



5-2005

A Study on the Ethical Implementation of Radio Frequency Identification Technology in Retail

Aaron Ingoglia

[How does access to this work benefit you? Let us know!](#)

Follow this and additional works at: <https://commons.und.edu/theses>

Recommended Citation

Ingoglia, Aaron, "A Study on the Ethical Implementation of Radio Frequency Identification Technology in Retail" (2005). *Theses and Dissertations*. 5370.

<https://commons.und.edu/theses/5370>

This Independent Study is brought to you for free and open access by the Theses, Dissertations, and Senior Projects at UND Scholarly Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of UND Scholarly Commons. For more information, please contact und.common@library.und.edu.

A STUDY ON THE ETHICAL IMPLEMENTATION OF
RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN RETAIL

by

Aaron L. Ingoglia
Bachelor of Science in Industrial Technology, University of North Dakota, 2003

An Independent Study

Submitted to the Graduate Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

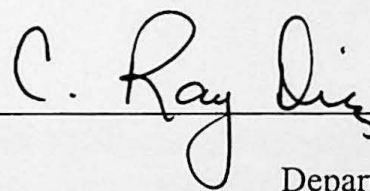
Master of Science in Industrial Technology

Grand Forks, North Dakota

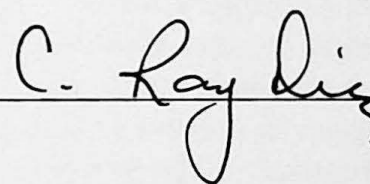
May
2005

Copyright 2005 Aaron Ingoglia

This independent study, submitted by Aaron L. Ingoglia in partial fulfillment of the requirements for the Degree of Master of Science in Industrial Technology from the University of North Dakota, has been read by the Department Chair and the Advisor under whom the work has been done, and is hereby approved.



Department Chair



Advisor



Student

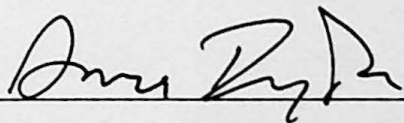
PERMISSION

Title: A Study on the Ethical Implementation of
Radio Frequency Identification Technology in Retail

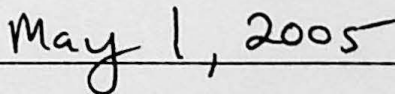
Department: Industrial Technology

Degree: Master of Science

In presenting this independent study in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my independent study work or, in his absence, by the chairperson of the department or the dean of the Graduate School. It is understood that any copying or publication or other use of this independent study or part thereof for financial gain shall not be allowed without my written consent. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my independent study.



Signature



Date

TABLE OF CONTENTS

ABSTRACT	vii
CHAPTER	
I. INTRODUCTION.....	1
Introduction of Topic	1
Statement of Need	3
Statement of Problem / Purposes of Study.....	3
Guiding Research Questions	4
II. REVIEW OF LITERATURE.....	5
Point-of-Sale Technology	5
Universal Product Code	5
Radio Frequency Identification.....	7
Privacy and Security Concerns	9
Technology Controversy	16
The Value of a Consumer's Personal Information.....	20
The Debate Over Restrictions	25
Current Laws on Consumer Privacy	27
Proposed Legislation on RFID Tagging.....	30
III. METHOD.....	34

IV.	RESULTS.....	36
	A Plan for the Ethical Implementation of Radio Frequency Identification Tagging in Retail	36
	Consumer Bill of Rights for Radio Frequency Identification Tagging	37
	Technology Awareness Policy	38
	Point-of-Sale Protection Program	40
V.	DISCUSSION	41
	Summary	41
	Conclusions	44
	Recommendations	45
	REFERENCES.....	46

This study is dedicated to my father

Gary Ingoglia

The greatest man I ever knew.

May you finally be at peace.

Thank you for all of your T...I...M...E.

Your memory will always be with me...always.

ABSTRACT

Long checkout lines at the grocery store can be very frustrating. Thanks to point-of-sale technology though, those lines aren't nearly as long as they could be. Point-of-sale technologies have been developed and implemented worldwide to help reduce the amount of time it takes a consumer to pay for products at the cash register. These technologies have also aided retailers and manufacturers in achieving higher levels of efficiency. Bar codes, for example, were first developed to decrease the amount of time required to purchase an item, improve the tracking of inventory, accelerate the acquisition of important statistical data, and facilitate market research. Now, retail store owners have their eyes on a more modern and advanced point-of-sale technology- radio frequency identification (RFID). Unlike manually scanning a bar code, this recently developed point-of-sale technology uses a tiny chip to wirelessly transmit data to a reader computer. RFID promises greater efficiency in retail than the bar code with respect to purchase time, inventory tracking capability, collection of important statistical data, and valuable market research. All of this could add up to greater profits for retail businesses, cheaper prices for consumers, and less time spent standing in line at the checkout. Although these promises sound beneficial, the use of RFID technology might also create privacy concerns for consumers. Many American consumers are not aware of the vast amount of personal data businesses gather on their customers, or what exactly they do with it. RFID technology will increase the retailer's ability to gather and store personal information on consumers. This raises the possibility for invasion of consumer privacy. Therefore, this

research paper was initiated to answer the question of whether or not radio frequency identification technology has the potential to invade consumer privacy rights. The aim of this research was to study how to ethically implement RFID technology into retail in a way that protects consumers against the invasion of their privacy. It first looked at Universal Product Code technology in the development of today's bar codes. Then, it defined radio frequency identification technology. It discussed the importance of carefully examining this, as well as any, new technology and centered on the controversy that surrounds RFID. It examined privacy and security concerns for the retail consumer and explored the value of a consumer's personal information. It also focused on the debate over restrictions, current laws on consumer privacy, and proposed legislation on RFID technology. From this study, the researcher deduced that RFID technology had the potential to invade consumer privacy rights. It was also found that a consumer's personal, identifiable information was protected under the Constitution as private property. It was concluded that a set of protective guidelines was necessary for the security of a consumer's personal, identifiable information. Therefore, a proposed plan for ethically implementing radio frequency identification technology into a retail business was created. This plan included a Consumer Bill of Rights for Radio Frequency Identification Tagging, Technology Awareness Policy, and Point-of-Sale Protection Program.

CHAPTER I

INTRODUCTION

Introduction of Topic

Efficiency is a top priority in industry. Businesses are constantly looking for ways to make their companies more efficient. If something can be done better and faster, increased profits can result. Any new technology designed to increase efficiency quickly gets adopted into industry.

This is true with respect to point-of-sale technology for the retail industry. The Universal Product Code (UPC), or more commonly referred to as the bar code, was first developed to "...speed up checkout counters and eliminate the drudgery of physical price marking" (Schmidt, 2001, p. 80). Cashiers were consuming major blocks of time having to manually punch in each item's long product code number.

According to Scanlon (2003), the old way of manually entering product codes all changed though in 1974, in Troy, OH, when "...a package of Wrigley's chewing gum was the first item scanned using the Universal Product Code" (p. 80). This standardization of coding created an individual number for each class of product sold. These product code numbers could now be rapidly entered, counted, and tracked worldwide.

Since the introduction of bar code technology into industry, retail businesses have seen substantial increases in efficiency. "It (UPC) eliminated the need for manual

pricing, resulting in lower-priced products. Checkouts became faster and more accurate, saving consumers time and money. The UPC also allowed retailers and manufacturers to manage and replenish inventory more efficiently” (Tarnowski, 2004, p. 26). The increase in efficiency at the point-of-sale was why the UPC was so widely adopted into the retail industry.

Advancements in point-of-sale technology do not end with UPC labeling though. Now there is pressure from industry to begin using an even more efficient point-of-sale technology- radio frequency identification tags. Radio frequency identification (RFID) tags are tiny microchips powered by a remote reader and can transmit, in real-time, large amounts of digital information via radio signal. According to the official website of Alien Technology (2005), a leader in the manufacturing of RFID chips,

In its (an RFID chip’s) simplest form, an integrated circuit on a small silicon chip is attached to a small, flexible antenna, creating a tag. The integrated circuit provides data storage to record and store information. A reader sends a signal to the tag. The tag absorbs some of the RF energy from the reader signal and then reflects the RF energy as a return radio signal containing information from its memory. (What is RFID section, ¶ 1)

This has the retail industry eagerly anticipating the day when all products will be able to communicate their location, in real-time, without the help of a single human finger.

It seems though that retailers have forgotten about consumer rights. All of this added technology could facilitate the collection of a consumer’s personal information without his or her consent. This personal data collected on shoppers might be more than

what is necessary to increase efficiency. Radio frequency identification technology may have the potential to invade a consumer's right to privacy.

Statement of Need

The need for this study was to determine how RFID can be used, what rights consumers have to privacy, how RFID could invade these consumer privacy rights, and what guidelines are needed to better protect consumers against the invasion of their privacy. To that end, this study will first benefit consumer-conscientious retail businesses that envision using radio frequency identification technology. It will provide them with a plan for the implementation of RFID in a way that values their customers' right to privacy, while also considering the growing need to instantaneously track merchandise in an effort to maximize efficiency. Second, this study will benefit consumers by providing guidelines outlining the necessary protection needed to help guarantee their rights to privacy. The study should result in a balanced plan for the implementation of radio frequency identification that benefits both customer and retailer.

Statement of Problem / Purposes of Study

Radio frequency identification technology, used in retail, might have the potential to invade consumer privacy rights. Therefore, the purposes of this study were to determine if this potential exists and develop a plan for the ethical implementation of RFID technology in a retail business.

Guiding Research Questions

The questions that guided this research were:

1. What are the point-of-sale technologies in retail that facilitate the collection of data?
2. Why is it important to carefully examine radio frequency identification chip technology? What controversies surround this newly emerging technology?
3. Are there concerns with consumer privacy and security that arise from RFID technology?
4. What is the value of a consumer's personal information? Why should companies consider creating a trusting relationship with their customers?
5. What is the debate over restrictions for the use of RFID technology?
6. What laws have been passed on consumer privacy?
7. What legislation is currently being proposed to protect the privacy of consumers using RFID technology?
8. What should a comprehensive plan for the ethical implementation of radio frequency identification tagging in retail contain?

CHAPTER II
REVIEW OF LITERATURE

Point-of-Sale Technology

Universal Product Code

Modern point-of-sale technology has come a long way. The first conception of gathering and processing retail data began around the mid-point of the Twentieth Century. According to Scanlon (2003),

In 1948 the president of a grocery store chain in Philadelphia implored a dean at Drexel Institute of Technology to develop an automated checkout system. Silver, a graduate student, overheard the conversation and was instantly intrigued.

Woodland, a friend and fellow grad student, shared Silver's enthusiasm, and the two devoted themselves to the effort. In late 1949 they applied to patent a system that drew on aspects of Morse code and movie sound systems. Similar to today's bar code scanners, their device used a light source and photosensitive reader to translate data encoded in linear symbols. (p. 80)

Silver and Woodland's invention was unfortunately too inconvenient for practical use at the register. Grocery stores weren't interested in the newly developed technology "... because it required a blindingly bright, extremely hot 500-watt incandescent light bulb and a large, unwieldy vacuum-tube photomultiplier to process data, the invention wasn't appealing for widespread use in grocery stores" (Scanlon, 2003, p. 80). The stores

were just not willing to integrate this bulky and bright advancement in point-of-sale technology.

It took about ten more years for retailers to finally realize the importance of Silver and Woodland's invention. Scanlon (2003) revealed that it wasn't until the late 1960s, when a "laser could provide an intense, low-heat light source" (p. 80), did the idea become practical. During this same period of time, "processors were becoming small and inexpensive enough for commercial use" (p. 80). Both of these advancements in technology during the 1960s helped Silver and Woodland's idea of an advanced point-of-sale system move closer to becoming feasible. Then in 1974, in Troy, OH, "...a package of Wrigley's chewing gum was the first item scanned using the Universal Product Code" (p. 80).

The Universal Product Code (UPC), also known simply as the bar code, was a new advancement in point-of-sale technology that quickly spread around the retail world. What began as an attempt to increase efficiency in retail swiftly turned into a worldwide crusade to categorize everything produced and sold. "Far exceeding initial expectations, five billion codes are scanned every day in 140 countries" (Schmidt, 2001, p. 80).

In their simplest form, UPCs are just groups of identification numbers specific to each product. The code is divided into two sections. The first set of numbers indicates which manufacturer produced the product. The second set of numbers distinguishes the actual item number. There is also a number system character to the far left of the UPC code. This character reveals which product group the item falls under. To the far right of the UPC code is a check digit. This digit is only used to insure the code's accuracy.

Every UPC must be coded into a decipherable form, since computers can only read bits (electronic ons and offs). Each digit, zero through nine, is given a unique, recognizable code. These codes are transcribed into various combinations of lines, each with different thickness and spacing. The width of the lines and spacing relate to the series of bits that each digit is assigned. A laser is then used to scan across the series of lines and read each line's thickness and spacing. The data is entered into a computer as a series of digits. These digits are then processed and stored in the computer as product codes.

Products are now able to be scanned much faster than manually punching in the entire product code by hand. This eliminated much of the human error involved in point-of-sale transaction. On the other hand, it facilitated the collection of consumer purchase data. "All of this information is valuable, and the only way it can be reliably collected and collated is through technology- point of sale [sic] systems hooked up to a database" (Greiner, 1997, p. 9). Such data could include: name of customer, date and time of transaction, name of product, type of product, amount of product, price of product, payment method, location of purchase, and whether or not the item was on sale.

Radio Frequency Identification

Although UPCs still are working well in today's market, they could pose some drawbacks. "Bar codes have limitations- they need to be scanned with a laser and are confined to individual product types, such as a five-pack of the Mach3 razor blades" (Clark, 2003, p. 1566).

Recently, the retail industry has become interested in a more advanced point-of-sale technology. This technology, called radio frequency identification (RFID), does not

limit product identification codes to only groups of individual products. Each individual product is given a unique code. One box of spaghetti, for example, could be marked with a unique number, different from all other identical boxes of the same spaghetti. "The Electronic Product Code- essentially a long number programmed into the RFID tag- could identify each...package individually" (Clark, 2003, p. 1566).

Putting a minute, readable chip on merchandise could also eliminate the need to manually keep track of inventory. "One of the big benefits is that RFID systems would theoretically eliminate the need to conduct inventories by hand" (Rosen, 2001, p. 22). Retail businesses across the nation are euphoric in learning that this technology has the potential to cut down the massive cost of manually keeping track of inventory.

Radio frequency identification tags accomplish the same basic job of identifying and tracking products as UPSs do, but have a much higher capability to store information. "Stored in the memory of the tag's chip, the code uses 96 bits...enough information to uniquely identify trillions upon trillions of objects" (Schmidt, 2001, p. 80).

The RFID tag's extreme capacity for data storage will allow for the numbering and tracking of every individual retail item in the world. "Bar codes identify only classes of products, not individual items, whereas a digital numbering scheme built into a (radio frequency identification) tag has the capacity to identify every single manufactured item that is currently made and sold" (Schmidt, 2001, p. 80).

The way a radio frequency identification tag functions at the basic level is relatively simple. By itself, the chip is a powerless, inactive tag. The chips must be powered-up by some form of energy. Schmidt (2001) detailed that these chips remain dormant until activated by a "reader" computer. When the chip's physical location

comes within range of the reader, the “tiny silicon chip...boots up and transmits a signal when exposed to the energy field” (p. 4). The chip then sends out a digital signal of the product’s identification number back to the reader. This allows for the instantaneous tracking of the chip, from birth to death. Unlike bar codes, the miniature chips are also capable of being placed within the product in an undisclosed location.

This relatively new technology opens huge doors of opportunity for manufacturers. According to Schmidt (2001),

Manufacturers hoping to recoup some of the billions lost every year to theft, counterfeit, and depleted stocks have been closely watching....The ultimate goal is to put a radio tag on virtually every manufactured item, each tracked by a network of millions of readers in factories, trucks, warehouses and homes, transforming huge supply chains into intelligent, self-managing entities. (p. 80)

This tracking of every item from creation, to point-of-sale, and finally product termination, will allow both the manufacturer and retailer to operate at even greater levels of efficiency. “Linda Dillman, CIO of Wal-Mart...described how RFID can greatly assist its inventory planning, allow faster demand response, (and) provide a more accurate accounting of inventory, while also increasing efficiency” (Microwave Journal, 2003, p. 65).

Privacy and Security Concerns

Although point-of-sale technology was designed to increase efficiency in product sales, inventory, and distribution; it seems that industry has quickly become addicted to collecting and analyzing consumer information. The availability of this consumer

information could greatly increase with the industry-wide push for RFID tagging. Brandt (2004) wrote,

One day, not long from now, virtually any store, restaurant, or business may be able to identify you, note what clothing you're wearing-and possibly even detect how much money you have in your wallet-as you enter the establishment. (p. 40)

At the surface, RFID tagging seems wonderful to the ordinary consumer. Lower prices and faster service are promised from the increase in tracking efficiency. What most consumers aren't aware of is how RFID tagging grants retailers and manufacturers the capability to track information past the point-of-sale. "That's what worries privacy advocates: how easily companies can read the tags and keep logs, identifying and profiling consumers long after the tagged products those consumers bought leave the store" (Brandt, 2003, p. 40).

All this talk about following a consumer's every move sounds a little too much like Big Brother, right? In the first place, in order to follow a consumer home and track what happens to the product, one would need a multitude of reader computers set up in each buyer's residence. Companies would have to invest large amounts of capital for these reader computers. No company would invest such an amount for the sole purpose of gathering marketing data. What if though retailers and manufacturers could persuade the consumer to purchase all those reader computers? Sounds like a silly question, huh? But this is exactly what is happening today with the idea of smart homes.

Smart homes are becoming more and more intelligent with advancements in radio frequency identification technology. These houses are fitted with "smart" appliances, developed to utilize RFID tagging to aid in everyday household tasks. Many of these

smart appliances are equipped with radio frequency reader computers so individual retail items may be identified. The justification for this identification is, once again, to increase efficiency.

What makes a “smart” home intellectually superior to a traditional residence is autonomous communication. The more a networked system within a house is able to independently communicate with either itself or other systems, the more points it scores on the “smart scale”. That is why designers have been working diligently to create a self-governing, residential smart system capable of communicating both inside and outside the home. “Everything in the house has a little brain that’s wirelessly connected to a big network. Everything talks to everything else. What’s known in one place is known throughout the network” (Hunter, 2002, p. 39).

This network communicates with the help of high-speed connections throughout the smart home. “Fully wiring a home means that high-speed phone and cable wiring will be as accessible in different places within the home as electrical outlets are now” (Conhaim, 1999, p. 6).

There seems to be no limit as to what could get hooked up to this network of communication within the home. According to Conhaim (1999),

Smart or automated homes may include the following components: use of computer or cable to control home operations; automatic thermostat adjustments, sprinkling operation, lighting, and even draperies; remote control of appliances; intercom system; and use of video, motion sensors, video cameras, and alarms to provide security. (p. 6)

Smart homes of the future will radically change the way appliances operate efficiently, thanks to radio frequency identification. Brody (2002) noted the following:

Internet-linked refrigerators and freezers can allow the user to record what is in the appliance and to reorder online each time a product is consumed. In the future, these appliances can be fitted with RFID (radio frequency identification) antennas that will read the contents of the refrigerator and freezer and the use-by dates. (p. 66)

As it is with traditional homes, the kitchen will probably be the center of activity for the smart home of the future. Maynard (2003) postulated that the refrigerator will soon be the network control center for the smart house. He agreed that the smart fridge will control such things as the television, dishwasher, lighting, air conditioner, garage, and security system.

All the hype over smart homes has many eagerly anticipating for the right moment when the technology becomes available at a decent price. But slow down a minute before deciding to wire up! There are some serious concerns consumers might be overlooking. Smart homes will compile a tremendous amount of personal data. “Meanwhile, the most personal data possible—stuff that describes my body, my activities in private, and relationships—are piling up” (Hunter, 2002, p. 47). The whole idea wouldn’t sound too threatening as long as the smart home network was isolated from the rest of the world. The entire system though is capable of connecting to the Internet. This outside accessibility into the smart home’s network could be volatile if not properly cared for. Hunter (2002) continued,

It’s as if the stuff (personal data) is radioactive. I can’t just dump it somewhere,

because it's dangerous for at least the next thousand years, especially if it gets into the wrong hands, which is hard to anticipate. How can I possibly know whether the company that does good things for me today is going to be bought out by a bad company tomorrow? (p. 47)

The idea of using RFID in a smart home that is connected to the Internet could facilitate the misuse of one's personal information. Outside access, deemed necessary by the retail industry for increased efficiency, to private information collected within the smart home may become tempting for other sectors of the corporate world. "Ultimately the information may be of interest to many others as well. Insurance companies...might like to know if there are any cigarette packages in the insured's home, whether she snacks regularly, and how often she eats fatty foods" (Froomkin, 2000, p. 1461).

This access into the home could be used to advertise, or even invade families, with unwanted material. "Any such two-way linkages raise privacy and security issues. Will any vendors be able to track shopping patterns and bombard homeowners with unwanted advertisements? How will children using their neighborhood networks be protected from unwanted intruders?" (Conhaim, 1999, p. 7).

If this technology makes it possible for legitimate companies to gather personal data from inside the home, what happens when this information gets into unlawful hands? Hunter (2002) wrote,

We can assume, for the moment, that anyone who wants to hack your house is either a criminal or a government agent. Criminals don't play by the rules, so if you're being hacked by a criminal, you can expect bad things to happen. As an example of the bad things, consider the potential for identity theft in an

environment in which much of the information needed to establish identity is transmitted wirelessly. (p. 45)

Take, for example, the use of surveillance when smart homes are fitted with wireless cameras. Once those cameras are in place, control over the property, in real-time, can begin. All of this control is great, if you are the protective father concerned about your family. But what if someone hacks into the surveillance system to get a virtual picture of what's going on inside? "That surveillance technologies threaten privacy may not be breaking news, but the extent to which these technologies will soon allow watchers to permeate modern life still has the power to shock" (Froomkin, 2000, p. 1461).

As the smart house of tomorrow begins to be a reality of today, privacy and security are critical issues that must be considered in relation to RFID tagging.

According to Hunter (2002),

The same issue- the *hackability* of the bit stream- arises with every wireless device and every wireless communication, but it seems particularly acute in this case. What goes on in one's house is the most private of all private information. It's also acute because it's easier for someone who wants to know about you to find you at your house, compared to following you in your car or on the street. (p. 45)

Many RFID enthusiasts are defending their positions that consumers can rest at ease knowing their personal information is only used to increase efficiency. "For us, the idea of this project (Benetton Group's test plan of embedding chips into its Sisley clothes

line) is to substitute the bar code technology in order to manage the supply chain in a better way,' said Sartor" (Clark, 2003, p. 1567).

The Italian clothes manufacturer Benetton Group may be interested in this point-of-sale enhancement with honest intentions, but what happens when personal information is made available to someone whose motives are less altruistic? "Unpleasant implications surface when these collectors of information...start selling the data. And don't delude yourself -- they do...what if someone with access to the database decides to peddle it to the highest bidder, regardless of their plans?" (Greiner, 1997, p. 9). This could be a potential threat to consumers if just the right kind of information made its way into the hands of someone with malicious intentions.

Only time will tell if manufacturers and retailers end up misusing RFID technology. For the moment, industry must seriously consider present consumer fears, rather than ignore public discomfort, if the technology is even going to survive into the future. Yoshida (2003) wrote,

Concerned over public perceptions that radio frequency identification chips are an invasion of privacy that could track an individual's buying habits, several chip makers are building a "kill" command into their upcoming RFID chips. Initial prototypes with the feature, which effectively removes a chip's ability to communicate, are expected to be available in June. The kill feature arrives as Italian clothier Benetton Group has backpedaled from a plan to embed RFID labels, based on Philips Semiconductors' I. Code chips, in millions of its garments. After the plan was made public, a backlash ensued that led to the formation of Boycott Benetton, a group that opposed the clothier's and other's

planned use of RFID tags to track products through the manufacturing and supply chains. Benetton now says it is reevaluating the plan's "potential implications relating to individual privacy". (p. 1)

Although RFID chips are being mass-produced with build-in self-destruct features that render the chip useless after the point-of-sale, many consumers will still be wary. The built-in kill feature might be difficult for shoppers to trust. Yoshida goes on to write the following concerning a built-in kill feature for RFID chips:

At the same time, Ischebeck (senior director for Identsystems in the Secure Mobile Solutions business group of Infineon Technologies AG) cautioned, "Just because an engineer said he has just deactivated your RFID tag, would you believe him? I wouldn't trust an engineer, because there is no way to prove it." The surest way to respond to privacy worries is to "take a pair of scissors and cut off the RFID tag yourself. Trust no one," he said. (p. 1)

Technology Controversy

Human beings, compared to many other mammals, are quite vulnerable in their natural state. With no thick hide, advanced immune system, hard shell, or disguise mechanism, humans are very susceptible to environmental extremes, predators, and sicknesses. They are slow on their feet, unable to leap great distances, unsuitable for swimming, and lack the ability to fly or glide. "Left with only their innate physical capabilities...humankind is a physically puny bunch" (Volti, 2001, p. 4). One of the reasons the human race has been able to survive for as long as it has could be because of

our ability to manipulate technology. Volti (2001) wrote,

...compensating for this physical weakness is an intelligence that is the ultimate source of technology. Humans stand apart from all other animals in their ability to gain and transmit knowledge, and to use this knowledge to develop tools and techniques. Without this capacity to invent and use a great variety of technologies, members of the human species would have never been able to establish themselves on virtually every part of the globe. (p. 4)

Humans have been created with a unique ability to reason out technology. Our level of intellectual capacity to reason things out has set us apart and above all other creatures on the earth. According to the book of Genesis in the Bible,

God created man in his own image, in the image of God he created him; male and female he created them. God blessed them and said to them, "Be fruitful and increase in number; fill the earth and subdue it. Rule over the fish of the sea and the birds of the air and over every living creature that moves on the ground".

(Genesis 1:27-28, New International Version)

This gift of cognitive reasoning was given to mankind to be a blessing. The ability to reason out and use technology allows humans to enhance their innate capabilities to perform work. With this endowment though also came the freedom of choice. Unfortunately, mankind has not always chosen to use their gift with pure intentions. Volti (2001) wrote the following:

Today, manned bombers fly well over twice the speed of sound, the battlefield has been transformed by electronically guided "smart" missiles, and our lives are threatened by intercontinental ballistic missiles (ICBMs) with nuclear warheads

that could destroy our cities in a matter of minutes. On the not-too-distant horizon are laser “death rays”, bacterial weapons, enhanced radiation bombs, and many other ghastly instruments of mass murder. (p. 251-252)

Advancements in technology present unclear moral questions. This ethical vagueness is why constant examination is crucial for every new technology used by mankind. Radio frequency identification chip technology is no exception. “...they (consumers) need to be better educated about the technology’s (RFID chips) benefits and potential for misuse” (Information Week, 2003, p. NA).

If advancements in technology are left unchecked, the tools used to enhance one’s innate capabilities to perform work could take control of those very same human faculties. An example of this is the implantation of RFID chips in humans. Like many other new technologies used by mankind, human chip implantation started as a harmless way of enhancing one’s natural ability to perform work. The idea of implanting an RFID chip first began by placing one outside the body. According to Merritt (2003),

The company’s (VivoMetrics) top priority is working more complex, less invasive sensors into the LifeShirt for measuring heart rate, brainwaves and other critical factors. Vivo is working with one company to develop a lightweight sensor that can track heart rate through clothes. BodyMedia (Pittsburgh) aims to enable such products with its SenseWear transceiver that Roche Diagnostics will start selling this summer in a \$300 to \$400 armband for weight-reduction monitoring. (p. NA)

Since these outer-body monitoring chips could be lost or destroyed, researchers took the next “logical” step of implanting the chips inside the human body. Merritt (2003) continued,

Beyond the wearable medical devices, researchers are exploring implantable chip-level devices on many fronts. Perhaps the most challenging and fascinating of these involves neural prosthetics, implantable silicon neurons that could some day carry out the functions of a part of the brain that’s been damaged by stroke, epilepsy or Alzheimer’s disease. (p. NA)

The possibilities of neural chip technology do not end with aiding damaged neurological functions. It could offer people with perfectly good brain functions an upgrade. According to Maguire and McGee (1999),

Computer visionaries predict that within our lifetimes, implantable computer chips acting as sensors, or actuators, may not only assist failing memory but even bestow a variety of capacities. With their aid, we may acquire fluency in new languages or “recognize” people we have never met. (p. 7)

Stambler (1990) explained how this neurological chip implant works in the following:

The chip contains a series of 8 to 16 [micro]m dia holes surrounded by indium microelectrodes that can either record electrical activity in a regenerated nerve or can transmit electrical signals to stimulate nerve activity. Initially, a chip does not contain any nerve fibers. But fibers from the end of the animal’s severed nerve regenerate through the holes to reconnect with nerve ends on the other side. The regenerative action has been demonstrated in tests with rats. (p. 130)

Implantable RFID chip technology is an ethical matter that should be seriously considered before continuing on with the technology. According to Maguire and McGee (1999),

Clearly, the technology for implantable devices is becoming available, at prices that make it cost effective. Three stages in the introduction of such devices can be delineated. The earliest adopters will be those with a disability who seek a more powerful prosthetic device. The next stage represents the movement from therapy to enhancement. One of the first groups of non-disabled "volunteers" will probably be in the professional military, where the use of an implanted computing and communication device with new interfaces to weapons, information, and communications could be life-saving. The third group of users will probably be people involved in information-intensive businesses who will use the technology to develop an expanded information transfer capability. The first prosthetic devices should be available in five years, with prototypes starting within ten years, and information workers using prototypes within fifteen years; general adoption will take roughly twenty [sic] to thirty [sic] years. (p. 7)

The Value of a Consumer's Personal Information

One does not need to look very far to see that many existing businesses do not assign a high value to customer trust. Unfortunately, these companies have been poorly educated as to how much customer trust is directly tied to increased profits. Businesses across the nation have still not figured out that they are only as good as their customers. Superficially, it may cost more to cater to customer trust. Underlying this small increase

in cost though is a gold mine of loyalty. There is a large market of loyal customers just waiting to pay a little more in exchange for a deeper feeling of trust. "Perhaps the single most valuable asset a bank can have is people's trust. And it is all too easy to forget the essential role trust plays in long-term sales success" (Brooks, 1999, p. NA). Although this is a banker's view of the value of trust, the same can be said for any company with customers.

Trust is a key ingredient for cementing a long-lasting relationship between company and customer. "Trust is essential if you are involved in a relationship-based sale" (Brooks, 1999, p. NA). Without a foundation of trust, customers won't build any significant relationship with a company.

Establishing a trusting relationship with customers can prove to be very beneficial. Not only can a company count on their customers for long-lasting loyalty, referrals about the level of trust can also quickly spread. Word-of-mouth advertising can cut down marketing costs significantly. Referrals have a very high batting average for scoring new customers in the game of advertising. "Referrals generate the highest-quality clients and engagements" (Bergholz & Nickols, 2001, p.25). A potential customer will feel more confident walking through the doors of a company for the first time if a friend, whom they trust, highly recommended the service.

Those companies that have tuned in to the idea of valuing customer trust have seen their businesses climb over the competition. Enterprise Rent-a-Car is a perfect example. James and LaMotta (2003) wrote,

Enterprise (Rent-a-Car's)...philosophy is "Put customers first and employees second, and profit will take care of itself." Enterprise outran Hertz and Avis to

become the largest car rental firm in North America. It continues to grow at more than 20 percent per year in a sluggish industry. With some 45,000 employees, the company hires more college graduates than any other firm in the country.

Enterprise's CEO has said that "a major difference between Enterprise and our competitors is that their business is cars and ours is people". (p. NA)

Enterprise Rent-a-Car understands the value of gaining people's trust. One of the reasons they have experienced such success in the rental car industry is because of their commitment to customer trust.

Customers who feel they are being treated as valuable assets will continue bringing their resources back to that particular company time and again. James and LaMotta (2003) revealed how Northwestern Mutual Life Insurance Co. has "...consistently focused on creating superior value for its policyholders" (p. NA). Because of its careful attention to value, this once-quiet insurance company has "...successfully parlayed its superior customer retention into lower costs and faster growth..." (p. NA), becoming the "...industry leader in individual life insurance" (p. NA). It is a well known fact that much of the money a company spends in advertising is trying to get the customer to use the product or service for the first time. It is much less costly to keep a customer loyal than to continually look for new ones.

Current technology allows businesses access to large amounts of consumer data. Contemporary businesses must respect their relationship with their customers when using technology if they are to continue to be successful. Cannon (2002) commented on the issue of customer trust and technology usage in the following:

Today, every information manager and technologist faces the challenge and added

responsibility of safeguarding the corporation's greatest asset: customer trust. Technology has advanced to a state where collection, enhancement, and aggregation of data are instantaneous. Corporations now have the technology to analyze the finest details about each customer. They can determine the most profitable clients and tailor their marketing messages accordingly. Information can be collaborated upon across the enterprise so the customer hears a single voice. While this ability is a positive development for the corporation and means better services for the client, it also adds a level of anxiety if the aggregation is not performed correctly and appropriately. (p. 42)

This accumulation of personal information from customers is becoming more and more accessible through continued advancements in technology. This high-accessibility to information could facilitate the misuse of it. "Technology allows the easy accumulation and distribution of personal financial data as well as the theft of these data" (Pugliese and Kravitz, 2000, p. 29).

It seems that current technology has so much potential to gather and misuse personal information, customers are eager to invest in businesses that will protect their date of birth, Social Security number, and mother's maiden name. According to an article written by Culnan and Bies (2003),

Managing the second exchange in a consumer transaction by treating the consumer's personal information fairly, then, is essential to building trust in a customer relationship. For consumer marketing, a central element of procedural fairness is the ability of individuals to remove their names from marketing lists before they are used or shared. In the offline world, this is typically done using an

“opt-out” where a consumer's information will be used for marketing unless he or she objects. (p. 323)

Communication is also an essential ingredient for a trusting relationship between customer and company. Companies eager to acquire loyal clients will openly communicate with a client any changes in the company that will directly affect them. In doing so, the client feels they are being considered in the company's decision-making process. “Never let customers be blindsided. Alert them about issues that will affect them. Do this even if it is painful. Be sure to give as much notice about anything that affects them as early as possible” (Brooks, 1999, p. NA). Communication is a key element in a trusting relationship. When communication breaks down, so can the relationship.

Companies in the retail industry gearing up to embrace radio frequency identification tagging are faced with the very important decision of whether or not to place their value in customer trust or the technological prophesy that collecting more data will earn higher revenues. A choice must be made to either listen to consumer opinions on RFID or not. So what exactly are consumer opinions on RFID? Kirsche (2004) stated in an article about gaining consumer trust with the use of RFID that,

A recent Cap Gemini Ernst and Young survey of 1,000 consumers about their attitudes toward radio frequency identification provides insight, including concerns, perceptions-and misperceptions--that retailers can use when incorporating RFID with the retail setting. While the retailer and supplier world is familiar with the technology, or increasingly is becoming so, 77 percent of consumers surveyed had never heard of RFID... Sixty-nine [sic] percent of

survey respondents said they were concerned that information gleaned from RFID tags would be used by a third party, 67 percent said they were afraid they would be hit with more direct marketing, and 65 percent said they were concerned they would be tracked through their purchases. A small percentage also cited health and environmental concerns. (p. 1)

This technology is a new one for the customer. Fear and anxiety are bound to grow in the buyer's heart if companies don't address the issue of trust.

Since they are the ones ultimately paying for it all at the cash register, consumers deserve to be factored into the privacy equation when discussing the ethics behind radio frequency identification. According to Culnan and Bies (2003),

Consumer privacy is at the center of an ongoing debate among business leaders, privacy activists, and government officials. Although corporations face competitive pressures to collect and use personal information about their customers, many consumers find some methods of collection and use of their personal information unfair. (p. 323)

Many customers seem to feel that some of the ways industry collects their personal information is unwarranted. If so, the next logical step would be to look at restrictions.

The Debate over Restrictions

Radio frequency identification is a relatively new technology. Laws on the subject are still in the infancy stage. Regulations too stiff will hinder commerce. No control suggests that consumer rights are worthless. While government battles with business to create some form of fair consensus, consumers are left in the middle.

Consumers are just not willing to sit back and let business have free reign in the decision over the protection of their personal information. Consumers, for example, recently expressed their opinions on the importance of protecting their private information when using the Internet. Garfinkel (2000) wrote,

There's a growing disconnect between American consumers and business on privacy and data protection. Consumers want Congress to step in and pass strong laws to protect information privacy, both online and off-line. A recent BusinessWeek/Harris poll found that 57% of Americans believe that "the government should pass laws now for how personal information can be collected and used on the Internet," while only 15% believe that voluntary privacy standards are the way to go. (p. 30)

Business can't continue to ignore consumers like they might have done in the past.

Today's consumer is a concerned and educated shopper. He or she realizes the value of privacy and is ready to protect it by demanding stiffer regulations.

Businesses are fighting any regulation at all on RFID, saying that this technology is too new to place restrictions on. According to Garfinkel (2000),

Businesses, on the other hand, argue that the current voluntary standards are working quite well, thank you very much. What's more, say businesses, any regulation would be premature: We're still in the early days of the Internet boom, and any fiddling with the Net's magic formula of pervasive surveillance and unbridled personal data collection might irreparably harm the engine that has been creating so much of the country's new wealth. (p. 30)

Again, one can see how some companies are overlooking the value of customer trust.

One possible solution that might insure consumers get what they are asking for regarding the value of their personal information, as well as allow businesses the opportunity to make use of RFID to improve efficiency, is to create a set of protective guidelines for all retail businesses to follow when utilizing the technology. These guidelines could include a much needed bill of rights for consumers using RFID in retail. Such a bill of rights has already been proposed by Garfinkel (2002). He wrote that consumers deserve the following rights:

The right to know whether products contain RFID tags. The right to have RFID tags removed or deactivated when they (consumers) purchase products. The right to use RFID-enabled services without RFID tags. The right to access an RFID tag's stored data. The right to know when, where, and why the tags are being read. (p. 35)

American consumers want to feel more secure about the use of their personal information when doing business with retail companies that employ RFID technology. Businesses want to use this technology to increase levels of efficiency. A set of protective guidelines, that includes a bill of rights for RFID, will most likely build customer trust and still allow for the use of the technology in retail.

Current Laws on Consumer Privacy

Radio frequency identification is a relatively new technology for the general public. As such, no laws exist that specifically address consumer privacy and the use of RFID technology. Although Congress has not yet penned into law anything directly tailored to RFID technology, laws have been passed on the protection of consumer

privacy. One needs only to look into the United States Code to find laws addressing the misuse of personal information. As stated in the Privacy Act of 1974,

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

The law does allow exceptions for certain agencies though, as long as the information is used in accordance with other parts of that section, as well as other sections of the United States Code. Such agencies include: Bureau of Census, National Archives and Records Administration, or any consumer reporting agency.

Another area the United States Code specifies how personal information shall be protected is with respect to the cable service industry. 47 U.S.C. § 551 (2002) established that,

At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of - (A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information; (B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made; (C) the period during which such information will be

maintained by the cable operator; (D) the times and place at which the subscriber may have access to such information.

The important point of this entire section is that a cable operator must provide a written notice to the customer when personal information is to be collected. This is a bold statement saying that the cable customer reserves the right to be notified when their personal information is being used. In other words, this information belongs to the customer. It is his or her property. Permission to use it must be granted.

There are also laws within the United States Code dealing with unfair methods of competition and unfair or deceptive acts. “Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful” (15 U.S.C. § 45, 2003). The critical question is whether or not RFID tagging is an unfair or deceptive practice. Unfortunately, there is no definition of an unfair or deceptive act or practice in that section of the United States Code.

Although the previously noted section of United States Code was vague on what exactly an unfair or deceptive act or practice is, other sections uphold that consumer privacy is a valuable commodity worth protecting. One area that points this out is with telecommunications. “Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier” (47 U.S.C. § 222, 2002). Here it is clearly stated that a telecommunication customer’s proprietary information must be protected. If that information was not valuable, why would its confidentiality be protected? If this protection is available for customers of

telecommunication services, one could hypothesize that the same private information isn't any less valuable when considering RFID technology.

According to these previously mentioned laws, personal information could be defined as a valuable commodity worth protecting. If this is true, to whom does this commodity belong? If the answer is to whom the information identifies, then it would be considered property of the individual. Any law-abiding citizen has the right to protect their personal property, at least if the Constitution of the United States has anything to say about it. According to the U.S. Const. amend. IV,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Proposed Legislation on RFID Tagging

Just because no legal regulation currently exists on how RFID chips shall be used to gather personal information, efforts are being made. While small-scale tests are being run on how the chips will perform for the retail industry, our legal system has begun to take action with RFID privacy concerns. Many bills are beginning to surface throughout the states. Politicians across the nation, willing to listen to the overwhelming concerns of the people, are backing legislation that protects consumer rights to privacy. Roberti (2004) wrote,

The formal debate over how RFID tags can and can't be used has begun in the

United States. Representative David L. Hogue (R-District 52) has introduced a bill in Utah that would require labels to indicate that products have RFID tags embedded in them or in the packaging. A similar bill has also been introduced in Missouri. California State Senator Debra Bowen (D-Redondo Beach) has penned a more comprehensive bill that would require retailers to inform consumers when using RFID tags and readers, to get consent before gathering personally identifiable information, and to kill the transponders before customers leave the store. (¶ 1-2)

Although the California bill was defeated by members of the California state assembly (July 5, 2004) on the premise that the bill should not have preceded the actual implementation of the technology, it shows that privacy concerns are reaching to the legislative level and receiving public attention. According to Swedberg (2004),

The California bill...SB1834 would have restricted the way business and libraries in California use RFID tags attached to consumer products or using an RFID reader that could be used to identify an individual. The only information the RFID system would have been allowed to collect would have been in regard to items customers were actually buying, renting, or borrowing. The bill would have prohibited businesses or libraries from using an RFID system to collect information on tagged items that the customer may have picked up but put back prior to a transaction, or to collect information from tags on clothing people were wearing and on items they were carrying in a wallet or purse. (p. 1)

Bowen plans to continue working on legislation dealing with RFID and privacy.

Another bill, specifically tailored to RFID tagging, is the Opt-Out of ID Chips Act. It was introduced to the House of Representatives on June 23, 2004, by Rep. Gerald D. Kleczka. The bill mandates that warning labels be placed on consumer products containing RFID devices. H.R.4673 (2004) proposed that,

It shall be an unfair or deceptive act or practice...to sell at retail any product containing a radio frequency identification device (RFID) unless such product bears a label meeting the requirements of subsection (b); and the person purchasing such product is provided with the option of having such device removed from the product or permanently disabled at the time of purchase.

Regarding the warning label on the product, subsection (b) of H.R.4673 (2004) stated that it shall,

State, at a minimum, that the product contains a radio frequency identification device, and that such device can be used to track the product and transmit unique identification information to an independent reader both before and after purchase; notify the consumer of such consumer's right to have such device removed from the product or permanently disabled at the time of purchase; and be in a conspicuous type-size and location and in print that contrasts with the background against which it appears.

The Consumer Privacy Protection Act of 2003 was drafted to deal directly with the issue of customer rights to privacy in regard to personal information. The act requires a disclosure of information collected that is not related to the point-of-sale transaction. H.R.1636 (2003) set forth the following regulation:

A data collection organization shall provide to a consumer a notice containing the

information required under subsection (b) as follows: (1) Upon the first instance of collection from the consumer of personally identifiable information, that may be used for a purpose unrelated to the transaction, by a data collection organization, the organization shall provide the notice at the time personally identifiable information is collected.

The question of whether or not restrictions are needed on RFID tagging to protect the personal information of consumers is clear. Consumers are overwhelmingly asking for them. Their personal data is private, valuable property worth protecting. According to the Declaration of Independence, it is the right of the people to alter or abolish government when it begins to affect their safety and happiness. Government has been set up to represent the people. The current laws that exist do not deal specifically with radio frequency identification tagging in retail. Therefore, legislation must be passed to protect the safety of consumer private information with the use of RFID technology in retail.

CHAPTER III

METHOD

It is important to consider any new technology that mankind begins to use. Radio frequency identification (RFID) technology is no exception. In order to better understand how RFID functioned in retail; as well as determine what rights consumers have to privacy, how the technology could invade these rights, and what guidelines are needed to better protect consumers against the invasion of their privacy; an in-depth review of literature was performed.

This review of literature first explored what were the point-of-sale technologies in retail that facilitate the collection of data. This section focused on the Universal Product Code (UPC) as well as radio frequency identification.

It then investigated the possibility of privacy and security concerns arising from RFID technology. Such topics as availability of consumer data, smart homes, misuse of information, and consumer fears were all covered in this section.

The literature review then looked into the controversy of accepting or rejecting new technology and why it is important to carefully examine RFID chip technology. Advancements in technology present moral questions that are not always so clear. This section within the review was designed to explore how RFID chip technology could control, rather than enhance, human faculties.

The next section of the review examined the value of a consumer's personal information. It centered on customer trust and why companies should even consider creating a trusting relationship with their customers. It also defined what kinds of consumer rights to privacy companies should protect if they want to value customer trust.

The review went on to discuss the debate over restrictions governing RFID technology. It revealed how consumers feel about the protection of their personal information. It probed into what businesses are saying about restrictions. It then looked at a possible solution for the dilemma- a proposed RFID Bill of Rights.

The following section concentrated on legislation that has been passed on consumer privacy. It researched laws relating to the misuse and protection of personal information, unfair methods of competition, and the right to secure one's private property.

The review of literature finally glimpsed at proposed legislation to protect the privacy of consumers using RFID technology. It examined various bills specific to RFID being pitched around the nation's political area.

Once this review of literature was concluded, a detailed plan was developed to aid retailers with the ethical implementation of RFID tagging in a way that preserves customer trust. The plan began with a Consumer Bill of Rights, boldly stating the natural rights every customer deserves. A Technology Awareness Policy was then developed to allow customers the right to know when, where, and why this new RFID technology is being used. Finally, a Point-of-Sale Protection Program was forged into the plan to ensure the protection of consumer private information past the point-of-sale.

CHAPTER IV

RESULTS

A Plan for the Ethical Implementation of Radio Frequency Identification Tagging in Retail

Radio frequency identification is a rapidly emerging technology that will most likely be adapted into much of the retail industry in the not-so-distant future. Therefore, companies employing this progressive technology must consider the possible drawbacks.

As previously revealed in this study's review of literature, consumers have a natural right to protect their personal information. Furthermore, radio frequency identification has the potential to invade consumer privacy rights. This invasion threatens valuable customer trust. Any retail business interested in preserving this trust must protect the private information of its customers.

The results that follow have been created to aid in the implementation of this technology for any retail business interested in preserving customer trust. These include a Consumer Bill of Rights for Radio Frequency Identification Tagging, a Technology Awareness Policy, and a Point-of-Sale Protection Program.

*Consumer Bill of Rights for
Radio Frequency Identification Tagging*

Personal, identifiable information is the sole property of the individual for whom it identifies. Therefore, according to the Fourth Amendment to the Constitution of the United States of America, every consumer reserves the right to protect that property.

The following statements followed by an asterisk () are a combination of ideas from Garfinkel (2002) and the writer.*

- Every consumer has the right to know when, where, and why radio frequency identification tags and readers are being used on the products or services they purchase, rent, or borrow.*
- Consent to use a consumer's personal, identifiable information for purposes other than what is solely needed to increase efficiency shall be obtained in writing from that same consumer.
- No information shall be obtained on any consumer from a radio frequency identification chip, except at the point-of-sale, unless the consumer has otherwise given his or her consent in writing.
- No consumer should be forced to use radio frequency identification technology. Opt-out options must be made available for anyone choosing to buy, rent, or borrow an item containing a radio frequency identification chip.*
- Consumers have the right to remove and destroy any and all radio frequency identification chips at or past the point-of-sale or transaction.*

Technology Awareness Policy

This policy was drafted to grant retail customers the right to know when, where, and why radio frequency identification (RFID) technology is being used, as previously noted in the Consumer Bill of Rights for Radio Frequency Identification Tagging. This policy calls upon all consumer-conscientious businesses which value customer trust to uphold the following such practices:

1. Provide a disclosure statement to customers entering a retail establishment that RFID technology is used for the sole purpose of increasing efficiency. This disclosure will direct customers where to go within the establishment to receive more information on the use of this technology.
2. Make available an informational center, somewhere near the front of the establishment, where customers can receive free educational information on how the business uses RFID technology. This educational information is to be in written format and available for the customer to take home. The educational information will include, but not be limited to, the following:
 - a) A general explanation of what RFID is.
 - b) A description of how RFID is used in the establishment.
 - c) An explanation of why RFID is used in the establishment?
 - d) A statement explaining how customers may opt-out of the collection of personal information through the use of RFID technology during the point-of-sale if they so choose.
 - e) A statement guaranteeing the option for consumers to purchase any product or service without the use of RFID technology.

- f) A statement explaining that a consumer's consent must be granted before any personal information pertaining to that consumer is to be sold. Knowledge of whom the information will be sold to will be provided before consent is solicited.
- g) A declaration proclaiming the Consumer Bill of Rights for Radio Frequency Identification Tagging, the Point-of-Sale Protection Policy, and this Technology Awareness Policy.

The educational information provided at the informational center will also be available online. The web address will be clearly visible and easy to locate.

3. Mandate that all employees receive 3 hours of educational training on the Consumer Bill of Rights for Radio Frequency Identification Tagging, the Point-of-Sale Protection Policy, and this Technology Awareness Policy.
4. Guarantee that all merchandise containing RFID chips be labeled with a legible awareness notice on some form of easily removable tag. This awareness notice must state that a RFID chip is being used and explain where to go within the establishment to get further information on the technology. This awareness notice must also provide instructions on how to remove the tag prior to the point-of-sale if the customer so chooses. All RFID chips will be placed only on this removable tag.

Point-of-Sale Protection Program

This policy was drafted to ensure the protection of consumer private information past the point-of-sale with the use of radio frequency identification (RFID) technology. This policy calls upon all consumer-conscientious retail businesses which value customer trust to uphold the following such practices at the point-of-sale:

The following statement followed by an asterisk () is a combination of ideas from Garfinkel (2002) and the writer.*

1. Any and all RFID chips used in retail will be terminated at the point-of-sale through some form of kill command software.
2. All point-of-sale locations will have some form of clearly visible notice stating that all RFID chips used during the transaction have been electronically destroyed. The notice will also remind customers that they may physically remove the tag containing the RFID chip anytime after the point-of-sale.
3. No customer will be forced into using RFID technology to purchase goods or services. The establishment will provide an alternative means of purchasing goods or services without the use of any RFID technology.*

CHAPTER V

DISCUSSION

Summary

The purposes of this study were to determine if radio frequency identification (RFID) technology had the potential to invade consumer privacy rights and develop a plan for the ethical implementation of RFID in retail.

The researcher first investigated what were the point-of-sale technologies in retail that facilitated the collection of data. The Universal Product Code (UPC) and RFID were the two most significant advancements that have taken place in point-of-sale technology. UPC was defined both technically and historically, while RFID was examined solely from a technical standpoint.

It was then discussed and noted that there were serious privacy and security concerns arising from the misuse RFID technology. RFID tagging not only facilitated the collection of personal information, it granted retailers and manufacturers the capability to track the information past the point-of-sale. These tiny chips could follow a consumer home and compile an abundant supply of personal data with the aid of smart home technology.

Further defined was the importance of carefully examining any new technology. Advancements in any technology designed to expand mankind's innate ability to perform work could begin to dominate those same natural abilities if left unchecked.

Advancements in point-of-sale technology with RFID were examined and found to hold potentially negative repercussions if left unrestrained.

The researcher then searched out the value of trust in a business relationship between a company and its customers. If consumer trust were to have a high value in business, companies that preserve it would be prosperous. It was found that customer trust was a key ingredient for establishing a strong relationship between company and customer. Customers who felt they were being treated as valuable assets would continue to bring their resources to the table. Customer-to-customer referrals were found to be very valuable as well. Ultimately, customers were eager to invest in companies that would value and protect their personal information.

The debate over restrictions governing RFID technology was then discussed. It was found that while business wished to keep restrictions to a minimum, consumers wanted government to pass stronger laws to better protect their personal information. A set of protective guidelines, including a bill of rights for the use of RFID in retail, was found to be one possible solution for building customer trust.

An investigation into current law was then undertaken to find out exactly what legal rights have been established for the protection of consumer privacy. It was found that no legislation specific to RFID technology had been passed into law. The next step was to then look at other current laws that dealt with the protection of consumer privacy. The researcher looked at the Privacy Act of 1974; the United States Code regulations governing cable service providers, unfair methods of competition, and telecommunications carriers; and the Constitution of the United States of America. After careful examination of this legal material, it was concluded that personal, identifiable

information was valuable property belonging to whomever it identified. Thus, this private property was protected under the Constitution.

The researcher finally explored proposed legislation to protect consumers using RFID technology. It found that the proposed legislation was calling for retailers to notify shoppers, through the use of a warning label, when using RFID technology; obtain consent before collecting personal information, as well as disclose any information collected that was not related to the point-of-sale transaction; and kill the technology before it left the store.

From this study, the researcher deduced that RFID technology, used in retail, did have the potential to invade consumer privacy rights. Therefore, the researcher developed a set of protective guidelines to help secure consumer personal information. This set of guidelines was a carefully drafted plan to aid in the ethical implementation of RFID technology in a retail business.

The plan first contained a Consumer Bill of Rights for Radio Frequency Identification Tagging. This bill of rights was a set of five bold statements designed to ensure retail customers using RFID technology the right to protect their personal information as private property. This bill of rights was also formulated to guarantee the freedom consumers had to choose not to use RFID technology when making a retail purchase.

The second part of the comprehensive plan contained a Technology Awareness Policy. This policy was drafted to grant retail customers the right to know when, where, and why RFID technology would be in use. The policy was written specifically for consumer-conscientious retail businesses interested in upholding customer trust.

The third part of the comprehensive plan contained a Point-of-Sale Protection Program. This program was designed to ensure the protection of consumer private information with the use of RFID technology past the point-of-sale. It was also written specifically for consumer-conscientious retail businesses interested in upholding customer trust.

Conclusions

As a result of this study, the researcher concluded the following:

1. Radio frequency identification technology used in retail had the potential to invade consumer privacy rights if left unchecked.
2. Personal, identifiable information was protected under the Constitution of the United States of America as valuable property, belonging to whomever it identified. Consumers therefore reserved the right to protect against the invasion of their personal, identifiable information.
3. With the retail use of RFID technology, a set of protective guidelines was necessary for the security of a consumer's personal, identifiable information. Therefore, a proposed plan for ethically implementing radio frequency identification technology into a retail business was essential. This plan needed to include a Consumer Bill of Rights for Radio Frequency Identification Tagging, Technology Awareness Policy, and Point-of-Sale Protection Program.

Recommendations

This study was an in-depth research into how radio frequency identification technology could invade consumer privacy rights, as well as what was needed to ensure the protection of these rights. As extensive as it was, one way it could be improved is by further researching strategies for implementing a new technology policy into an existing retail company. The success of the proposed plan depends on how well it is implemented. There are many studies available on how to best integrate a new plan into an existing retail company so that the transition is as smooth as possible. Research into these types of studies would be very useful.

This study is also lacking of any statistical data. It would be very beneficial if a pilot program for the implementation of the plan proposed in this study could be tested in a number of different retail companies. The aim of the plan developed from the research in this study was to protect consumer privacy rights with the use of radio frequency identification technology in retail. Therefore, this objective would need to be tested to see if the proposed plan would be significantly effective.

REFERENCES

- 15 U.S.C. § 45 (2003).
- 47 U.S.C. § 222 (2002).
- 47 U.S.C. § 551 (2002).
- Bergholz, H., & Nickols, F. (2001). Building your consulting practice through referrals. *Consulting to Management – CSM*, 12(3), 25-26.
- Brandt, A. (2003). Tracked by the shirt on your back? (privacy watch). *PC World*, 21(7), 40.
- Brody, A. L. (2002). Active and intelligent packaging: the saga continues. *Food Technology*, 56(12), 66.
- Brooks, B. (1999). Don't underestimate value of customer trust. *American Banker*, 164(14), NA.
- Cannon, D. (2002). The ethics of database marketing: personalization and database marketing- if done correctly- can serve both the organization and the customer. *Information Management Journal*, 36(3), 42-45.
- Clark, D. (2003). Big Brother, or Benetton, can watch you. (usage of radio frequency identification tags). *National Journal*, 35(20), 1566-1567.
- Conhaim, W. W. (1999). Wired neighborhoods (internet). *Link-Up*, 16(4), 5-7.
- Consumer Privacy Protection Act of 2003, H.R. 1636, 108th Cong., 1st Sess. (2003).
- Culnan, M., & Bies, R. (2003). Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323.
- Froomkin, M. A. (2000). The death of privacy. *Stanford Law Review*, 52(5), 1461.
- Garfinkel, S. L. (2002). An RFID bill of rights. *Technology Review*, 105(8), 35.
- Garfinkel, S. L. (2000). U.S. shouldn't wait to enact privacy legislation. *Computerworld*, 34(16), 30-32.

- Greiner, L. (1997). Supermarkets and summertime paranoia (collection and sale of personal information by supermarket cards, credit cards and online services). *Computing Canada*, 23(14), 9.
- Hunter, R. (2002). *World without Secrets*. New York: John Wiley & Sons, Inc.
- James, V., & LaMotta, C. (2003, November). Taking the high road: building loyalty—several successful companies have profited by cultivating customer loyalty. *Direct*, NA.
- Kirsche, M. L. (2004, March). Gain consumer's trust in RFID before it hits shopping baskets—automation and technology. *Drug Store News*, 26-28.
- Kravitz, P., & Pugliese, A. (2000). Lawmakers tackle privacy. *Journal of Accountancy*, 189(6), 29.
- Maguire, G.Q., & McGee, E. (1999). Implantable brain chips? Time for debate. *The Hastenings Centre Report*, 29(1), 7.
- Maynard, N. F. (2003). Smart plug-ins (home front: tips and trends from the world of residential design). *Residential Architect*, 7(3), 23.
- Merrit, R. (2003). Identification intended to infiltrate us—if it has surface then a chip can be implanted to mark you and yours. *Electronic Engineering Times*, October 13, 2003, p. NA.
- Opt Out of ID Chips Act, H.R. 4673, 108th Cong., 2d Sess. (2004).
- Privacy Act of 1974, 5 U.S.C. § 552 (1974).
- RFID backers, privacy advocates seek common ground. (2003). *Information Week*, NA.
- Roberti, M. (March 1, 2004). The law of the land—legislation introduced in Utah and California will force companies in the United States to address the privacy issue. *RFID Journal* [Online journal]. Retrieved July 14, 2004, from the World Wide Web: <http://www.rfidjournal.com>
- Rosen, C. (2001, June). The fast track: radio-frequency devices promise to make it easier to monitor the flow of inventory across the supply chain. *Information Week*, 22, p. NA.
- Scanlon, L. (2003). Behind bars: the inventors of the first linear bar-code system were decades ahead of their time. *Technology Review (Cambridge, Mass.)*, 106(3), 80.

- Schmidt, C. (2001). Beyond the bar code (technology information). *Technology Review (Cambridge, Mass.)*, 104(2), 80.
- Stambler, I. (1990). Computer implants could bring new life to human limbs: microelectronics. *R&D*, 32(4), 30-31.
- Swedberg, C. (July 5, 2004). California RFID legislation rejected-the state assembly's Committee on Business and Professions voted against a bill seeking to set privacy standards for RFID technology. *RFID Journal* [Online journal]. Retrieved July 14, 2004, from the World Wide Web: <http://www.rfidjournal.com>
- Tarnowksi, J. (2004). Ode to the code. *Progressive Grocer*, 83(11), 26-27.
- U.S. Const. amend. IV.
- Volti, R. (2001). *Technology and Society* (4th ed.). New York: Worth Publishers.
- Wal-mart leading the way with RFID. (2003). *Microwave Journal*, 46(9), 65.
- What is RFID? (2005). Alien Technology website. Retrieved May 8, 2005, from the World Wide Web: <http://www.alientechnology.com/what/index.php>
- Yoshida, J. (2003). RFID 'kill' feature aims to soothe privacy fears: as Benetton backpedals, makers rethink tag tracking. *Engineering Times*, 1, NA.