Data can be stored on tags in an encrypted form, however, the Gen 2 standard does not provide for encrypting data being transmitted from tag to reader. According to Juels of RSA Laboratories, the small size of the Gen 2 chip makes secure cryptography for Gen 2 tags doubtful (O'Connor 2005). Even when the capability to control access to or lock certain areas of chip memory exists, these areas may not be locked due to a lack of understanding of chip functioning on the part of business users or because of the frequent need to update the stored data, leaving the chips "open to hacking (Newitz 2006)."

6.3 Combined Legal and Technological Approach: "Opt-In" Versus "Opt-Out"

Assumption 1: An extension of the current development directions of RFID technologies indicates that anyone with an RFID reader will be able to read most passive RFID tags. Currently, most passive tags are not encrypted and the market for growth in

their usage suggests that the greatest economic benefits will come from their continued open access (e.g. GPS – There was a time when only surveyors and the military used the system because it was "closed").

Assumption 2: Every surveillance camera in the future will have a built in RFID reader. Technologically it will be possible to match up the tags sensed with the specific person that purchased the items.

Assumption 3: A large proportion of the population would like to be able to control which RFID tags may be linked to their identity, tracked over time and under what circumstances. That is, RFID tags that they carry with them in the clothes or other items that they have purchased.

Research Question: Assuming this emerging technological environment, how might this control by each individual be implemented legally and technologically?

6.3.1 Mandating "Opt-In"

Under this approach a federal law would be passed stating that no individual, organization or agency may link data from an RFID tag to any individual without the express and explicit permission of that individual.

Analysis: Such laws have been passed by Congress in the past and held to violate corporate free speech rights. Unless the U.S. Supreme Court changes direction, the only way to override their previous rulings would be to pass a constitutional amendment. An amendment highly likely to allow the imposition of "opt-in" laws on the corporate sector might read as follows:

> Human Rights Amendment: Humans shall have a right to life, liberty and the pursuit of happiness while corporations and other legally constructed entities shall not.

If a large majority of voters and legislators found privacy to be supportive of their well-being and happiness, the free speech rights of corporations would be insufficient to override these constitutional rights of humans and "opt-in" legislation would clearly be constitutionally supported. The likelihood of a U.S. constitutional amendment clearly evoking human rights over corporate rights in the near future is doubtful.

6.3.2 Do Not Link Registry: "Opt-Out" Options

Another possible way to facilitate control over the collection and use of RFID data is through a means similar to the National Do Not Call Registry (FTC 2005) established under regulations created by the Federal Trade Commission and the Federal Communications Commission. The goal of such a Do Not Link Registry would be to provide individuals an efficient method for "opting-out" of having their actions monitored without their permission, an approach that has been held to not violate corporate free speech rights. The registry would probably be created and run by a government agency or NGO established for the purpose, and registration would be possible through a website, by a telephone call, or perhaps at a town office or other public office. This registry could be set up through a variety of options. The following four options are analyzed in this section:

Option 1: "Opting-Out" Completely

Option 2: "Opting-Out" But "Opting-In" When Desired by the Individual: Identity Checking by Businesses

Option 3: "Opting-Out" But "Opting-In" When Desired by the Individual: Identity Checking at Registration by the Registry

Option 4: "Opting-Out" But "Opting-In" When Desired by the Individual: Relying on Identity Checking at Registration by Credit Card Companies

Within the context of each option an exploration is carried out on how registration might be accomplished and how the purchase transaction might proceed.

6.3.2.1 Option 1: "Opting-Out" Completely

A law is passed stating that if individuals have placed their names on the Do Not Link list, companies may not link their identities to uniquely identifiable items they purchase or link their identities to other RFID observations when observed elsewhere.

6.3.2.1.1 Option 1 Registration Process

A person accesses the registry website and enters her name and address, or alternatively, calls the registry and provides this information. Upon registering, she would be assigned a unique ID number. A unique ID number would probably work better than other potential identifiers, for example a person's name. A name often does not provide a unique means of identification, and although a name and address could uniquely identify a person, address information might need to be updated from time to time. An alternate approach of registering each tag's serial number probably would not be feasible. If tags

became embedded within most or all manufactured goods, the size of the registry of tag serial numbers would be potentially massive.

Use of a unique number as an identifier may not appeal to some, as they do not want another national ID number in addition to a social security number. They may fear the potential function creep, that the unique number might be employed for uses not originally intended, as happened with the social security number. However, one company, Seisint, has already assigned a unique identifying number to every adult citizen of the United States in order to gather and link data regarding each individual. According to Poulsen, Seisint's chief technology officer, "data that belongs together is already linked together (O'Harrow 2005)."

After assignment of the unique ID number, the registrant would then choose a PIN. The unique ID number and PIN would be stored at the registry (e.g. non-profit or private organization) in order to verify an identity during a future transaction (e.g. grocery store purchase). This would be accomplished by means of comparing the PIN entered at the time of the transaction and the PIN linked to a unique ID number that is stored at the registry. To facilitate the entry of the unique personal ID number, the registry would send a card containing the unique ID number within the card's magnetic strip, similar to the ATM cards issued by banks, which could be swiped at transaction time to initiate the process of linkage prevention. Alternatively, the registry card could contain a RFID chip storing the registry ID number, which could be scanned at transaction time.

6.3.2.1.2 Option 1 Transaction Process

If using cash as payment for the transaction, the purchased items would not be linked to a specific identity. However, if using a credit card, debit card, loyalty card, or potentially even a check, an identity could be tied to the items containing RFIDs. Credit card companies might provide the option of issuing credit cards with a customer's unique ID number included within the magnetic strip of the card. Banks could do the same with debit cards issued to their customers, or perhaps even include the unique ID number on checks. The options discussed here will focus on the use of credit cards and debit cards. If a person's unique number is not included on the credit or debit card, the person would need to swipe the card issued to her by the registry. Under current practice, if using a loyalty card to obtain discounts, a person typically signs away her ability to prevent linkage to her identity with items purchased. Loyalty card agreements would still be in effect but the Do Not Link list would now prevent linking to uniquely identifiable objects (i.e. the store can record you bought a jar of Acme strawberry jam but not link your ID or name to the specific jar.)

The registry card should be swiped at the start of the transaction process, so that from the outset it would be known whether linking to the purchased object was allowed. The customer would swipe her registry card, or her credit or debit card that contained her unique ID number. She would be prompted to enter her registry PIN. The store would send that PIN along with her unique ID to the registry for comparison with the PIN and unique ID number stored there in order to verify the customer's identity. If the numbers matched, this would also serve as verification that she was currently on the registry list. Verification confirmation would then be transmitted back to the store. If on the list, the

customer's identity could not be linked to the specific objects purchased. If a company subsequently linked the tags with the person's name without the person's further explicit permission, the company would be in violation of the law and subject to civil lawsuits for actual or preferably statutory damages.

Assume later that the purchaser walks by a video surveillance camera with an RFID reader. The reader would be able to link the store at which items were purchased and what those items are, if that data was included in tag memory, but not be able to link the purchaser since the identity was never collected.

6.3.2.1.3 Potential Problems with Option 1

A potential problem arising through use of option 1 is the difficulty or even the inability to verify the identity of the person registering through the website or on the telephone. This may lead to an individual using someone else's identity to register for a unique ID number. This may not seem like a very serious problem if the only use to which the number can be put is to prevent or allow linking of purchases to a particular individual. However, if the use of these unique ID numbers was ever expanded to include a type of national ID number to supplement use of a social security number for instance, the ability of someone to register under another person's identity becomes more menacing, creating another potential means of identity theft. A person might register multiple times under false identities, whether those identities belonged to real or fictional individuals. Potential solutions could include either checking identity at the time of purchase or requiring registrants to verify their identities at the start of the registration

process. Methods for carrying out these solutions are discussed below in options 2 through 4.

6.3.2.2 Option 2: "Opting-Out" But "Opting-In" When Desired by the Individual: Identity Checking by Businesses

The second option is similar to the first but provides flexibility for the individual to "opt-in" on the fly for specific items or to receive specific services. Also, the cashier would be responsible for checking the identity of the customer that uses a registry card or credit card containing a registry ID number.

6.3.2.2.1 Option 2 Registration Process

For option 2, the registration process would involve the same steps as that of option 1. Individuals would be able to register through a website or by telephone. Each individual would enter his/her own name and address, would be assigned a unique ID number, and then would be able to choose a PIN. A registry card would be sent to the individual.

6.3.2.2.2 Option 2 Transaction Process

As with option 1, the customer would swipe her registry card or credit card containing the unique registry number at the beginning of the transaction process. After entering her PIN, the PIN along with her unique number would be sent to the registry to verify her identity and that she is on the registry list. For additional verification, the cashier could check the customer's identity, comparing the customer's name on the Do

Not Link Registry card to another form of identification, such as a license or credit card. This process seems less than ideal, as each additional step of the transaction only adds to its length and complexity. In addition, just comparing names would not rule out the possibility of someone with an identical name using the registry card. Even comparing the ID number were it printed on the registry card to another card on which the number is printed makes the process more cumbersome. A better solution to verifying identity might be through means of options 3 or 4.

If at the checkout in purchasing an item the individual is in the Do Not Link Registry, the customer would be given the choice of whether to allow linking in this particular instance or not, perhaps being offered a discount on the purchase or some other incentive if the restriction on linking is lifted. In the event that a Do Not Link ID number is present but not verified, the store could have the option of deciding whether to go ahead and link the purchases with the customer's identity, or to recognize the customer's intent and desire not to be linked and therefore not attempt to do so.

Once the allowance or disallowance of linkage is determined, the process of credit card purchase authorization would operate similar to current methods. Leaving the portion of the transaction requiring authorization of the credit card purchase itself until after determining whether linking is allowed appears less complicated than trying to fit this into the process at the outset. Also, placing the credit card authorization first does not allow for application of discounts towards the purchase amount, as the amount has already been approved.

6.3.2.3 Option 3: "Opting-Out" But "Opting-In" When Desired by the Individual: Identity Checking at Registration by the Registry

This option operates nearly the same way as much of option 2. However, this option differs in that it provides choices for verifying the identity of an individual at the time of registration, rather than at the time of the transaction.

6.3.2.3.1 Option 3 Registration Process

After the individual has supplied his name and address to a secure registry website or over the phone, the registrant would be required to provide one or more forms of identification (e.g. license number or state ID number) before being assigned a unique ID number by the registry and being prompted to choose a PIN. As with the previous options, the unique ID and PIN would be stored at the registry and the registrant would be issued a card. A check of the submitted form of identification would be made before a card was issued. If the form of identification provided could not be authenticated, then the unique ID number assigned by the registry would be invalid and subsequently deleted from the registry. If an attempt were made to use the number, say by providing it to a credit card company for inclusion on a credit card, when the individual went to use the card, the registry number would not be recognized and therefore would be of no use to the individual. This system does not provide a foolproof means of identity verification, since anyone who obtained the license number of another person for instance, could use that as a way to register under a false name. Therefore, additional means of verification are required, although making it a federal crime to register as another individual or

submitting a false form of identification during the registration process might deter potential violators of the system.

Option 3A: A minimum additional level of verification could be achieved by charging registrants a nominal fee requiring payment by a credit card linked to the registrant's name so that a record of the registrant is obtained. This could be implemented if registering either through a website or by telephoning the registry.

Option 3B: Another option providing a higher level of verification would be to gather biometric data such as a photo, fingerprint, iris scan or other biological identifier as part of the registration process. This would make it easier to track down those engaged in fraudulent registrations. Biometric data could be collected at a public office, perhaps at the Department of Motor Vehicles. At the time a driver's license is issued or renewed, the form might include a question as to whether a person would like to register on the Do Not Link list. Alternatively, a separate form specifically for registering on the list could be available. Collecting a digital photo is normally part of the driver licensing process. To enhance verification of identity in order to better enforce information privacy protection an additional identifier such as a thumbprint might be advisable and would not unduly slow down the process. In fact, collection of a thumbprint has been a requirement in Georgia since 2000.

With the requirement for the collection and storage of biometric data, questions arise as to where the data would be stored and who might have access to the data, both presently and in the future. People are generally wary of potential access to databases containing their personal information, whether by governmental entities for possible surveillance purposes or by identity thieves, but may be even more concerned if

biometric data were included within the database. The biometric data could be stored within the registry, along with an individual's registry number and PIN. Wherever the data collection took place, the data would then need to be transferred to the registry. Security measures for protecting the database and the biometric data transfer would be necessary. Currently research is being conducted to develop algorithms to protect biometric data such as fingerprints, facial images, and iris scans from unauthorized replication and use (Biever 2006).

6.3.2.3.2 Option 3 Transaction Process

For both options 3A and 3B, the individual would swipe her registry card or her credit card containing her registry number at the start of the transaction process as previously outlined in options 1 and 2. After entering her PIN, her registry number and PIN would be sent to the registry to verify that she is on the registry list. If on the list, then linking of her personal identity to the RFID-tagged items being purchased would not be allowed. The individual would have the opportunity to allow linking in exchange for possible discounts. After determination of the allowance or disallowance of linking at the option of the purchaser, the typical credit card transaction authorization process would proceed as usual.

6.3.2.4 Option 4: "Opting-Out" But "Opting-In" When Desired by the Individual: Relying on Identity Checking at Registration by Credit Card Companies

Under the three previous options a person in effect is registering himself or his identity, with the unique ID number being the means of checking whether he is in the registry. Option 4A requires that a financial transaction occur in the registration process thereby requiring that the person registering has already met the identity requirements of a financial institution. Option 4B involves the added ability of a person to register his credit card or debit card numbers with the registry.

6.3.2.4.1 Option 4 Registration Process

Option 4A: A person would provide his name, address, and if desired, one form of identification in a web form or over the phone to verify his identity at the beginning of the process. He would be assigned a unique ID for the registry and could choose a PIN. A minimum additional level of identity verification would be provided by requiring the charge of a fee to a credit card linked to the registrant's name, as outlined in option 3A. If a higher level of verification was desired, as stated in option 3B, biometric data could be gathered at the time of registration, but this should probably require an in-person visit to a physical office to minimize fraudulent identity generation activities. It might be best to avoid mandating additional security under this option and rely on the security mechanisms that credit card companies already use. If security measures are already sufficient for financial transactions, the envisioned system could simply rely on those

same security measures for identifying persons in order to better enforce their privacy desires.

Option 4B: While a person would still be required to enter his name, address and one form of identification to verify his identity during the registration process and to receive a unique registry number, he could also then enter his credit card or debit card numbers. After he was assigned a unique ID number, he could then choose a PIN. The unique ID would still be necessary as it would allow him to access the registry to update his account, whether to add or delete credit card or debit card numbers, or perhaps change his address, and the PIN would provide an additional security measure. Security for this registry system would need to be more robust than for some of the previous options, since accessing a person's registry account would lead to obtaining actual credit card numbers, enabling identity theft. Maintenance of records about multiple credit card numbers would also pose a heavy burden on both the registrant and the registry. This option puts a burden on the consumer to keep updating the registry when he acquires new or drops old credit and debit cards. Because of the increased management burden on both credit card users and credit card companies, and increased complexity over a single identifier for those desiring identity protection, option 4B is not recommended.

6.3.2.4.2 Option 4 Transaction Process

Under option 4A, it is now known that the person registering is highly likely to be that person in fact, and the unique ID correlation is appropriate. Under this option the burden might remain on the business to determine if the client has a Do Not Link ID number and to respect her preference if she does (i.e. transaction processes under options

2 or 3.) Alternatively the burden might be placed on credit card companies to check the registry for their card holders, respect the Do Not Link requirements, and convey to businesses at the time of transactions that the card holder can't have purchase items linked without permission. In this alternative approach the burden of checking the registry falls upon the credit card companies or banks issuing debit cards. This could be part of the regular credit card authorization process that is currently implemented at the time of purchase. If checking for inclusion on the Do Not Link list was checked at a remote location during every transaction, it would be an extra step in addition to verifying that the card was valid and that the person had not gone over her credit limit.

If the burden is put on the credit card companies to check the registry, a registry card may not be necessary. However, if no registry card is used there must be some way to inform the store where the purchase is taking place that no linking is allowed. The responsibility for this could be placed on the credit card companies. This might be accomplished through sending a message (i.e. card holder's Do Not Link ID number) to the store along with the credit card authorization approval. Alternatively the Do Not Link ID might be included directly on the credit card.

When an individual applies for a new credit card she could be given the option of supplying to the credit card company her registry ID number. Credit card companies would probably want to do this as a matter of course to speed up the transaction process as a benefit for their clients. The credit card company could then include that ID number on the credit card itself, after verifying that the individual was indeed registered on the Do Not Link list. After swiping her credit card at the time of purchase, she would be prompted to enter her Do Not Link PIN. These numbers would be transmitted to the

credit card verification site. If the PIN is correct, the credit card authorization site would transmit this data back to the store. The individual would then be prompted for a decision on whether she will grant permission to link her identity with the RFID-tagged items in this instance for some type of discount. If she allows linking, the discount is applied to the purchase amount, the credit card verification site is contacted to authorize the amount of transaction and informed that linking can occur, authorization verification is transmitted back to the store, and both the store and credit card company link the RFID-labeled items to her identity.

6.3.2.5 Potential Benefits and Issues Raised

With implementation of a Do Not Link Registry, no linking of tag data to a person's name occurs at the time of purchase without the person's explicit permission. Therefore, in many cases it would not be possible for RFID readers dispersed throughout the environment, such as those located on street corners or building entrances, to link the tag IDs of items to a person. That is, no person is on record as having purchased the specific items being recognized. However, the possibility of combining RFID with other technology, such as surveillance cameras, does exist and could allow the linking of individual identity with specific tag IDs. Again, however, if face recognition software indicated that a specific person was affiliated with a specific tag at a specific time, that association could not be linked legally if the person so identified has registered with the Do Not Link list. One issue then is how to inform the database that the individual recognized through face recognition, through the license plate of his car, or some other evidence is on the list. Perhaps an individual could carry a device that could either

continuously broadcast his registry ID number or transmit that number when a RFID reader is detected. As consumers may not wish to have their registry numbers broadcast, transmission of another code number or message might be possible. So when the message reached the database along with the tag data, the database would be informed that no linking of the individual's name to the tag IDs was allowed.

Perhaps every Do Not Link Registry card issued, or alternatively credit cards or driver's licenses as previously discussed, should itself carry a passive "privacy RFID" that responds with a Do Not Link number when applicable. Legislation could make it illegal to link other RFIDs to the person with the "privacy RFID" without that person's permission even if that person was identified through other means. The law would be applied to the commercial and private party sectors with waivers under appropriate circumstances for law enforcement.

Another possibility is use of a carried or worn item containing a RFID tag that when scanned by the reader in effect "blanks out" the electronic space around the surveillance camera. So while the person was within a certain distance of the camera, the RFID reader could not scan any other RFID tags, whether prevented perhaps by jamming the signal or through means of some type of blocker tag, examples of which were discussed in chapter 5. However, chances are that use of this type of an item would be legally prohibited, or at least heavily protested, as it might enable criminals to commit crimes with less possibility of detection. Various other approaches for preventing the recording of tag data by RFID readers have been proposed, such as putting tags in a "sleep" mode so that no tags affiliated with an individual will respond to a reader or programming the tags so that they will only respond to specific reader requests (Intermec

2005). However, many of these approaches require some change to RFID technology, which is a methodology not pursued in this work.

Already discussed was the possibility of linking a person's identity to previously unlinked tag ID numbers if the person was identified through face recognition software utilized by a surveillance camera with a built-in RFID reader. Conversely, if the tag ID numbers were already linked to the individual, a digital image captured by a camera could then be linked to the individual's identity. This could pose additional privacy concerns as it might increase the potential for personal tracking. However, one beneficial application might be to aid in the identification of criminals. If law enforcement personnel were unable to identify a suspect viewed in a crime scene surveillance video through face recognition software, perhaps due to the wearing of a mask by the suspect, the recorded tag ID numbers from items the individual was wearing or carrying might allow identification, provided the tags were linked to an identity. Even if the tags were not linked to a specific identity, having the tag ID numbers might allow law enforcement to ascertain where the individual had traveled after leaving the crime scene. For instance, if police believed a suspect might flee the area, readers placed at airport or bus station entrances, or at toll booths at highway entrances, could be used to determine whether and at what time the suspect had passed that way.

Another scenario involves the identification by the RFID reader of one or more tags that were linked to a person's identity at the time of purchase. There needs to be a way to ensure the additional tags on his person are not now linked to his identity as well. One possible way of dealing with the situation where a person had previously "opted-in" so that one or more of the tags currently on his person were linked to his name in a

database, would be for that database to also link his registry ID number to the RFID tag IDs previously linked to his name. That way when the tag ID number currently being scanned by the RFID reader reached the database level, it would be known that the other tags on his person should not be linked to his identity. Questions arise as to whether such a database of RFID tag information will exist in the future, and if so, who will have access to this database. The EPCglobal Network is a system being set up with the goal of connecting servers holding information relating to EPC RFID-tagged items. As part of the network, the ONS could be queried for the IP address of information relating to a particular tag's EPC number. The information would be available to trading partners within the network (EPCglobal 2004). Since through this network, data could be shared with other business entities and would be accessible through the Internet, the possibility of widespread access to a tagged item's history and last known location exists. Although sharing of the data contained within the network may initially be limited to business partners, the question of who potentially will be able to access the network in the future should be addressed, as data collected for one purpose is often used for many other purposes or shared with other entities at a later date, perhaps among those who later form business alliances.

If an individual chooses to allow no linking by others of tag data to his name, he may not be able to link his identity to a RFID tag's unique ID at a later date. This might affect a person's ability to reliably prove a particular item belonged to him in the event that the tagged item was stolen and later recovered. However, if the linking by others of tag IDs to a person were banned, the tags would still be useful for most purposes to which one wanted to put them. For example, if an individual had a personal RFID reader in his

home he could still read the tags of items in his pantry, refrigerator, and closet. His identity does not need to be linked to the specific jar of peanut butter for him to take an inventory of his pantry. Also, since the person would have the ability to read his own tags at any time he desired, he could record the tag IDs of various items, perhaps to inventory his possessions for insurance purposes. Thus the shortcoming of not being able to tie an object to himself is readily overcome by taking an automated inventory of all his possessions through use of an RFID reader and keeping the resulting inventory in a secure place, whether lockbox, his sister's freezer, or his brother's external hard drive.

One major benefit of a Do Not Link Registry approach to privacy is that it would not require any change to the RFID technology itself. This is important since modifications to technology after implementation are often costly in terms of both time and money. Likewise, future developments in RFID technology should not prevent implementation of the Do Not Link Registry.

Another benefit is that the registry would provide a legal basis for compliance and action against violators of the regulations. In order to take action against violators, one would need to realize that a violation had occurred. Perhaps one way to recognize the occurrence of linking would be if a person received a special "Welcome Mary Smith" message or a discount offer as she walked by a store. Mary may know that she has never allowed any of her purchases to be linked. However, even if the store checked and found Mary to be on the Do Not Link list, they would be allowed to assume that she may have opted to allow some items to be tracked and therefore the store appears to be doing nothing wrong from its perspective. It may be difficult for Mary to identify and prove who specifically was responsible for linking her RFID tag data to her identity in the first

place. One possibility is for individuals or investigators to record where items are purchased, perhaps by scanning the RFID tags in the items with a personal RFID reader, then downloading the tags' ID numbers to a personal computer and storing them with the purchase locations. Then if identifying greetings or discounts based on profile were offered, she could use the knowledge of where the items she was wearing or carrying were purchased to go after specific companies. Pursuing violations could lead to subpoenas of suspect databases and massive claims against corporations, which might prove to be a large deterrent to potential commercial offenders.

Linking the tag to an identity may have occurred at a time after purchase, which potentially could be dealt with through scan logs – recording all RFID reader scans on a portable device such as a cell phone (Reiback et al. 2005). The device might require the use of a "tag emulator" such as has been developed at the MIT Auto-ID lab. The "tag emulator" would act like a tag, listening and decoding reader communications, so that these could be recorded (Reiback et al. 2005). Currently the reader-to-tag protocol does not include a reader ID or a data collector ID, necessary for knowing who is collecting and recording the tag data. As discussed in section 5.3.1, Floerkemeier et al. (2004) propose inserting these into the protocol, along with other data. Then the individual could have a record of who has been collecting data. These scan logs could be downloaded to a home computer.

A number of issues arise in identifying violators through the recording of scan logs. Firstly, these scan logs would involve recording and storing a huge amount of data if readers were to saturate the daily environment. It would probably be necessary to download the scan logs every day, depending on the storage capacity of the portable

device, which would be inconvenient. Storage of the daily scans on a home computer might also consume a large amount of memory. Secondly, to include a reader ID and a data collector ID in the reader-to-tag protocol would require a change to current RFID standards and possibly necessitate the registration of readers, perhaps imposed through legal requirements. Standards committees may be reluctant to include these IDs absent a law compelling them to do so. Thirdly, the individual would have the problem of searching through all her records to figure out when the linking took place and by whom. A person would have to record what she wore each day and store that data along with the scan logs. Then she would have to search her records to determine the days on which she wore the same tags as the day she was offered a discount or through some event became aware that linking to her identity had occurred. In the end a person may not be able to prove that a specific entity linked a tag to her identity, but only that a scan of the tag data occurred at specific times and locations and who initiated the scans. However, an investigator looking for widespread abuses by corporate entities in order to pursue class action suits would probably be able to accumulate a preponderance of evidence to make their case without an overly heavy investigative burden.

6.3.2.6 Recommendations

The chosen recommendations not only provide an individual the ability to "opt-out" of the linking of his identity to specific RFID tags, they also afford him the opportunity to "opt-in" when he so desires. Additionally, they include a verification of identity at the outset of the registration process, limiting the potential for registering under false identities. Integration of a law disallowing the linking of an individual's name

to items he has purchased, or linking his name to RFID-tagged items observed on his person, provides a legal foundation for the registry that allows action against violations of the law.

6.3.2.6.1 Registration Process Recommendation

Based on the material outlined in the above sections, it appears that registration option 4A would work the best from both technological efficiency and practical perspectives, in order to facilitate the most widespread use of the registry. Verification of identity at the time of registration provides a safeguard against false registrations and could either be implemented at a minimal level through requirement of a nominal fee charged to a credit card linked to the registrant's name, or a higher level through the collection and recording of the registrant's biometric data. When considering which level would be deemed acceptable by the majority, there is a tradeoff between ease of registration access and a more secure system to verify identity. The minimal level of verification provides easier access. Individuals could register on a website or telephone the registry at their convenience if the only verification required was a credit card charge with a match of first and last names in the registry with a match of first and last names on the credit card. A requirement to travel to a specific location such as a public office (e.g. DMV) could prove difficult for some individuals and would involve a greater time commitment.

The level of difficulty and the time required for registering on the Do Not Link list would no doubt influence the number of individuals who chose to register. However, providing the option of registering at a public office would give individuals who do not

have a credit card with which to register online or over the phone the ability to register in person through presentation of one or more forms of identification. Also, individuals with a greater concern for identity verification may prefer the use of biometric identifiers such as a photograph or fingerprint. However, there is also a need to balance a high level of identity verification with concern over storage of and access to biometric data, data that would be very enticing to identity thieves. Additionally, a system incorporating biometric data would involve more complexity in system architecture, as the biometric data would need to be collected and then transmitted to the registry in a secure manner. The cost of purchasing and installing data collection equipment into a public office would no doubt be quite high, in addition to the cost of training equipment operators and maintenance of the equipment, hardware and software. Therefore, designating the DMV as a potential biometric data collection site seems reasonable, since most if not all of those offices already have the equipment to collect at least one form of biometric data (e.g. digital photo).

The chosen approach should attempt to provide the best option for the majority while allowing personal choice when possible. Ease of access to registration is perhaps in the best interest of individuals. Therefore, identity verification through requiring a credit card transaction at registration may be the best approach, if a choice has to be made of one approach over the other. It is after all credit card transactions rather than cash transactions that allow most linking to occur, and thus parties with credit cards already are those who would be most interested in registering. Increased use of biometrics would be best incorporated by allowing Do Not Link registrations to be incorporated as part of the state driver's license application and renewal processes. Due to the less complex

nature of identity verification by credit card transaction validation, beginning with this approach seems reasonable, with the goal of adding other options later on, such as allowing the capture of biometric data if individuals so desire. Also to be implemented is a means of ensuring that all individuals, whether possessing credit cards and drivers' licenses or not, have access to the registration process. An example of the website registration form for the recommended Do Not Link registration process is illustrated in Figure 1.

National Do Not Link Registry

Those supplying false or misleading information will be in violation of a federal offense and subject to the full prosecution of the law (U.S. Code xxxx)

The Do Not Link Registry provides you with a computer readable identification number and identification card that places businesses and government agencies on notice that they may not link your identity to products containing radio frequency identification tags without your explicit permission.

To register you must enter the following information:

First name:

Middle name:

Last name:

Address line 1

Address line 2

City:

State:

Zip code:

Email address*:

*An email address is collected so that a confirmation of your registration may be sent to you via email within 24 hours. If you do not receive an email confirming your registration within that time period, contact us at help@DoNotLink.org or by calling us toll-free at xxxx.

Please provide at least one form of ID**:

Driver's license number

State I.D. number

Passport number

**Provision of this form of ID is optional. It is an additional means of verifying identity at the time of registration, if desired by the registrant.

Figure 1. Website form for recommended Do Not Link registration process.

Credit card information:

A fee of $5 will be charged to your credit card as part of the registration process. The credit card used must be in your own name. Use your name below **exactly** as it appears on your credit card. The first and last name below may NOT be different from that listed above.

First name:

Middle name:

Last name:

Address line 1

Address line 2

City:

State:

Zip code:

Type of card:

- ○ Visa
- ○ MasterCard
- ○ Discover
- ○ American Express

Credit card number:

Expiration date:

○ I agree to pay the $5 charge required to process my registration.

○ I certify that to the best of my knowledge all information provided on this form is accurate and does not contain any falsehoods or misrepresentations. Further, I grant permission for registry officials to verify that the form of identification I provided is legitimate. I understand that supplying false information or misrepresenting my true identity may lead to fines and/or criminal charges.

Submit

Figure 1 (cont.). Website form for recommended Do Not Link registration process.

6.3.2.6.2 Transaction Process Recommendation

Option 4 provides the best choice for transaction process as well. Under this option every business would be responsible for making sure that no linking to individuals in the registry occurs without their explicit permission. This would incentivize businesses to make the "opt-in"/"opt-out" process efficient.

It seems appropriate to require businesses to check whether or not a person is on the Do Not Link list, as businesses are the ones actually collecting the data at the point of sale. This of course would only be efficient if done in a completely automated fashion. Imposing the requirement would force the process to become efficient. Even though all stores would be bound legally to enforce the Do Not Link Registry requirements, the credit card companies may find it more efficient to embed Do Not Link numbers in their cards and do this checking as part of the automated transaction process. Ultimately, credit card companies, stores, and all other parties would be bound by the Do Not Link Registry list. If one of these entities is unwilling to share who is or who is not on the Do Not Link list with the other entities, each entity would be responsible for checking the registry independently. The market would eventually arrive at a solution among credit card companies and retail stores. An action flowchart of how the recommended transaction process would proceed is illustrated in Figure 2.

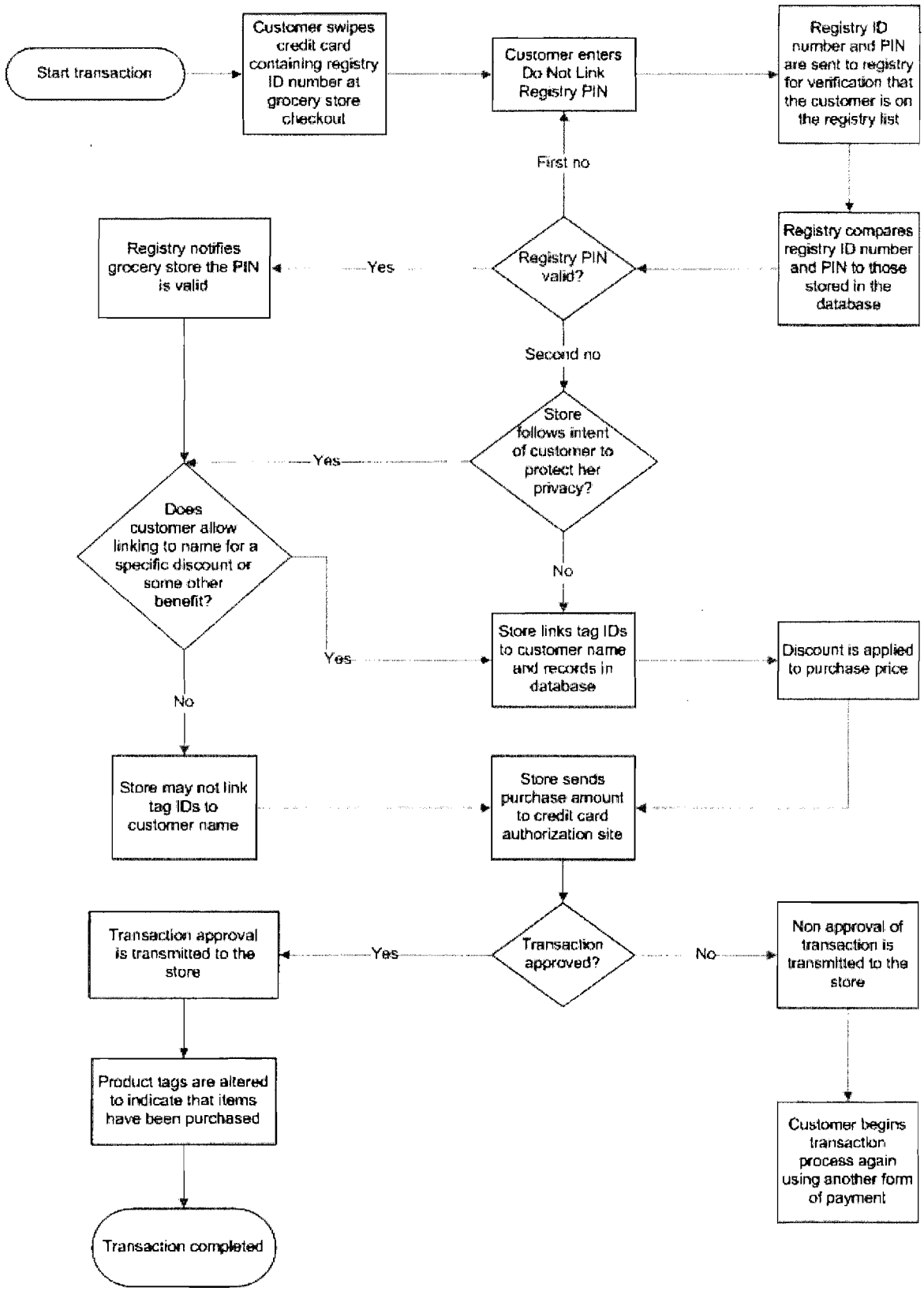

Figure 2. Action flowchart of recommended transaction process.

6.4 Contractual Approach to Autonomous Location Privacy Protection

Autonomy would mean that individuals had options as to how they desired their personal information to be handled, so as to gain control over that information. To provide those choices or options in a location-based service context, Bhaduri and Onsrud (2002) propose the application of a universal contract model that puts control over release of personal location information into the hands of an individual (Bhaduri 2003). The theory is that a market solution that allows users to choose and readily alter their privacy preferences under continually changing circumstances will be more successful in the market than location services that don't offer this capability. Herein proposed is the extension of that concept to a RFID environment, allowing individuals who have registered in the Do Not Link Registry to temporarily "opt-in" to RFID data collection when they desire to do so, and under what standard contract conditions they desire.

A market solution might be based on incentives, such as if an individual allows personal tracking in exchange for discounts on goods or services. By permitting an individual to decide whether and to what extent to allow tracking, this places the obligation for protecting privacy on the individual, but also empowers the individual with autonomy to decide. Since the universal contract model would promote the achievement of each individual's personal preferences, people would likely choose this market solution over others, resulting in a market that naturally gravitates towards an environment that would protect privacy responsive to the comfort level of each individual.

6.4.1 "Opting-In" On-The-Fly: Considerations for System Design

In order for this on-the-fly system to function efficiently in providing privacy protection, a universal contract model needs to be developed. A contract lays out the rights and responsibilities of all parties involved. In this case, it is the rights of the individual consumer and the rights of the business (e.g. grocery store) or the provider of some service. Use of a contract would facilitate growth within the industry as individuals would be more apt to "opt-in" if they knew they had some legal recourse if the contract was breached. A uniform contract employed across industry would allow for easier integration of services between various business entities and their customers. Additionally, there would be less confusion for individuals as they would not have to keep track of numerous contracts with varying structures.

When considering contract parameters, one issue to be addressed regards the length of time data could be stored. If an individual "opted-in" for a specific service or discount, would the data collected be stored temporarily or retained for all time? Incorporated in the Do Not Link enabling legislation might be a provision stipulating that the link of a RFID tag to a name was to be expunged after a certain time period or perhaps after a service was completed, unless the Do Not Link registered user explicitly agreed to a different time period. Perhaps the standard industry contract could also allow the consumer to change her retention length preferences on a daily basis.

In the grocery store scenario where a customer is purchasing goods, a contract with default settings might apply when the customer agrees to "opt-in" for a discount on the purchased goods. However, when signing up for some type of service there could be more opportunity to create a contract specifying one's preferences. In this case, one

might make decisions not only on the length of data retention, but what data could be collected, and the purpose to which it could be put. If the consumer is given the ability to set and change her preferences as she so desires, the core ethical principle of individual autonomy is supported.

6.4.2 "Opting-In" for Services

Myriad applications are envisioned for RFID technology. Previously discussed was the scenario of "opting-in" for discounts at the grocery store. "Opting-in" for services is another possibility. One proposed service involves providing information to the user based on location of personal belongings, such as reminding the user not to leave her umbrella on the train, or informing her of where she can find a taxi or bus at the train station through use of an RFID enabled cellular phone with Internet access (Shimizu et al. 2005). The potential applications for RFID technology appear endless. However, with the creation of a Do Not Link Registry, along with laws limiting RFID data linking and the ability of individuals to "opt-in" for services or discounts, privacy protection that facilitates personal choice may be possible even in a RFID laden environment.

Chapter 7

CONCLUSIONS AND FUTURE WORK

This thesis highlights the problem of privacy loss within a milieu of ever expanding surveillance and tracking technologies, examines privacy protection methods proposed by others, and presents a recommended approach to personal privacy protection within a pervasive RFID environment. The recommended approach merges both legal and technological means of privacy protection, enabling individual control over the decision of whether or not to allow linking of RFID tag data to personal identity. This chapter provides a thesis summary, discusses the conclusions reached, and outlines potential future work.

7.1 Summary

Privacy has become a matter of great concern to individuals, especially in light of the many recent data privacy breaches involving the records of data warehouses, credit card companies, or other entities. Although surveillance technologies have become a common element of daily life, their increasing capacity to track when an individual is at a specific location and even what she bought at that location, has heightened concerns over privacy. Moreover, RFID technology could facilitate the continuous tracking of individuals through the RFID-tagged items they are wearing or carrying, and that data could be merged with other personal information, raising the potential privacy threat level to a new high.

In order to lay the foundation for a discussion of privacy and the pursuit of a solution for preventing privacy loss, this thesis defined privacy from various perspectives and presented issues relating to privacy both in general aspects and specifically to location-based privacy. An examination was made of proposed methods of protecting privacy through both legal and technological means.

To find a privacy solution within RFID environments, one must first understand the technology. Therefore, the components of a RFID system and the operation of a RFID system were covered. A discussion was provided on the privacy issues relating to RFID technology and how they differ from issues arising through use of other technologies. A discussion was also included on how current and future uses of RFID technology raise specific concerns relating to privacy.

As legal or technological approaches on their own do not provide a total solution to privacy protection, a better solution may be reached by combining these approaches through a contractual relationship between data collectors and consumers, with technology designed to enforce the contract. By allowing consumers to contract with data collectors as to how much or when data may be collected, they have the option of setting their own privacy preferences, thus promoting individual autonomy.

The privacy protection model presented in this thesis allows consumers to choose whether they want the RFID tags embedded in items they purchase to be linked to their identities. The opportunity to register on a centralized list that provides notice of an individual's desire not to have this linking take place, legally supported through privacy law, would provide this choice for consumers. At the same time, if a consumer chose to "opt-in" for a particular benefit, this option would be available to him, enabled through

private contract with a particular business or service provider, supporting the principle of autonomy by allowing the consumer to choose his own privacy preferences. Technological means of implementing this system and potential issues arising from implementation were also addressed.

Since it is impossible to foresee exactly what advancements in RFID and other computing technology will be reached at the time when full-scale RFID adoption occurs, this research was conducted under the following assumptions:

- Most or all consumer products will be embedded with RFID tags.
- A pervasive system of RFID readers will exist.
- Data from RFID tags can be linked to personal identity.
- RFID systems will be interoperable, allowing continuous tracking of tags.
- RFID technology will remain a fairly open system, facilitating access to most passive RFID tags by any RFID reader.

7.2 Conclusions

The goal of this thesis was to explore whether an approach could be conceptualized that might sufficiently protect individual privacy in the use of RFID technologies while simultaneously supporting a marketplace environment that would foster expansion of innovative RFID applications. Bearing in mind the assumptions listed in the previous section, several questions were posed in chapter 1 and investigated and analyzed through the course of this research. These questions are restated below, and are followed by the conclusions drawn.

- *What is the minimum standard of privacy protection that would prove acceptable to the general populace and how could technology be used to enforce that level of protection?*

This research exposed that minimum levels of privacy comfort vary among individuals, as well as over time as circumstances change. Thus minimum levels of comfort need to be responsive to individual choice. By examining both past and current legal and technological proposals for privacy protection, an approach was developed based on individual choice. While the model gives individuals autonomy to choose, it is also makes them responsible for intelligently protecting their own privacy if they value it. Legal protections in the form of privacy legislation are included in the proposed approach, supporting choice.

By incorporating this privacy protection method into the purchase transaction process, consumers are allowed to prevent the linking of tag data at the outset of their relationship with an RFID-labeled object. The current technology that is set up for credit card transaction authorization provides the type of architecture required for businesses and other service providers to validate the registry PIN number that customers provide by swiping their credit cards or registry cards at the time of RFID-tagged item purchases. Since current technology can be utilized, successful implementation of the recommended approach appears to be realistic. As technology advances, technological alterations are readily envisioned as capable of being incorporated into system design and operation.

- *How might purchasers of RFID-tagged items be afforded control over the amount and nature of personal or location information that may be obtained through the recording and tracking of their tags by RFID readers?*

  The Do Not Link Registry provides consumers the ability to effectively "opt-out" of the linking of RFID tag data to other personally identifiable information. This centralized list approach has been successfully implemented through the National Do Not Call Registry and the legal approach recommended appears to be clearly supported by past constitutional case law.

  The approach proposed in this thesis enables consumers who have registered on the list to "opt-in" when they so choose through a standard industry-wide form contract approach defining the legal relationships between all businesses using RFID tags and all consumers choosing to register on the Do Not Link list. The standard contract would enable consumers to limit tag data collection according to their privacy preferences and to change their preferences over time as desired.

- *How could unauthorized linking of RFID tag data to individual identities be prevented?*

  One instance for potential linking might arise when a reader detects on a person several tags that were linked to the person's identity in the past when the person "opted-in" to linking. In this case, once the RFID tag data reached the database, notification that no linking is allowed would be provided since at the time of purchase the person's registry ID number was stored along with the purchaser's name and the item's unique identifier.

Linking of tag IDs to personal identity may be possible through the combination of a RFID reader and a surveillance camera. If a person was identified through use of an alternative method, this could be dealt with by means of carrying a Do Not Link Registry card that was embedded with a "privacy RFID" responding to RFID readers with the person's Do Not Link ID number, providing notification that no linking was allowed. The Do Not Link enabling legislation could make linking other RFIDs to a person with a "privacy RFID" illegal, if done without explicit permission.

Absolute prevention of linking may not be possible without the use of technology such as a RFID signal jamming device or a blocker tag, as previously discussed. However, by enacting legislation stating that individuals registered on the Do Not Link list may not have their names linked to RFID embedded items they purchase without granting explicit permission, a legal basis for action against violators of the laws is provided. These individuals would be subject to civil lawsuits for actual or statutory damages, which should provide a deterrent to potential offenders.

- *Since a multitude of consumer RFID applications are envisioned for the future, how might privacy be enabled in a way that permits continued tag usability after the purchase of RFID-tagged goods?*

As modifications to tag technology involves both time and monetary costs, the proposed approach strove to provide privacy protection that did not involve any alterations to RFID tags. Therefore, tags will still retain their usability after purchase, whether utilized in the home environment or for applications outside the

home. If the combined technological and legal model recommended through this research were implemented, it might drive RFID tag developments in a direction where legal privacy protections were enforced automatically.

- *How might consumer privacy protection be facilitated, while at the same time not hindering the growth of useful RFID applications and the RFID market?*

  The Do Not Link Registry provides a means to "opt-out" of the linking of personal identity to RFID-tagged items. The "opt-in" capability enabled through the universal private contract approach allows even those who would otherwise not allow linking to "opt-in" when they wish to receive some type of benefit or for a desired service. If no information privacy protections are provided, the market is likely to experience wide-ranging destructive counter technologies that will have a disruptive affect on the market. Since it is in the best interest of businesses and service providers to have access to RFID data, this will undoubtedly lead to the development of applications and services that incorporate individual choice in the setting of privacy preferences and allow users to alter their preferences easily and at any time.

The conclusions outlined above support the hypothesis of this thesis, and it is thus ultimately concluded:

> *A combined legal and technological approach has greater potential for sufficiently protecting individual privacy in the use of RFID technologies while also strongly supporting marketplace uses of such tags than would use of technological or legal solutions alone.*

7.3 Future Work

RFID is a rapidly advancing field of technology. Abundant research is currently being conducted in many aspects of this field, such as improved tag functionality through increased microchip computing power and storage capacity, greater read range, commonality of RFID operational standards, applications of RFID technology, and privacy protection. In addressing RFID and privacy issues, this thesis research has discovered additional avenues for future work. The following sections address areas that extend this research specifically, in addition to suggesting other areas of related research.

7.3.1 Extensions of Proposed Approach

This research presents a conceptual model of privacy protection - lays out the model components, presents various options for system architecture, recommends one option to pursue, and discusses potential issues resulting from system implementation. Actual implementation of the proposed model was not within the scope of this research. In order to implement the model, further attention needs to be focused on the specific components of the model.

7.3.1.1 Registry Oversight

In considering implementation of the Do Not Link Registry, the question arises of which type of entity should be responsible for overseeing the system. Two possibilities are a government agency or a non-profit organization. As U.S. citizens are cognizant of recent domestic spying programs, trust in governmental oversight of personal information has diminished for some individuals, and they may prefer oversight by a non-profit

organization. Conversely, other individuals may feel the government should be the institution overseeing such a program. Determination of which type of oversight would be preferred and trusted by the majority would help ensure that the registry was used by the largest number of individuals. If people feel they cannot trust the system, they will be wary of using it.

7.3.1.2 Contract Development

Consideration needs to be given to development of the universal contract that is used when individuals who have registered on the Do Not Link list decide to "opt-in" to linking in a specific instance. This contract would be in force between the consumer and the data collector. Contract design should take into account the needs and desires of individual users. Therefore, consideration should be given to questions such as:

- What privacy settings would individuals desire?
- Using those settings, how could the contract be developed so as to allow users to readily select and change their preferences?
- How would data collectors be held accountable for the misuse of data collected?
- How could industry be incentivized for model acceptance?

Whichever contract design is chosen, the design needs to be flexible to accommodate multiple user preferences and support dynamically changing contract parameters (Bhaduri 2003).

7.3.1.3 Legislation

Privacy legislation would provide the strength to the Do Not Link Registry, allowing investigation of and action against violators of the law. Creating legislation is generally a difficult and a time-consuming task. In this case, with legislation requiring incorporation of RFID technology, it may prove to be an even more complex process and require considerably more effort to construct, especially because future developments of the RFID technology are not fully known. Initially, businesses may be inclined to block passage of such legislation, unless they are able to see the potential benefits and potential profits.

7.3.1.4 Calculation of Costs

As with implementation of any project, cost becomes a significant issue. Costs associated with implementation and maintenance of a Do Not Link Registry need to be calculated and responsibility needs to be assigned for cost coverage. Additionally, to support the verification process of registry PIN numbers at the time of a purchase, businesses would need to have the technological capability to perform this function, as well as ensuring RFID-tagged items are not linked to a person's name in the business' database if that person is registered on the Do Not Link list. These capabilities would require the installation of additional hardware and/or software. While larger corporations may be able to absorb these expenditures more easily, the costs may prove a heavy burden for smaller stores that would likely be forced to pass these costs on to their customers. Without the new technology, stores would have to assume that no customers may have their identities linked to their purchases, thereby giving a distinct advantage to

the larger businesses. However, credit card companies might very well take on the role. Other costs to be considered include technical costs in terms of additional processing time for purchase transactions, data storage capacity needs, and security provisions. Although some of these costs may seem to be quite high when considered only from a monetary viewpoint, when weighed against the cost to society of not protecting personal privacy, they may not appear nearly as costly.

7.3.1.5 Security

Security is always a concern when dealing with any type of personal data. Reliance could be placed on the same security mechanisms that credit card companies currently employ in the transmission and storage of data. However, due to the sometimes lax security measures that have led to recent data breaches, a more secure system may be desired. Outcry from victims of these security breaches may force credit card companies to develop and implement a higher level of security which could also be applied to the transmission and storage of registry data. Determination of the required or desired level of security would need to take into account not only current technological capabilities, but also attempt to foresee what future security issues might arise, as technology is advancing at a rapid pace. The appropriate amount of security necessary to employ this system may depend ultimately on the use to which the registry ID number is put. If at some time in the future this number is used as a supplement or replacement of a social security number, then a more robust form of security is desirable, as possession of the registry ID number may enable access to copious amounts of personal information, as a social security number does presently.

7.3.2 Another Area of Research

RFID technology provides a rich field of research. Privacy, though only a relatively small part of the research being conducted in this field, is a very important aspect of RFID technology. Assuming the technology becomes ubiquitous in the future, additional privacy concerns will no doubt arise, perhaps with each step towards ubiquity.

Previously discussed in this thesis was the potential for embedding a RFID reader into a surveillance camera, possibly facilitating the identification of people whose RFID-tagged clothing and other carried items were not currently linked to their individual names. Additional technologies could be joined with RFID technology. One such example is combining RFID and GPS, which is already being employed in shipment tracking. The real-time tracking capabilities of GPS, along with the ability of RFID technology to link vast amounts of data to a particular tag, and therefore a particular individual, heightens the threat for a continuous tracking environment. With this potential to combine RFID with various other technologies comes the need to discuss privacy issues arising from specific combinations of technology, and to consider potential solutions to limit privacy loss.

REFERENCES

ACLU (2003) Defunct Big Brother Spying Program Resurfaces as "Little Brother" in Seven States. October 30, 2003. Available: http://www.aclu.org/privacy/spying/15722prs20031030.html

ACLU (2005) Second major Snoop Program Shut Down by Privacy Opposition. April 15, 2005. Available: http://www.aclu.org/privacy/spying/15324prs20050415.html

Albrecht, K. (2004) METRO Future Store Special Report. Available: http://www.spychips.com/metro/scandal-payback.html

Armstrong, M.P., G. Rushton. and D.L. Zimmerman (1999) Geographically Masking Health Data to Preserve Confidentiality. Statistics in Medicine, 18 (5): 497-525.

ARTICLE 29 Data Protection Working Party (2005) Working Document on Data Protection Issues Related to RFID Technology. January 19, 2005. Available: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Asif, Z. and M. Mandviwalla (2005) Integrating the Supply Chain with RFID: A Technical and Business Analysis. Available: http://www.ebi.temple.edu/programs/RFID/RFIDSupplyChain.pdf

Bailey, D. and A. Juels (2006) Shoehorning Security into the EPC Standard. Available: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/shoehorning/EPCshoehorningSCN.pdf

Beckwith, R. (2003). Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive Computing 2(2): 40-46.

Bender, K. (2005) Berkeley Puts $650,000 into Library Book Tracing System: Some Raise Privacy Concerns Over Technology. Alameda Times-Star (2/08/05) Available: http://www.insidebayarea.com/timesstar/ci_2558852

Berdik, C. (2005) Technology Now Used on Toll Roads and in Stores is Moving into Hospitals. The Boston Globe (2/1/05).

Beresford, A. R. and F. Stajano (2003). Location Privacy in Pervasive Computing. IEEE Pervasive Computing 2(1): 46-55.

Bhaduri, A. (2003) User Controlled Privacy Protection in Location-Based Services. Masters Thesis, Dept. of Spatial Information Science and Engineering. University of Maine.

Bhaduri, A. and H. Onsrud (2002) User Controlled Privacy Protection in Location-Based Services, Extended Abstract, Proceedings of the 2nd International Conference on Geographic Information Science (GIScience 2002), Boulder, Colorado, September 25-28, 2002.

Bibas, S.A. (1994) A Contractual Approach to Data Privacy. Harvard Journal of Law & Public Policy 17(2): 591-611.

Biever, C. (2006) A Code to Keep Your Fingerprints Secure. New Scientist. June 3, 2006. Available: http://www.eurekalert.org/pub_releases/2006-05/ns-act053106.php

Black, C.L., Jr. (1997) A New Birth of Freedom: Human Rights, Named and Unnamed. (New York: Grosset/Putnam).

Bono, S., M. Green, A. Stubblefield, A. Rubin, A. Juels, and M. Szydlo (2005) Analysis of the Texas Instruments DST RFID. Available: http://rfidanalysis.org/

Bruening, P.J. (2004). Prepared Statement for the Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce on Radio Frequency Identification (RFID) Technology: What the Future Holds For Commerce, Security, and the Consumer. July 14, 2004. Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearing&docid=f:95455.pdf

ByteandSwitch.com (2005) HP, Philips Drive Adoption. Available: http://www.byteandswitch.com/document.asp?doc_id=80549

CASPIAN (2004) Scandal: The "Undead Machine" Available: http://www.spychips.com/metro/scandal-deactivation.html

CASPIAN (2003) RFID Right to Know Act of 2003. Available: http://www.nocards.org/rfid/rfidbill.shtml

CASPIAN et al. (2003) RFID Position Statement of Consumer Privacy and Civil Liberties Organizations Available: http://www.privacyrights.org/ar/RFIDposition.htm

Center for Democracy & Technology (2001). Privacy Rules For Access to Personal Data. Available: http://www.cdt.org/security/guidelines

Cavoukian, A. (2004) Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. Available: http://www.ipc.on.ca/docs/rfid.pdf

Department of Defense, Office of the Deputy Under Secretary of Defense (Logistics and Material Readiness) (2006) RFID Frequency Identification (RFID). Available: http://www.acq.osd.mil/log/rfid/rfid_faq.htm#DoD_RFID_Policy

Dipert, B. (2004). Reading Between the Lines: RFIDs Confront the Venerable Bar Code. Available: www.reed-electronics.com/ednmag/article/CA468418?pubdate=10%2F14%2F2004

Duckham, M. and L. Kulik (2005) A Formal Model of Obfuscation and Negotiation for Location Privacy, In H.W. Gellersen et al. (Eds.), Pervasive Computing: Third International Conference (PERVASIVE 2005) Munich, Germany, May 8-13, 2005. Springer-Verlag pp. 152-170. Available:http://www.springerlink.com/media/99ELVPMWWG6E51MLPT6Y/Contributions/K/W/L/V/KWLVM0DE5MGA8DE2.pdf

Electronic Frontier Foundation (EFF) (2005) Appendix B: RFID and the Construction of Privacy: Why Mandatory Kill Is Necessary. In Garfinkel, S. and B. Rosenberg, (Eds.), RFID: Applications, Security, and Privacy (Westford, MA: Addison-Wesley), 497-506.

Electronic Privacy Information Center (EPIC) (2005) EPIC Alert. Vol 12.10. May 20, 2005. Available: http://www.epic.org/alert/EPIC_Alert_12.10.html

Electronic Privacy Information Center (EPIC) (2004a) FTC Workshop on Radio Frequency Identification: Applications and Implications for Consumers. June 21, 2004. Available: http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf

Electronic Privacy Information Center (EPIC) (2004b) Guidelines on Commercial Use of RFID Technology. July 9, 2004. Available: http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf

Electronic Privacy Information Center (EPIC) (2004c) Radio Frequency Identification (RFID) Systems. Available: http://www.epic.org/privacy/rfid

Electronic Privacy Information Center (EPIC) (2004d) The USA PATRIOT Act. Available: http://www.epic.org/privacy/terrorism/usapatriot/

EPCglobal (2005) Guidelines on EPC for Consumer Products. Available: http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html

EPCglobal (2004) The EPCglobal Network Demonstration. Available: http://www.sun.com/software/solutions/rfid/epcglobal_network_demo.pdf

Farmer, D. and C. Mann (2003) Part One: Surveillance Nation. Technology Review. April 2003.

Federal Trade Commission (FTC) Fair Information Practice Principles. Available: http://www.ftc.gov/reports/privacy3/fairinfo.htm

Federal Trade Commission (FTC) (2005) National Do Not Call Registry. Available http://www.ftc.gov/donotcall/

Fiskin, K. and S. Roy (2003) Enhancing RFID Privacy via Antenna Energy Analysis. Technical Report Technical Memo IRS-TR-03-012, Intel Research Seattle, 2003. Presented at the MIT RFID Privacy Workshop, November 2003.

Floerkemeier, C., R. Schneider and M. Langheinrich (2004). Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan. Available: http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf

Garfinkel, S. (2002). Adopting Fair Information Practices to Low Cost RFID Systems. In Ubiquitous Computing International Conference Privacy Workshop, September 2002. Available: http://www.simson.net/clips/academic/2002_Ubicomp_RFID.pdf

Garfinkel, S. (2004) RFID Rights. Technology Review. Available: http://www.technologyreview.com/articles/04/11/wo_garfinkel110304.asp?trk=nl

Gilbert, A. (2004) Theme Park Takes Visitors to RFID-land. CNET News.com. Available: http://news.com.com/Theme+park+takes+visitors+to+RFID-land/2100-1006_3-5366509.html

Gruteser, M., G. Schelle, A. Jain, R. Han and D. Grunwald (2003). Privacy-Aware Location Sensor Networks. Available: http://systems.cs.colorado.edu/Papers/Generated/2003PrivacyAwareSensors.html

Hitachi (2004). The World's Smallest RFID IC. Available: http://www.hitachi.co.jp/Prod/mu-chip/#top

Hong, J.I., J. D. Ng, and S. Lederer (2004). Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. Designing Interactive Systems (DIS2004), Cambridge, Massachusetts, 1-4 August 2004.

Hulme, G. and T. Claburn (2004) RFID's Security Challenge. Information Week. Available: http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID=52601030

Intermec Technologies Corporation (2005) Will Your EPC Gen 2 System Be Up to Standard? Available: http://epsfiles.intermec.com/eps_files/eps_wp/Gen2SysStand_wp_web.pdf

Juels, A. (2006) Technological Approaches to the RFID Privacy Problem. In Garfinkel, S. and B. Rosenberg, (Eds.), RFID: Applications, Security, and Privacy (Westford, MA: Addison-Wesley), 329-339.

Juels, A. and J. Brainard (2004) Soft Blocking: Flexible Blocker Tags on the Cheap. Workshop on Privacy in the Electronic Society (WPES '04), October 28, 2004, Washington, DC, USA. Available: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/softblocker/softblocker.pdf

Juels, A., R.L. Rivest and M. Szydlo (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In 10th Annual ACM CCS 2003, May 2003. Available: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

Katz v. United States (1967) 389 U.S. 347.

Kourouthanassis, P. and G. Roussos (2003). Developing Consumer-Friendly Pervasive Retail Systems. IEEE Pervasive Computing 2(2):32-39.

Kumagai, J. and S. Cherry (2004). Sensors and Sensibility. IEEE Spectrum 41(7):22-28.

Lace, S. (2004). Calling in the Chips?: Findings from the First Summit Exploring the Future of RFID Technology in Retail. Available: http://www.ncc.org.uk/technology/calling_in_chips.pdf

Langheinrich, M. (2001) Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, In: Proceedings of Ubicomp 2001, September 30 - October 2, 2001, Atlanta, GA. Available: http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf

Langheinrich, M. (2002a). A Privacy Awareness System for Ubiquitous Computing Environments. 4th International Conference on Ubiquitous Computing (UbiComp2002), Göteborg, Sweden, 29 September – 1 October, 2002. Available: http://www.vs.inf.ethz.ch/publ/papers/privacy-awareness.pdf

Langheinrich, M. (2002b). Privacy Invasions in Ubiquitous Computing. Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing. 4th International Conference on Ubiquitous Computing, UbiComp2002, September 2002. Available: http://www.vs.inf.ethz.ch/publ/papers/uc2002-pws.pdf

Laurant, C. (2004). Prepared Statement for the Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce on Radio Frequency Identification (RFID) Technology: What the Future Holds For Commerce, Security, and the Consumer. July 14, 2004. Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearing&docid=f:95455.pdf

Marx, G. (2001) Murky Conceptual Waters: The Public and the Private. Ethics and Information Technology, 3(3):157-169, 2001.

McHugh, J. (2004) Attention, Shoppers: You Can Now Speed Right Through Checkout Lines! Wired. Available: http://www.wired.com/wired/archive/12.07/shoppers_pr.html

Molnar, D., R. Stapleton-Gray, and D. Wagner (2005) Killing, Recoding, and Beyond. In Garfinkel, S. and B. Rosenberg, (Eds.), RFID: Applications, Security, and Privacy (Westford, MA: Addison-Wesley), 347-356.

Monmonier, M. (2002) Spying With Maps: Surveillance Technologies and the Future of Privacy (Chicago: University of Chicago Press).

Morgan, M.G. and E. Newton (2004) Protecting Public Anonymity. Issues in Science and Technology 21 (1): 83-90.

Myles, G., A. Friday and N. Davies (2003). Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing 2(1): 56-64.

National Research Council (2000) The Digital Dilemma: Intellectual Property in the Information Age (Washington, D.C.: National Academy Press).

Natsui, T. (2005) Appendix C: Guidelines for Privacy Protection on Electronic Tags of Japan. In Garfinkel, S. and B. Rosenberg, (Eds.), RFID: Applications, Security, and Privacy (Westford, MA: Addison-Wesley), 507-514.

Newitz, A. (2006) While You Were Reading This Someone Ripped You Off. Wired. May 2006.

O'Connor, M.C. (2005) SecureRF Creates New Encryption Method. RFID Journal. November 9, 2005. Available: http://www.rfidjournal.com/article/articleview/1973/1/1/

Onsrud, H. (2001) Contract Approach to Addressing Privacy in the Use of Location Based Services. Center for Spatially Integrated Social Science: LBS Specialist Meeting, Santa Barbara, CA.

Onsrud, H.J, J. Johnson, and X. Lopez (1994). Protecting Personal Privacy in Using Geographic Information Systems. Photogrammetric Engineering and Remote Sensing LX(9): 1083-1095.

Organisation for Economic Co-operation and Development (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available: http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html

Platform for Privacy Preferences (P3P) Project (2003) Available: http://www.w3c.org/P3P

Plichta, G. (2004). Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines. Available: http://www.epic.org/privacy/rfid/rfidplichta.html

Psion Teklogix Inc. (2004) Understanding RFID and Associated Applications. Available: http://www.psionteklogix.com/assets/downloadable/Understanding_RFID_and_Associated_Applications.pdf

Rieback, M. R., B. Crispo, and A.S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. Proc. 10th Australasian Conference on Information Security and Privacy. (ACISP 2005), Brisbane, Australia, July 2005. Available: http://www.cs.vu.nl/~melanie/rfid_guardian/papers/acisp.05.pdf

Rosen, J. (2004) The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. (New York: Random House).

Rotenberg, M. (2003) The Privacy Law Sourcebook 2003: United Sates Law, International Law, and Recent Developments (Washington DC: EPIC Publications).

Sarma, S., S.A. Weis and D.W. Engels (2002) RFID Systems and Security and Privacy Implications. In Workshop on Cryptographic Hardware and Embedded Systems, 2002, pp. 454-470, Lecture Notes in Computer Science. Available: http://theory.lcs.mit.edu/~sweis/ches-rfid.pdf

Schilit, B., J. Hong and M. Gruteser (2003) Wireless Location Privacy Protection. Computer 36(12): 135-137.

Senicar, V., B. Jerman-Blazic, and T. Klobucar (2003) Privacy-Enhancing Technologies – Approaches and Developments. Computer Standards & Interfaces 25: 147-158.

Shimizu, N., R. Yagiu, and M. Saito (2005) A Study of Information Services Based on Personal Belongings. Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA '05).

Shorter v. Retail Credit Co., D.C.S.C. 251 F.Supp. 329, 330

Singel, R. (2005) No Encryption for E-Passports. Wired News 2/24/05) Available: http://www.wired.com/news/privacy/0,1848,66686,00.html

Sistla, A., O. Wolfson, S. Chamberlain, and S. Dao (1997) Modeling and Querying Moving Objects. Proceedings of the 13th Conference on Data Engineering (ICDE), 1997, Birmingham, U.K.

Smith, H. and B. Konsynski (2003) Developments in Practice X: Radio Frequency Identification (RFID) – An Internet for Physical Objects. Communications of the Association for Information Systems 12: 301-211. Available: http://cais.isworld.org/articles/12-19/default.asp?View=Journal&x=60&y=8

Solove, D.J. and M. Rotenberg (2003) Information Privacy Law (New York, NY: Aspen Publishers).

Spinello, R. (2003) Cyber Ethics: Morality and Law in Cyberspace (Sudbury, MA: Jones and Bartlett Publishers).

Steinhardt, B. (2004) Prepared Statement for the Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce on Radio Frequency Identification (RFID) Technology: What the Future Holds For Commerce, Security, and the Consumer. July 14, 2004. Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearing&docid=f:95455.pdf

Swedberg, C. (2004) California RFID Legislation Rejected. RFID Journal. Available: http://www.rfidjournal.com/article/articleview/1015/1/1/

Taipale, K. (2004) Technology, Security and privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd. Yale Journal of law and Technology, January 2004.

Trans Atlantic Consumer Dialogue (2005) Resolution on Radio-Frequency Identification (RFID) April 2005. Available: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=274

Transponder News. Current Trends in Transponders Systems. Available: http://www.transpondernews.com/trends.html

U.S. Department of Health, Education & Welfare (HEW), Secretary's Advisory Committee on Automated Personal Data Systems (1973). *Records, Computers And The Rights Of Citizens.*

U.S. West, Inc. v. FCC, 182 F.3d 1224 (1999).

Vibbert, C. (1990) Freedom of Speech and Corporations: Supreme Court Strategies for the Extension of the First Amendment. Communication 12: 19-34.

Waldrop, M. (1996) The Trillion-Dollar Vision of Dee Hock. Fast Company October/November 1996. Available: http://pf.fastcompany.com/magazine/05/deehock.html

Ward, D. (2004) 5-Cent Tag Unlikely in 4 Years. RFID Journal. August 26, 2004. Available: http://www.rfidjournal.com/article/articleview/1098/1/1/

Warren, S.D. and L. Brandeis (1890) The Right to Privacy. Harvard Law Review 4.5: 193-220.

Weinberg, J. (2004) RFID and Privacy. Available: http://www.hwswworld.com/downloads/d5/weinberg.rfid.paper.pdf

Weis, S.A. (2003). Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, Dept. of Electrical Engineering and Computer Science. Massachusetts Institute of Technology. Available: http://theory.lcs.mit.edu/~sweis/masters.pdf

Weis, S.A., S.E. Sarma, R.L. Rivest and D.W. Engels (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. 1st Annual Conference on Security in Pervasive Computing. Available: http://citeseer.ist.psu.edu/cache/papers/cs/27786/http:zSzzSztheory.lcs.mit.eduzSz~sweiszSzmasters.pdf/weis03security.pdf

Weis, S.A.(2004). RFID Privacy Workshop: Concerns, Consensus, and Questions. IEEE Security & Privacy March/April: 48-50.

Weiss, A. (2004) Spying on Ourselves. netWorker. 8(2):18-24.

White, J. (2003) People, Not Places: A Policy Framework for Analyzing Location Privacy Issues. Available: http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf

Zeller, T. (2005) Personal Data for the Taking. The New York Times, May 18, 2005. Available: http://www.nytimes.com/2005/05/18/technology/18data.html

Zetter, K. (2005a) Brave New Era for Privacy Fight. Wired News. January 13, 2005. Available: http://www.wired.com/news/privacy/0,1848,66242,00.html

Zetter, K. (2005b) Feds Rethink RFID Passport. Wired News. April 26, 2005. Available: http://www.wired.com/news/privacy/0,1848,67333,00.html

Zevenbergen, J. (2004). European Privacy Law and its Effect on Location Information. Location Privacy Workshop: Individual Autonomy as a Driver of Design, Schoodic Peninsula, Acadia National Park, Maine, USA, 5-7 August 2004.

BIOGRAPHY OF THE AUTHOR

Eeva Kaarina Hedefine was born in Millinocket, Maine on January 15, 1967. She graduated from Sumner Memorial High School in East Sullivan, Maine in June, 1985. She earned an Associate of Science from the University of Maine – Augusta in Legal Technology in 1998 while working at Hale & Hamlin, LLC, a law office in Ellsworth, Maine. After her introduction to the SIE department through a boundary law course, she decided to pursue a career in engineering and earned a Bachelor of Science degree from the University of Maine – Orono in Spatial Information Engineering as Magna cum laude in 2002. Then she decided to pursue a Master of Science degree in Spatial Information Science and Engineering. While earning the master's degree Eeva served as a National Science Foundation GK-12 Fellow, working with local middle schools and high schools in the area of sensor technologies.

Eeva is a candidate for the Master of Science degree in Spatial Information Science and Engineering from The University of Maine in August, 2006.