RFID Tagging: Final Report

Stephanie Allen

Gina Calcaterra

Michael Gray

Rahul Nair

Sumit Pahwa

Edward Robertson

History of RFID

While RFID is a new buzzword in the world of business it has existed in various forms for over 50 years. The earliest technique for detecting objects using radio frequency waves was the RADAR (Radio Detection And Ranging) which was perfected during World War II. While initial radar could only locate objects using radio waves, this would soon change. In 1948, Harry Stockman published his landmark paper "Communication by means of reflected power". This paper laid the groundwork for what has now become RFID technology. During the fifties the military was once again at the forefront of this by creating the "friend or foe" transponders that allowed the identification of aircraft from a distance.

In the 56 years since Stockmans paper, RFID has had grown explosively and is now poised to enter every facet of our lives. Appendix A gives a timeline of how RFID technology has grown over the years while the next section deals with the current state of RFID.

RFID Technology

RFID (Radio Frequency Identification) technology consists of a system of tags and readers that can be used to identify and encode a variety of information. The tags are small silicon chips that contain a unique identifying code and may also contain some form of stored battery power and on-chip memory. An RFID reader is a unit that emanates radio signal at a precise frequency that causes the RFID tags to respond with their identifying code. While RFID chips can be classified on the basis of several characteristics such as frequency, multi read capability, signal strength, and data storage, the primary distinction between RFID systems is based on the tag power source.

Tags that either contain an onboard power source or are connected to an external power supply are called "**Active**" RFID tags while those tags that depend on the RFID reader for their power are called "**Passive**" RFID tags.

Active RFID technology

Active RFID technology tags have access to a continuous power supply. This power is usually received in the form of a battery connected to the RFID tag. Since active tags have this built in power source they have a greater range than passive RFID tags. The power source also allows them to have built in sensors to monitor their environment. They can be set to actively contact an external reader if they notice any anomalous reading from their sensors. Another major advantage of active tags is the faster read speed. Active tags can be read when moving at up to 100 miles an hour (e.g.: Automatic toll payment systems) and the readers are capable of reading as many as a thousand tags a second. They also have a much larger memory than passive tags and due to their higher processing capabilities are also more secure.

The greatest weakness of active RFID is the fact that their life cycle is limited by their power source. Prof. Gregory Abowd, an associate professor at Georgia Tech and an early adopter of RFID opines "It is possible to increase the life span of an active RFID tag by reducing the duty cycle of a tag from several times a second to once every few minutes, they are still limited by the fact that their batteries eventually run out." Another weakness of active RFID is the high cost, the addition of a battery to the tag increases the cost of an active tag to several dollars while adding sensors to a tag will push the price to over $100. The continuously emissive nature of active tags has also led to their frequencies being much more controlled (Appendix B).

Due to their operating cost and characteristics active RFID tags are suitable for applications that require unconstrained mobility of assets, continuous or periodic monitoring, sophisticated sensing and high security. Example applications include area monitoring, cargo security, electronic on-chip manifest and high speed identification.

Passive RFID tags

Passive RFID tags absorb and temporarily store some energy from the readers signal to generate their own response. For Passive RFID, the communication range is limited by two factors: 1) the need for very strong signals to be received by the tag to power the tag, limiting the reader to tag range, and 2) the small amount of power available for a tag to respond to the reader, limiting the tag to reader range. These factors typically constrain Passive RFID operation to 3 meters or less. A direct result of this limited read range is that it is more difficult to read multiple co located tags. Since the tags must remain within range of the reader at all times there are severe limits on the mobility of tags during the read operation.

Since they do not require any internal power source passive RFID tags have a virtually infinite life cycle. The minimal on-board circuitry of passive RFID tags means that they are much cheaper (~20 cents) than active tags and as such are suitable for tagging individual consumer products. Passive tags can also have a limited amount of onboard memory (typically 128 kilobytes) but it is usually much lesser than active tags.

Passive RFID is usually more suited towards applications with the following characteristics:

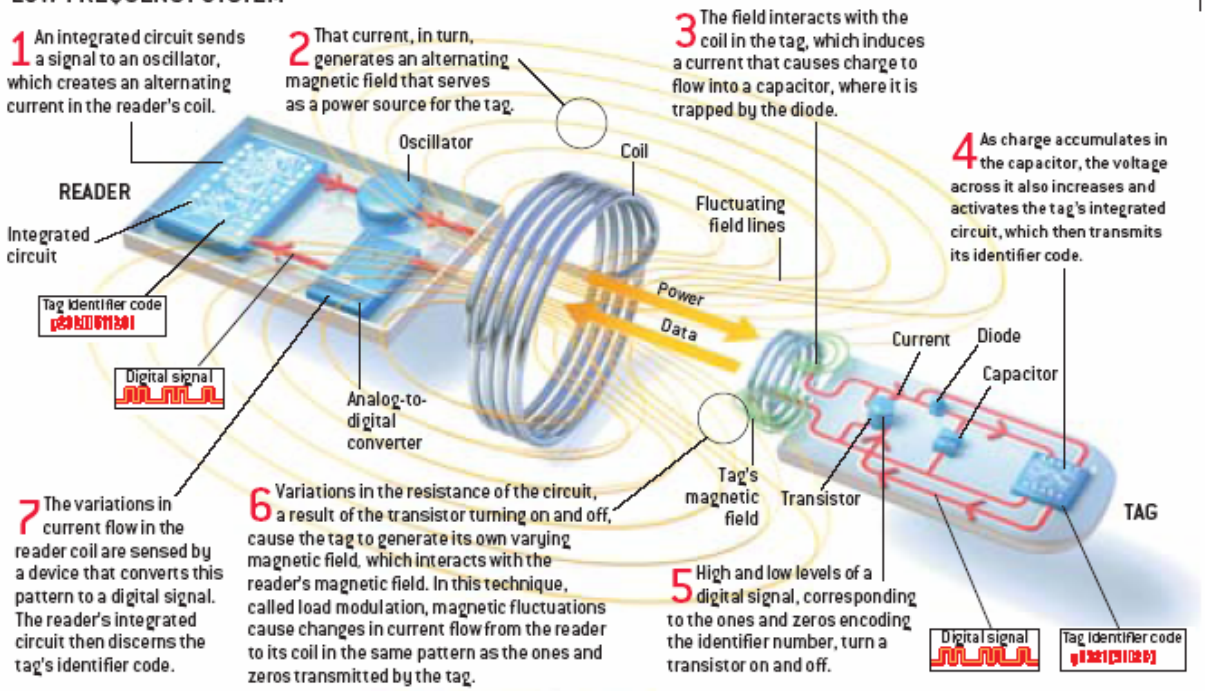
- Low cost solutions are needed
- movement of assets is strictly controlled
- low security
- long lifespan required with no possibility of changing the power source
- no or limited sensing needs
- low or no storage is required

Examples applications include supermarket checkout, shoplifting checks, and smart cards.

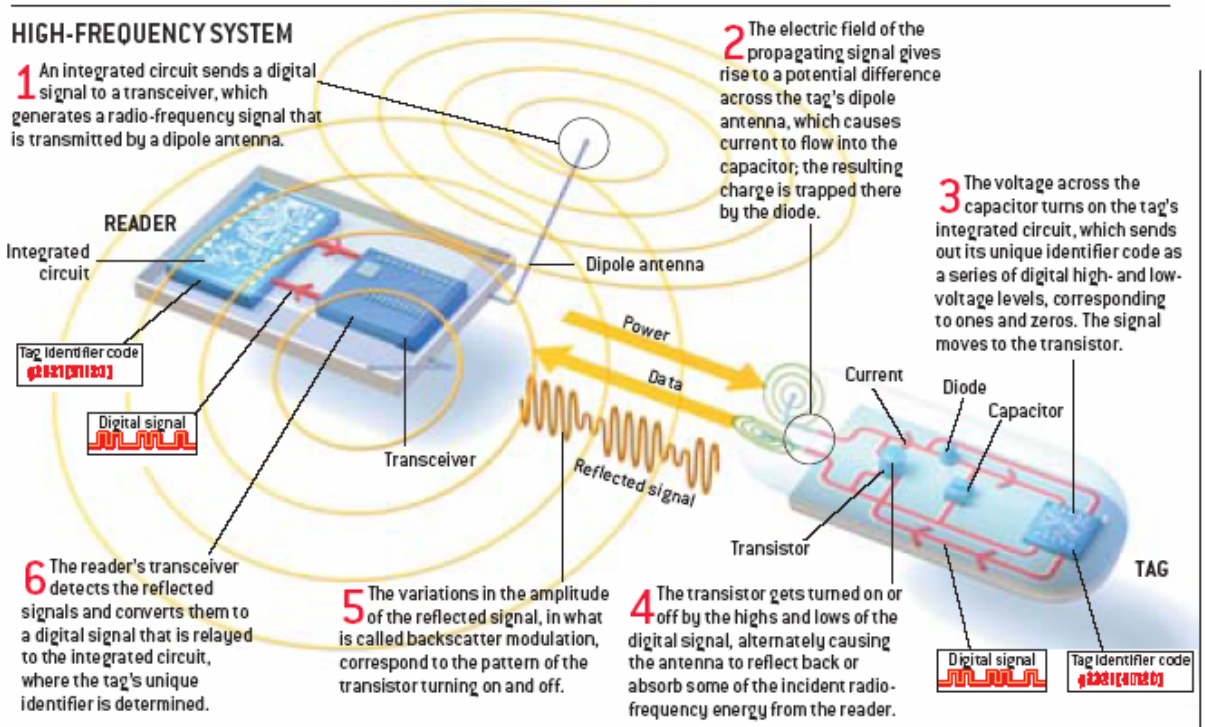
HOW RFID WORKS

RFID systems operate in both low frequency (less than 100 megahertz) and high frequency (greater than 100 megahertz) modes. Unlike their low-frequency counterparts, high-frequency tags can have their data read at distances of greater than one meter, even while closely spaced together. New data can also be transmitted to the tags, a process not shown here.

LOW-FREQUENCY SYSTEM



HIGH-FREQUENCY SYSTEM



Animal Microchipping

The RFID used for animal microchipping is the size of a grain of rice and is commonly implanted in a domestic pet near the shoulder blades and if the hoofs of livestock. The procedure takes only a few minutes and has very minimal impact on the animal. The process has gained acceptance world-wide.

Domestic Pets

Animal microchipping can serve different purposes. Microchipping domestic pets gives an owner piece of mind by knowing that their animal has been registered in a national database. Currently over 3 million pets have been microchipped and over 70,000 lost pets have been reunited with their owners. However there are problems with microchipping pets. First, there is more than one national animal registry. The two most prominent organizations which provide these services are AVID Identification and the American Kennel Institute. These databases are not cross registered so an animal will only be registered with one database service. In addition there are multiple brands on RFIDs that are used for this process. When a pet owner chooses to get their pet microchipped, they don't get a choice of the device that is implanted into their animal. Veterinarians and Animal Shelters usually have their preferences, and that is all that they provide, so it is up to the pet owner to research the different options.

Another problem is that no RFID reader will recognize all of these different RFIDs used for Animal Microchipping. This means that if a pet shows up at a shelter whose RFID reader does not recognize the brand of microchip implanted in the animal, there may be no indication at all that the animal has been microchipped. The animal may very well never be reunited with its owner.

Livestock

RFIDs are slowly taking the place of tattoos, brands, ear tags, and other methods that are used to track live stock. RFIDs provide a way to track the entire supply chain process from farm-to-fork. The biggest push for such a process has been the concerns about disease control and prevention. The USDA has put a plan is place to create a national animal identification system that can track livestock movements by assigning a unique ID to each animal, or in the case of chickens, groups of animals. By 2005, the USDA plans to track all animals and all intrastate movement by 2006.

The European Union has recently adopted the regulation of goats and sheep by using RFID given concerns about recurring animal disease epidemics. It is expected that tracking animal data through electronic means will ease many consumers' minds about the quality and origin of the meat that they eat. The Europe Union intends to pool this information and store it in central databases that will be contained within each member state.

There are several pressing concerns about using RFIDs for tracking livestock. The first is durability. These RFIDs must be able to withstand environmental elements as well as many chemicals. In addition, most RFIDs have a very short range read which poses a problem when dealing with thousands of animals in either a pasture or a processing plant. Phillips Semiconductors is currently researching a long read-range RFID that can withstand large amounts of electronic noise as well as environmental elements.

Farmers are concerned about the cost effectiveness of the program. Current tools used to track herds are almost negligible. Implementing RFID tracking systems involves such costs as purchasing readers, software, implanting equipping, and of course the RFID itself.

Wal-Mart

Wal-Mart surprised its suppliers in the summer of 2003 by announcing an aggressive timetable for the implementation of RFIDs on their shipments. Wal-Mart stated that it expected its top 100 suppliers to use radio tags on shipments by the end of 2004, with all suppliers complying by the end of 2005. By November of 2003, the suppliers had swelled to 123 and the roll-out for 2004 had been scaled to a limited number of goods shipped to three distribution centers serving 150 stores in Texas.

Wal-Mart announced later in the year that the manufacturers of the most tightly controlled prescription drugs were to be on the fast track. Drug manufacturers have more to gain with RFID technology given concerns about counterfeiting and tampering with products. They were supposed to send bulk shipments on the drugs in radio tag containers to a distribution center near Wal-Mart's headquarters by March 2004. Within days of the deadline, Wal-Mart admitted that it would not be met. While a few companies were able to meet the deadline, the rest will now have until June 2004 to comply.

This is not the first accommodation that Wal-Mart has had to make in its deployment of RFID technology. Wal-Mart is slowly beginning to realize that neither their suppliers nor the technology is ready for such an aggressive roll-out. Most of Wal-Mart's suppliers are not in the financial position to implement the technology given the current cost. Until the cost drops to approximately five cents for each RFID, companies will not be able to recover the investments from the savings generated by using the RFID technology to improve the supply chain process. These suppliers are also facing the problem of ensuring that they're RFID tagging systems will be compatible across the different retailers which distribute and sale their products (i.e. Target)

In addition there are also still obstacles with the RFID technology itself. Currently the RFIDs cannot be detected through liquid or metal. This poses a problem when trying to use an RFID reader on a pallet of Coca-Cola cans.

Wal-Mart does not seem to be raising any concerns for consumers though. A Wal-Mart executive has already stated that Wal-Mart plans to use RFIDs to track the merchandise but intends to remove the tags from items that have been purchased.

Tesco

Tesco, a supermarket chain based in the UK, is taking a different approach to RFIDs. Tesco ran it's first pilot in the summer of 2003 where RFID tags were placed on certain items within the store, Gillette razors for example. When a customer picked up one of these products, their picture would be taken. There picture would be taken again as they purchased the product. During this pilot, Tesco was evaluating the use of RFIDs for theft control purposes. A Gillette spokesman claimed that the test was being used to monitor communication in the store and the tracking of out-of-stocks and replenishment rates. Regardless, this test did not go over well with consumers. Many protested outside of the Cambridge store, where the pilot took place, until the pilot was over. Tesco claimed that the pilot ran and ended as scheduled and that the protesting had nothing to do with the length of the pilot.

In October 2003, Tesco ran another pilot at their Milton Keynes distribution centre which involved attaching an RFID tag to transporation cases in order to improve supply chain visibility. An item level trial involving DVDs is scheduled to begin in May 2004.

Tesco has proceeded in their plan to implement RFIDs in their stores following what they considered to be successful pilots. Tesco is taking a different approach to their RFID implementation than other retailers which may prove beneficial. Tesco is using the name 'radio barcodes' to describe the technology. They have also provided a wealth of consumer information about the technology on a dedicated section of their website. On their website, Tesco describes the RFID technology as a next generation barcode where no other information is stored on the RFID tag other than the product code. Tesco also provides information about the range of the tag and what the tag is to be used for which is for supply chain management and monitoring the flow of goods.

Later this year Tesco will begin undertaking a comprehensive standards review in order to compile and finalize a list of supplier requirements along with a list of products to be tagged initially. By early 2005 Tesco anticipates that they will have completed implementation of case-level RFID tagging. While they have piloted with item-level tagging, there are currently no plans in place to implement the process.

Problems for Prada

In December 2001 Prada opened a new $40 million Epicenter store in New York's trendy Soho district. Prada took a bold initiative and worked with IDEO to use RFIDs in order to enhance every aspect of their customer's experience. Clothing, shoes, dressing rooms and even customer cards are now tagged with RFIDs.

Prada's expectations of their Epicenter have not quite come to pass. The store has been open a little more than two years now, and most of the technology just sits idle. It was even rumored that Prada had silently removed the RFID tags from their items due to objections from their customers about the data that was being collected. The rumor while untrue, also has turned out to be unfounded as it appears that the RFIDs aren't being used for much of anything at all. It seems that Prada's employees never quite embraced the handheld tools and are simply too overwhelmed by large crowds to assist shoppers with the handheld RFID readers. In fact, most of the handhelds are put away as to keep the tourists from playing with them.

In addition, the automated dressing rooms with the smart closets are either malfunctioning or ignored. Prada's RFID smart closets are failing to recognize the RFID tags attached to the clothing and accessories and the touch screen simply remained blank or broadcasted random video loops. On the rare occasion that the RFID is recognized, the system promptly crashes. Analysts blame the system's failure on a ubiquitous computing design that was simply too ambitious and not well thought out. The store's failings have cost Prada big bucks and they are currently re-evaluating their epicenter strategy.

How Are RFIDs Really Performing in Retail

It may be some time before RFIDs are successfully implemented in retail establishments, at least the item-level. Even companies such as Wal-Mart and Tesco who are only currently looking to use the technology to track pallets and cases are facing problems. The technology still has faults such as the inability to read the tags through liquid and metal, so not all pallets can currently be tagged. In addition the tags are still currently lacking in reliability. The tags are falling far below the 99 percent reliability rate of UPC tags due to difficulties with transmittance of clean signals.

The costs for passive RFIDs are currently very prohibitive to manufacturers. RFIDs currently cost between twenty and thirty cents a piece. When tagging millions of items, these costs can add up all too quickly. For most manufacturers, the decision to use RFIDs simply doesn't make financial sense until the costs drop to around five cents a piece because of the costs associated with not only the RFIDs but the cost of altering packaging lines to accommodate the tags. However, for the costs to drop, volume must increase, so the industry is really in a catch-22 scenario.

Problems related to item-level tagging mostly revolve around consumer's concerns of privacy violations. There really haven't been any good examples of where RFIDs provide benefits to the customers, so it is hard for them to buy into the concept. Companies that are seeing the least resistance to consumer advocates are those which are taking the time to educate the consumer about both the technology and their plan for using the technology. Consumers are less up in arms when they no that big brother is not looking over their shoulder or following them out of the store.

Privacy Issues raised by RFID

These tiny RFID chips—which can be implanted in or attached to virtually anything from washing machines, sweaters, and milk cartons to livestock and, it is anticipated, one day, people— are able to broadcast information to radio signal scanners up to ten feet away. Although prospective users of these tags have lauded their tremendous promise for streamlining the stocking, warehousing, and delivery of goods, as well as in preventing theft and other losses, privacy advocates point out a worrisome possibility of a multitude of commodities with the capacity to disseminate information about consumers without their permission or even awareness. After all we all have the right to be free of "unreasonable searches and seizure," as guaranteed by the Fourth Amendment of the U.S. Constitution.

In order to properly dissect the privacy issues surrounding RFID we have to consider the location of the RFID in the context of its proximity to the public setting. First case, is while the RFID is still in the public arena, including on the merchants retail floor, near the checkout counter, and in proximity to the security detection devices near exits. Second case, is when the RFID finds itself again in the public domain, namely when the purchaser has disposed of the product containing the tag into a waste or recycling receptacle. Lastly, the third case is all that remains between, when the RFID is in the consumer's home or possession, the times when the consumer has the greatest expectation of privacy.

Even more personal of case three is the example of when family decides to install a wireless sensor network in its home. One part of this network is the set of radio frequency identification (RFID) powered floor mats located in the doorway of each room. Inside each mat is a transmitter that powers the passive receptor tags that each member of the family wears on his or her shoes. As that family member steps over the mat, the transmitter sends out a signal to the tag that, in response, returns the number of the passive tag. This number, along with a date and time stamp, is sent to a CPU that associates it with the name of the person. The network combines the information pertaining to each member of the household into a set of histograms that illustrate the traffic patterns throughout the house, or to implement other "smart" technology. This is not a hypothetical example. A system of this kind is already partially developed and deployed at the Georgia Institute of Technology. (In the Aware Home Residential Laboratory at Georgia Tech.; <http://www.cc.gatech.edu/fce/ahri>.)

Case 1:
This is the easiest case. In this case the consumer has no expectation of privacy, and no legitimate claim to violations to the right of privacy. All reasonable consumers know that as they pass through the security gates they are being scanned for stolen merchandise. Furthermore, if the consumer is broadcasting, either passively or actively, radio

frequencies in this public arena, they have no reasonable hope of preventing others from receiving these transmissions.

Case 2:
In this case the legal analysis is slightly more complicated, but still relatively simple. There are numerous legal cases involving the Fourth Amendment and, of all things, garbage. Bearing most directly on the point here is the consistent finding that people cannot claim a privacy right in their garbage unless the garbage is placed within recognized private spaces (or the "curtilage"). In California v. Greenwood, (486 U.S. 35 1988), for example, a case that has served as precedent in many that followed, the U.S. Supreme Court concluded: "accordingly, having deposited their garbage in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it, respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded." This means quite simply that once a consumer has brought their trash to the curb or equivalent location, all rights to privacy have been surrendered.

Case 3:
It is an understatement to label this case as murky. As of yet there is no clear precedent on this issue and a lack of parallels in the precedent that does exist. Academics have dissected this issue thoroughly only to produce academic fodder. Legal sources (see references section) have constructed a four prong “box test” to evaluate this complex case. The RFID tags contained in the Georgia Tech Aware Home will be used as a representative case for evaluating Case 3, because they are by definition wholly contained within the most private local of the private residence.

The four prongs of the box test are: the Political Prong, the Moral Prong, the Teleological Prong, and the Deontological Prong. Political: one factor to consider in deciding whether a room that is equipped with an RFID mat can still be deemed a private space that is under the control of only one person is the impact on social institutions. How might the recognition of such a right affect a judicial system that is facing increasingly complex questions about ownership of personal information? What would the consequences be for the social and judicially endorsed principle of personal privacy of not according such a right to the individual? Moral: is it "fair" to hold the use of a mat to constitute a waiver of privacy? Is it fair to require that, as the price of enjoying the benefits of a context-aware sensing application in one's own home, one must forgo a right to privacy that one would otherwise have? Teleological: How will the goal of maintaining the status of the home as the central case of privacy be furthered by distinguishing the privacy interests in the tag data depending upon the room from which it originated? Deontological: For the purposes of the mutual access/joint control rule, does the presence of the RFID transceiver constitute shared access and control over an individual's bedroom?

The academic analysis of case 3 is to a largely academic problem; RFID ranges of several feet makes third-party home radio frequency “invasion” seemly impossible. Furthermore, because of the exponential decay of radio frequencies with distance, and the dogmatically understood physical limitations of passive RFID technology, expanding

beyond these short ranges is believed to be impossible. As such, it is highly unlikely that this case will ever evolve into a real legal issue. Whether true issues and precedent in this third case will emerge remains to be seen.

Therefore, with the current state of the art passive RFID technology, and with future technologies, there does not appear to be a legal liability associated with attaching RFID tags to merchandise, or in implementing other home-based RFID containing products. However, as the Benetton case in the next section demonstrates, companies may discover that considerable liabilities exist for RFID containing products in the "court of public opinion."

Benetton Bends to Customer Pressure

On March 11, 2003 Phillips Semiconductors announced that they were developing an RFID that would be embedded into the label of every new garment bearing the name of Benetton's core clothing brand, Sisley. Phillips estimated that in 2003 alone, they would ship approximately 15 million RFID chips to Benetton that would store information about the style, size, color and intended destination of the times. The RFID tags were estimated to cost less than 20 cents per unit given the high volume. However, the relationship between Phillips and Benetton never came to be.

Benetton was in a very unique position in the clothing industry because they control every aspect of their supply chain from design to sales in their retail stores. The RFID tag would have allowed Benetton to track the individual items of clothing throughout the supply chain. These tags would have also have been used to control and prevent theft of items.

Benetton bowed to public pressure though, and announced on April 4, 2003 that no RFID tags were currently embedded in any of their products nor were there any existing plans to put them there. Benetton claimed that this was due to a lack of feasibility studies on the industrial introduction of RFIDs. However, given the immediate turnaround of Benetton's position with respect to RFIDs and their agreement with Phillips, it could be inferred that Benetton was concerned about the outcry of a potential privacy violation. Consumer advocacy groups were claiming that by embedding RFID tags in their clothing, they would lose their ability to move around anonymously.

It became obvious that Benetton had no intention to become a pioneer in Retail Supply Chain Management. Industry analysts viewed Benetton's actions as detrimental for RFID technology because they backed out of the deal with Phillips rather than provided answers. In fact, in later press releases Benetton actually blamed Phillips for jumping the gun and failed to make it clear that the plan was to test the technology first and roll it out only if the tests showed that Benetton would get a return on its investment. In hindsight, Benetton should have taken a different approach. They should have educated their consumers about RFIDs. In reality there are few true privacy concerns involved in

leaving the store with a tagged item. However, Benetton has yet to explain this to their customers.

Octopus Card

The most successful e-cash application of smart cards is the Hong Kong **Octopus** card. This prepaid card was initially launched in 1997 to allow travelers to use a single payment method to use any of the five major public transport services in Hong Kong. Users who initially buy a card pay $6 for a card which they can then "top-up" with cash. Top-ups can be done at ATM's or at any train station. As the market penetration of the Octopus card grew several companies realized the potential of using a contactless RFID smart card. The Octopus card is now accepted in more than 200 outlets including 7-11 stores and Starbucks. Several building have begun using the Octopus card as an access control mechanism. The cards currently have a market penetration of over 95% and records 7 million transactions a day with a value of over $6.5 million. 25% of the daily transactions are not related to transportation making the Octopus system the most successful e-cash venture ever.

A study by the University of Auckland (APPENDIX C) found that users felt that the greatest advantages of the Octopus card were Quick payment service, easier to carry than cash and the versatility of the system. When asked for suggestion of other places to implement Octopus card services they responses were overwhelmingly towards quick service establishments such as supermarkets, newspaper stands, road tolls, and snack stands. None of the over 500 surveyed users had any privacy concerns and were concerned about security only to the extent that they might lose some of the money that they had on their cards.

Abstracting from the user experiences with the Octopus card we can say that users are concerned about the privacy of their data but will usually be willing to give up some privacy if they get a satisfactory return.

Solutions to address Consumer Concerns

As RFID begins to infiltrate our society, there is one major issue that needs to be addressed: the privacy concerns of the consumer. Solutions must be developed to ease these concerns and combat the resistance felt towards this emerging technology. Researchers have recognized the privacy concerns that have arisen with RFID and are continuing to develop better approaches to protecting consumer privacy. Some of the solutions that are being investigated are: the Kill Tag approach, the Faraday Cage approach, the Active Jamming approach, the "smart" RFID tag approach, the Regulation approach, and most recently the Blocker tag. Each of these approaches and their weaknesses are discussed.

1. Kill Tag approach

This is the simplest solution to addressing privacy concerns. It essentially involves "killing" the RFID tags before they are placed in the hands of consumers. After a tag is killed it can never be re-activated, and thus consumers don't have to worry about being scanned. For example, as a consumer moves through the checkout line at the supermarket, the clerks would "kill" the tags of the purchased goods that were being tagged for inventory purposes and no active RFID tags would leave with the consumer.

Problems with this approach:

The problem with this approach is that there are actually some cases where consumers will want the tags to remain active while in their possession. Inexpensive RFID tags may inevitably be used for a variety of applications in the future that will require these tags to remain active upon purchase. For example, microwave ovens are being developed that read the cooking instructions from food packages, and thus would naturally rely on active tags to do so. Researchers are also envisioning "smart" washing machines that can read RFID tags embedded in an individual's clothing and know what cycle the clothes should be washed on. Other reasons to keep tags active are reasons such as 1) they can be scanned and categorized for recycling purposes, 2) they can be embedded in store-issued coupons for ease of scanning at the checkout counter, 3) users can scan their possessions when a recall for a specific set of products is issued, or 4) a user's refrigerator can tell when some food or drug has passed its expiration date and notify the user. Thus, though the kill-tag approach may handle many instances of concern, it is not a completely satisfactory solution considering the potential useful applications of RFID that will directly benefit consumers.

2. Faraday Cage approach

This approach involves shielding RFID tags by using a faraday cage, a container made of metal mesh or foil that is impenetrable by radio signals. For example, a consumer could use a foil-lined wallet if high-value currency notes are printed with active RFID tags.

Problems with this approach:

Many products, such as clothing and of course, human beings, are too large to fit conveniently in containers, thus making this only a partial solution to consumer privacy concerns.

3. Active Jamming approach

This solution requires consumers to carry a device that actively broadcasts radio signals in order to block the operation of nearby RFID readers.

Problems with this approach:

This approach may not made be legal as it would severely disrupt all nearby RFID systems, even in situations in which privacy is not a concern. This could be severely problematic for retailers as it would disrupt their inventory processes.

4. "Smart" RFID tags

A possible approach is to make tags "smarter" so that they provide the desired functionality but protect privacy better. This would involve the use of cryptographic methods.

Problems with this approach:

This type of approach is very challenging to design given the heavy cost constraints on the basic RFID tag. Designing smart tags would involve adding more logic-gates and thus largely increase the cost to produce these tags.

5. Regulation approach

This is an approach that is basically just focused on making the consumer more aware that they are being tagged. An "RFID Bill of Rights" has been proposed as a voluntary framework for commercial development of RFID tags, which includes the following 5 articles:

1. the right of the consumer to know what items possess RFID tags
2. the right to have tags removed or deactivated upon purchase of these items
3. the right of the consumer to access the data associated with an RFID tag
4. the right to access of services without mandatory use of RFID tags
5. the right to know to when, where, and why the data in RFID tags is accessed.

6. Blocker Tags

The approach to addressing privacy concerns that is currently being investigated by RSA laboratories and computer science researchers at MIT is the use of blocker tags. Blocker tags simulate the full spectrum of possible serial numbers for tags, in effect obscuring the serial numbers of other tags. When a consumer carries a blocker tag, he/she induces a physical region of privacy protection in which readers are incapable of reading tags. Blocker tags could be used in two forms: universal blocker tags or selective blocker tags. Universal blocker tags would be incredibly problematic because they would disrupt normal RFID-based commercial processes like inventory control and would thus likely not gain widespread acceptance. These would suffer from the same problems of the Active Jamming approach mentioned earlier and would thus not be an acceptable solution. With selective blocker tags, consumers can designate "privacy zones" consisting of a restricted range of tag serial numbers. The blocker tag would disrupt the reader from reading tags in these zones.

The blocker tag has been viewed in two ways: as a privacy-protection tool and as a malicious tool. As a privacy-protection tool, the tag can designate a particular zone or range of serial numbers as subject to privacy-protection. This feature can be used to protect the items a consumer holds while also permitting unimpeded reading of tags in commercial environments. As a malicious tool, a blocker tag may shield all serial numbers from reading or target everything made by a particular manufacturer. Using a blocker tag in this manner may disrupt business operations or perpetrate theft by shielding merchandise from inventory- control mechanisms.

One advantage of the blocker tag approach, if it is used for its intended use as a privacy-protection tool, is the low cost of implementation. The ordinary RFID tags do not need to be modified at all (most likely) to be compatible with this solution. The blocker tags themselves can also be very cheap, merely consisting of one or two standard RFID tags with slight modifications made. At most, the blocker tag would cost only twice that of a standard RFID tag. This approach and the "kill tag" approach appear to be the cheapest solutions being investigated right now.

The current state of affairs

RSA demonstrated the blocker-tag prototype at the RSA conference on February 24, 2004. They demonstrated the prototype by having people enter their mock "RXA pharmacy" and select a medication type, all of which bore RFID tags linking the drug purchase to the customer's records. Customers were also given paper blocker bags which contained RSA blocker tags that shielded the content of the bag from scanning. The patent on these blocker tags is still pending. They will probably not be sold for a couple of years, and even then not unless stores begin to embed individual products with RFID tags. RSA envisions the future where retailers could offer customers blocker tags embedded in shopping bags rather than killing them at the checkout. This way, no one could surreptitiously discover the contents of the shopper's bag and the shopper could effectively "enforce" their privacy by blocking unauthorized scanning. The advantage of this over just killing the tag at checkout is that once the consumer gets home, he/she can still use the tag in the item for things such as keeping track of the items in his/her cupboard or refrigerator. Thus, the useful aspects of the RFID tags are still retained while privacy is also protected. Though the blocker tag can't do it all, it does appear to be a hopeful solution for protecting the privacy of law-abiding consumers.

Concerns about these solutions

Even with the introduction of solutions like blocker tags, there is a concern that people who don't know that tags are embedded in their items and don't know what this technology is capable of will not know how to protect their privacy. Katherine Albrecht, the director of "Consumers Against Supermarket Privacy Invasion" commented that "You could wind up only with the technology elite equipping themselves with blocker tags instead of working on a solution to protect everyone. It's important to not set up a situation of haves and have-nots when it comes to privacy protection." Thus, before any of the solutions mentioned above could be deemed effective in protecting privacy, strides

need to be made in deciding how the naive consumer can be made more aware of RFID and what RFID means in terms of their privacy. This is an issue that needs to be explored more fully now in parallel with the development of solutions.

The Future of RFID

For many applications, the future of RFID is now. The use of active RFID is growing in the markets that can benefit from its capabilities and handle its limitations. Among these are shipping container tracking, measuring environmental conditions in storage containers, and motor vehicle fleet maintenance. The use of passive RFID is limited only by the amount of money that businesses can save using it, and the benefits that the consumer/customer can gain from having it available.

Additional rollouts of RFID for inventory tracking and supply chain management are proving successful as a cost saving measure, as well as a revenue enhancer. The main issue is the court of public opinion. For businesses to be able to successfully reap the maximum benefits of RFID as a cost-saver, they must convince the consumer that in no way will RFID allow the business or any third party to track them without their knowledge. This can be accomplished a number of ways, including removal or destruction of RFID tags at retail checkout and assertions that RFID will be used to track items on a group basis, not individual items.

Due to its memory and complexity limitations, passive RFID is not currently capable of handling security requirements. There simply is not enough power in a passive RFID chip to be able to handle complex key exchange mechanisms, pseudo-random number generation, and encryption/decryption algorithms. Without all of these factors, and potentially others, passive RFID cannot be expected to be used for any security-related purposes.

Use of RFID for transactions by consumers comes down to one main idea: value for the customer. If customers perceive that the use of RFID is going to benefit a business by reduced cost or added sales, but not benefit themselves, they will not care to use it. It will be yet another piece of technology they are being told to learn about and use, but which they will ultimately reject. However, when there is an actual benefit, like with the Octopus card, which reduces wait times for public transportation, then RFID can be wildly successful.

APPENDIX A

RFID timeline

1940s - Radar refined and used major World War II effort
1948 - Harry Stockman invents RFID, with the publication of his paper "Communication by Means of Reflected Power."

1950s - Early explorations of RFID technology
1950s - D.B. Harris patents "Radio transmission systems with modulatable passive responder"
1959 - Friend or Foe (IFF) long-range transponder system reaches breadboard demonstration stage

1960s - Development of the theory of RFID. Start of applications field trials
1963 -1964 - R.F. Harrington advances theory with "Field measurements using active scatterers" and "Theory of loaded scatterers"
1966 - Commercialization of EAS, 1-bit Electronic Article Surveillance technology: Checkpoint, Sersormatic

1970s - Explosion of RFID development. Tests of RFID accelerate. Early adopter implementations of RFID.
1973 - Transponder system and apparatus
1975 - Los Alamos Scientific Laboratories (LASL) releases its RFID research to public sector, publishes "Short-range radio-telemetry for electronic identification using modulated backscatter"
1975-1978 - Large companies, e.g. Raytheon, RCA, and Fairchild, develop electronic identification systems
1977 - Electronic license plate for motor vehicles
1978 - Electronic detection and identification system
1979 - First implantable RFID tags.

1980s - Commercial applications of RFID enter mainstream.
1982 - molded-neck collar EID
1984 - Radar apparatus for detecting and/or classifying an agitated reflective target. Batteryless, portable, frequency divider useful as a transponder of electromagnetic radiation. Animal feeding and monitoring system
1985 - Electronic proximity identification system. Electronic tag identification system. Remote passive identification system. Implant telemetry system.
1986 - Glass-encased injectible EID.
* First RFID toll collection system implemented in Norway

1990s Emergence of standards. RFID widely deployed. RFID becomes a part of everyday life.
1991 - TI establishes TIRIS, the first multinational semiconductor company to develop and market RFID.

1991 - AAR adopts RFID standard.
1993 - ISO EID standard developed.
1992-1995 - Multi-protocol traffic control and toll collection systems implemented in Texas, Oklahoma, and Georgia.
1994 - All USA railcars equipped with RFID.
1996 - City of L.A. adopts pet tagging.
1997 - Octopus RFID smart cards are launched in Hong Kong.

2000s - Over 350 direct reference patents, vast number of companies enter RFID marketplace.
2003 - Walmart announces that all its suppliers must use RFID by 2006
2004 - RSA technologies demonstrate the first commercial RFID blocker tag.

APPENDIX B

Summary of global frequency regulations for the most common Active RFID bands is shown below. 433 MHz is the most widely accepted frequency for active RFID applications

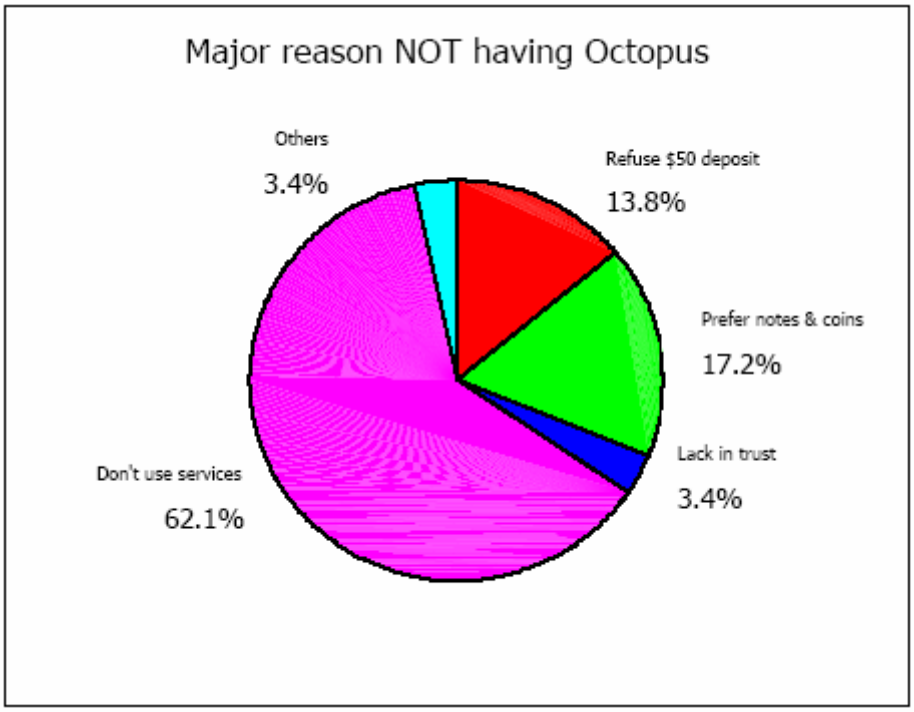
Band	303 MHz	315 MHz	418 MHz	433 MHz	868 MHz	915 MHz	2400 MHz
	302-305 MHz	314.7-315 MHz 42 dBuA/m @10m	418.95-418.975 MHz 10 mW ERP	433.050-434.790 MHz 10mW ERP 10%	868-868.6 MHz 25mW ERP 1%	902-928 MHz	2400-2483.5 MHz
USA	✓	✓	✓	✓		✓	✓
Canada	✓	✓	✓	✓		✓	✓
Great Britain				✓	✓		✓
France				✓	✓		✓
Germany				✓	✓		✓
Netherlands				✓	✓		✓
Singapore		✓		✓	✓	✓	
Taiwan	✓	✓	✓	✓			✓
China / Hong Kong		✓		In process		Limited	Limited
Australia				✓		Limited	Limited
Summary	**Limited acceptance**	**Limited acceptance**	**Limited acceptance**	**Better Choice**	**Limited duty cycle**	**Limited acceptance**	**Poor technical performance**

APPENDIX C

User reactions to Octopus card. Data collected from "An arm's length evaluation of Octopus" by Paynter, J. and Law, P., University of Auckland

	Factors that lead to success of Octopus	Score	Count	%
1.	Quick payment service	937	384	83.8
2.	Easy to carry compared to notes and coins	740	343	74.9
3.	Versatile (wide range of services supported)	443	265	57.9
4.	Allows for negative balance	190	115	25.1
5.	Accurate	142	86	18.8
6.	Savings over traditional methods	105	59	12.9
7.	Loyalty programme	85	52	11.4
8.	Low failure rates in readers and cards	79	49	10.7
9.	Other benefits	5	3	0.66

	Major reason not to use Octopus for all purchases	Score	%
1.	Difficult to stop payment/ get a refund	102	36.7
2.	Worried about security / financial loss	74	26.6
3.	Does not have statements to keep track of expenses	71	25.5
4.	Does not benefit from interest free period	22	7.9
5.	Other reasons	9	3.2
		278	100%



Potential Services (Ranked)	Count	%
1. Supermarkets / Chinese market	135	74.2
2. Newspaper stand and magazine stand	110	60.4
3. Road Toll	90	49.5
4. Snack/ food stand	73	40.1
5. Stationery Shop	55	30.2
5. Video games centre	55	30.2
7. Transportation	46	25.3
8. Other services	12	6.6

APPENDIX D - References

Animal Microchipping

"Philips RFID Expertise Used to Protect Against Animal Disease Epidemics in Europe", February 17 2004, http://biz.yahoo.com/bw/040217/176019_1.html

"USDA Begins Animal ID Program", December 9, 2003, http://www.rfidnews.org/archives/000380.html

Ronsvalle, J. "RFID Microchip Implants: Pets and Other Animals", *Charagma Watch,* Champaign, IL, 2003

Wal-Mart

Glasner, J. Mar. 26, 2003, http://wired.com/news/print/0,1294,58204,00.html

Feder, B. "Wal-Mart Hits Snags in Push to Use Radio Tags to Track Goods", *New York Times,* March 29, 2004

Prada

"PRADA Epicenter Revisited", *Fredhouse.net,* April 5, 2004, http://www.fredshouse.net/archive/000159.html

Woodhead, B. "Chips out of fashion at Prada", October 21, 2003, http://afr.com/cgi-bin/newtextversions.pl?pagetype=printer&path=/articles/2003/10/20/1066631355534.html

Tesco

Ericson, J. "RFID Complications at Gillette", *E-Business News*, Friday, April 04, http://www.line56.com/print/default.asp?ArticleID=4554

McCue, A. "Gillette slams privacy concerns over RFID tracking", *silicon.com,* August 14, 2003, http://www.silicon.com/networks/lans/0,39024663,10005596,00.htm

"Tesco Starts Full-Scale FRID Initiative", *RFID News*, November 16, 2003, http://www.rfidnews.org/archives/000328.html

RFIDs in Retail

"RFID tag makers may lose their shirts", *Reuters*, November 3, 2003, URL: http://zdnet.com.com/2100-1103-5101130.html

Benetton

Yoshida, Junko, Clothier Benetton adopts Philips' RFID technology for 'smart' labels, *EETimes*, March 12, 2003, http://www.eetimes.com/article/showArticle.jhtml?articleId=9901084

EE Times Staff, Benetton backs off RFID deployment, *EE Times*, April 5, 2003, www.eetimes.com/article/showArticle.jhtml?articleId=12804031

Batista, Elisa, 'Step Back' for Wireless ID Tech?, *WIRED NEWS*, www.wired.com, April 8, 2003

Benetton Explains RFID Privacy Flap, *RFID Journal*, June 23, 2003, http://www.rfidjournal.com/article/articleview/471/1/1/