

6

RFIDs: Who's Listening?

Alex Bitz and Joseph R. Osborn

Introduction

The parents of two young children decide to take a family vacation to Paramount's Great America theme park in Santa Clara, California. Upon arriving at Great America's ticket booth, they are caught off guard when the clerk asks if they wish to purchase a locator bracelet to place on their children for the day. After inquiring about the bracelet, the clerk informs the parents that this is a new technology that the park has recently implemented to help locate lost children. They are told that each bracelet contains a Radio Frequency Identifier (RFID) that transmits a unique code over radio waves. The unique number stored in each bracelet is transmitted constantly, allowing for readers throughout the park to track the location of the RFID bracelet and store its location in the park's central database. Parents are then given a device, which they can plug into kiosks all throughout the park, to see exactly where their children are located in the park at any given moment.

The new technology that Paramount's Great America theme park has implemented is produced by a company called SafeTzone (*Information Week* 2004) and relies on the use of RFID technology. RFID is short for radio frequency identifier, which is a term that is used to describe any technology that emits a unique identifier over radio waves. RFIDs are much like a wireless barcode system in which a self-powered microchip transmits a series of numbers over a short distance, generally 300 to 1000 feet. A receiver is used to pick up the unique number transmitted by the RFID and send it on to a system which then compares that number against its own database. The system is responsible for determining what the received number represents. This number could be used to represent a product such as an individual

bottle of shampoo or even an individual person such as in the case of the wristband at the amusement park.

History of RFIDs

The concept of RFID technology dates back to the 1960s when R. F. Harrington studied the electromagnetic theory related to RFID in his papers "Field Measurements Using Active Scatterers" and "Theory of Loaded Scatterers" in 1963-1964 (Chiesa et al. 2002). Though it was researched extensively in the 1970s, it was not until the 1980s that the technology made its first commercial appearance, which initially came in the form of animal tracking devices. In the later part of the 1980s, the technology had been implemented as a toll road access device similar to the current E-ZPass tollway system that is commonly used today. This technology was first implemented in Norway in 1987 and quickly found its way to the United States where it was put to use on the Dallas North Turnpike in 1989 (Chiesa et al. 2002). RFIDs in the 1980s were effective for their purposes at the time but the devices were still too large and expensive to be used for many practical applications.

RFIDs Today

Advancements in technology have allowed manufacturers to produce RFID tags that are as small as a grain of sand at a price range of five to fifteen cents per unit. The size and affordability of transmitters has led many companies to look at the possible benefits of using RFIDs in their industry rather than the standard barcode that is in widespread use today. Unlike the barcode, RFIDs can have both read and write capabilities which allow for the number that the RFID transmits to be changed in real time. The radio waves transmitted from an RFID can travel through many different substances and conditions such as snow, fog, and paint, requiring no direct line of site to be read by a RFID scanner. This gives RFID tags an enormous advantage over the standard bar code label which must be within inches of a scanner to be read. In addition to this advantage, RFID tagged products can be scanned at 150 to 1,000 items per second while a barcode tagged product must be scanned one at a time.

Benefits of Using RFID tags

In addition to being an upgrade from the standard barcode, RFIDs have two attractive benefits for those who use them. For one, they allow a company to assign multiple values such as a product name and/or expiration date to every RFID that they purchase. Secondly, receivers throughout their company can track those values automatically without any human interaction. This presents a very efficient scenario for companies who wish to use RFIDs for inventorying their products. With such a system in place, a company such as Wal-Mart now has the ability to install an RFID on every product that is stored in their warehouse. Once the product leaves the warehouse shelf, a receiver will immediately receive the signal and determine that the product has been taken out of stock. Under this structure, the system would know the exact quantity of every item in stock and could be programmed to automatically reorder items when needed. Wal-Mart specifically has

already mandated that all its suppliers include RFIDs in their products by the year 2005 (Privacy and Human Rights 2003: Threats to Privacy).

Implementations

The potential uses of RFID tags are already being realized by many organizations and industries that are anxious to adopt the technology for various reasons. Hospitals, for instance, are considering using RFIDs to track patients once they are admitted in order to reduce the risk of incorrect surgeries being performed. An RFID could be placed inside the band each patient is already given when admitted to the hospital and would be transparent to the patient. In addition to tagging patients, hospitals are also considering putting tags on every employee so that they can track them throughout the hospital to increase productivity. The technology that has been discussed for this purpose is called Skinplex which involves implanting an RFID in the skin of the employee and the skin itself acts as the RFID antenna (RFID 2004).

McDonalds Corporation has discussed the future implementation of an RFID system that will be labeled MC Radio Chip. This system will allow customers to use an RFID card, issued by McDonalds, to speed up purchases. Under this system, once a customer has received their order they will no longer need to pay cash or have their credit card run by a clerk. Instead, the clerk will already have the customer's information in the system because McDonalds will know who they are as soon as they walk in the door. The MC Radio Chip will be linked to the customer's credit card and all they will need to do is confirm the amount of their order and be on their way (In Brief: McDonald's to Use MC Radio Chip System).

Inventorying products is one thing but what about inventorying people? The country of Mexico has one of the largest child abduction rates on the planet. In response, the government of Mexico is researching and considering the implementation of a nation-wide RFID tracking system that will allow parents to implant an RFID chip in their children so that they can be tracked if kidnapped. This possibility has been discussed for years, but Mexico would become the first country to actually implement such an elaborate system of tracking people (How RFID Will Help Mommy Find Johnny, 15 September 2004).

Technical Background

In order to make an informed decision about whether or not the use of RFID tags should be a concern to the consumer, it is important to understand how these devices work. There are three main components that make up a usable RFID system, the first of which is the antenna. RFID antennas are typically made of copper or aluminum and they are fairly easy to see once a person knows what they look like. A much cheaper alternative to the common metal antenna that has recently come about, thanks to companies such as QinetiQ Metal Printing, is the use of specially formulated metallic ink as an antenna. These new inks, created specifically for use as RFID antennas, contain conductive silver or carbon, which can serve as channels for electronic signals. This form of antenna is nearly imperceptible to the human eye and can easily be concealed in product packaging if a producer wishes to do so. The second component of the RFID is the transceiver, which both sends and

receives the radio or microwave transmission through the antenna. The last of the three components is the transponder, which transmits a signal so that the position of the transponder can be monitored.

There are two types of RFID tags in production today, active and passive tags. Passive tags are programmed with an ID when they are manufactured and can transmit that ID up to 1000 feet in ideal conditions. Active tags have read/write capabilities, which allow them to be reprogrammed in real time, but as a consequence of this capability, they can only transmit their signal approximately 50 feet.

Consumer Concerns

The uses of RFID technology that have been mentioned thus far vary in their level of intrusiveness to consumers. While manufacturers can obviously benefit a great deal from the technology, consumers are naturally concerned about the implications of such technology to their personal privacy. Each of the uses mentioned, by itself, may or may not be considered intrusive but consider what the implications might be if corporations begin to consolidate the information that can be learned from the various uses of the technology. To address this concern, it is necessary to first isolate the usage of an RFID tag within a single environment.

Scenario: Wal-Mart's Proposed RFID Implementation

The lifecycle of an RFID tag as it is intended to be used in Wal-Mart's proposed implementation would be as follows: At an early stage of manufacturing, the producer installs an RFID in a product. The producer uses that RFID to track the product through its production cycle and increase efficiencies during production. The product then goes to the producer's warehouse where it sits in stock until it is purchased by Wal-Mart. Once purchased, the product is shipped to Wal-Mart's warehouse where the RFID is scanned and the specifics of the product are entered into Wal-Mart's database. Wal-Mart uses a cross-docking strategy so the product is then taken directly from one truck and placed onto another truck, being scanned automatically by readers that are installed in each truck. Wal-Mart's system now knows that the product has left the first truck and is sitting on the second truck. The product is then shipped directly to a Wal-Mart retail store where it is automatically scanned upon arrival through the process of being carried off the truck and placed on the stock shelf in the back of the store. Soon, the item is moved from the back of the store to the floor where it is displayed and eventually picked up by a customer. The customer puts that item in their shopping cart, along with the other items they wish to purchase, and walks straight out of the store. Upon leaving the store, an RFID scanner located at the exit door automatically reads the unique code that is being broadcast from each of the 20 items sitting in the customer's shopping cart as they walk through the door as well as the unique code off the customer's Wal-Mart card which is linked directly to their Visa for immediate payment.

The entire situation above, with the exception of the checkout scenario, can already be accomplished through the use of a traditional barcode system and some additional labor. This is where the concern begins however. In the proposed scenario, the customer has just left the

store and they now have a shopping cart full of items that are still broadcasting their ID even though the RFID tag's purpose has been fulfilled. There is currently no legislation that requires a store to inform customers of the presence of RFIDs on the products they purchase so the customer may not even be aware that they exist in the first place. A non-technical customer may not have any idea that the technology that just allowed them to avoid the checkout line does not disable itself upon leaving the store. This concern will be addressed in more detail later.

Assuming that Wal-Mart is using active tags rather than passive tags and they have the ability to disable the tag after it has been scanned at the store's exit door, it would be plausible to conclude that there is little harm in using RFIDs as long as they are isolated for use within a single store. This is not their intent as far as the authors are aware but for the purposes of this example, it allows us to assume that the tracking mechanism is disabled once the product has left the store. With this assumption in mind, consider the possibility, however, that Wal-Mart not only has an RFID scanner at their loading docks and their exit doors, but they also install multiple scanners in every department of the store. Doing so would allow them to track each product in a person's shopping cart as he or she carries it around the store. Now, Wal-Mart not only has the ability to track the items that people purchased but they can track their shopping habits all throughout their store. Once someone has walked out their door after making a purchase, all the items in their cart are tied to them as a shopper.

Implications of Wal-Mart Scenario

With a system that is designed to automatically compile all the necessary data, Wal-Mart can very easily generate a report that shows when someone entered their store (based on his or her Wal-Mart card which is scanned when he or she walk in), and what items they placed in their cart as well as the exact time they pulled those items off the store shelf. They will also have the ability to see that they went straight to the movie section and immediately put a copy of a new release in their shopping cart. They carried the movie around through several departments and then fourteen minutes later; put a red sweater in their basket from the clothing department. They also put a name brand juice in their cart, which they carried around within the food department for only two minutes before putting it back on the shelf and selecting the less expensive store brand equivalent of the item.

Tracking consumers in this fashion is the equivalent to having a human follow each consumer around the store and take notes of their every move so that their habits can later be permanently stored in the company's records. This is certainly an invasion of one's privacy as it has been defined in this book and it is likely that the majority of consumers would feel as though their privacy had been violated if such a practice were put in place without their consent.

Information, of course, is not kept within a single store's computer system. Reading one of the numerous privacy statements that from any financial institution, shows that personal information is shared between that institution and its affiliated companies. This means that Wal-Mart can take all the knowledge that they have about a person's buying habits within their store and share it with as many of their hundreds of

affiliated companies as they wish. The information that Wal-Mart collects, combined with the information that is acquired from their affiliated companies, can be used to build an incredibly accurate and complete profile about an individual. That profile could then be used to help Wal-Mart and all of its affiliates market their products more effectively to people's buying needs, habits and desires. Richard Hackathorn, who has written the eye opening article "The Future: eXtreme data warehousing," has explained that the magnitude of data collection will "increase by multiple orders of magnitude in future generations" and the access to this data will be fairly easy – due to numerous web and other advancements. Because of this ever increasing array of data, the theory of "PAPA" (Privacy, Accuracy, Property and Accessibility), which outlines four crucial ethic categories, must be looked into more intently.

Opposition to RFID Technology

The marketing implications involving the use of RFID tags alone have drawn great opposition to the technology. Many civil liberties groups, such as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), feel that this type of consumer surveillance is an invasion of privacy. Leaders, such as Katherine Albrecht within CASPIAN, have criticized such organizations as MIT's "Auto ID Center" for making light of the privacy concerns associated with RFID implementation.

Ownership of Information

Perhaps a greater concern than those surrounding the marketing possibilities is the issue of property. Who owns the data that is collected about a consumer? Does Wal-Mart own the data they collect simply because they own the system that allows them to collect it or does the consumer own the data because it is their personal information? If the data is the property of the store that captured it, then it is quite possible that store would be allowed to make a profit from selling the information to outside parties who would be interested in paying for such knowledge. According to the *Business Intelligence Journal*, "the general consensus is that this information is owned by the company and is not a privacy issue as long as it is used to better serve [a companies] customers and prospects" (Adelman et al. 2004). This philosophy is flawed because it leaves the company that stands to benefit from the use of the consumer's information to be the sole decision maker regarding whether or not the use of that information "better serves" the customer. There needs to be an outside influence in the decision-making process in order for the decision to truly be made in the best interest of the consumer.

Information Access

Access is another topic of concern. Who will have access to the data once it has been obtained and will those who have access be limited to seeing only a portion of the data or will they have unrestricted access to the entire data set? This concern must be dealt with on multiple levels. As mentioned earlier, hospitals are looking at implementing RFID tags on their patients. Even though the initial implementation is intended to

be a bracelet that will be worn while the patient is in the hospital, it is entirely possible that future implementations could involve the use of an RFID that is embedded into a health insurance card. This type of system could not only track the frequency that a patient visits a single hospital, but, if shared among affiliates, the data could show how often a person visits a doctor, hospital, pharmacist, physical therapist, dentist, eye doctor or any other type of medical clinic. Much of this information is already kept by a single medical coverage provider but it is not likely that a health care company would currently have information regarding a subscriber's dental or vision habits.

The Health Insurance Portability and Accountability Act (HIPAA), regulates the use of health insurance information in the United States. Thanks to HIPAA, the concerns regarding the sharing and accessibility of healthcare information as a result of the implementation of RFID technology in the healthcare industry would ultimately be regulated by the HIPAA guidelines as well.

Scenario: Wrongly Accused

Some industries do not have guidelines such as HIPAA to follow however. When it comes to criminal court cases, law enforcement agencies can access a great deal of information that would normally be unavailable to outside parties. Going back to the Wal-Mart example, what if someone has primarily frequented the same Wal-Mart for over a year, and Wal-Mart has all his shopping visits and purchased items stored in their system for that time period. Out of the blue, a co-worker asks him to fill in on the company softball team one evening. He has never played softball or any other sport before but decides to help the team out. The game is in an area that he does not visit often and on the way, he stops by the local Wal-Mart store in that area to pick up a softball bat. On his way home, he stops by Lowes Hardware, a Wal-Mart affiliate and picks up trash bags, amongst other things, because he forgot to buy them the past weekend.

The next day, he receives a visit from the police who have named him as a suspect in a brutal homicide that occurred in the same area as the softball field at which he played the night before. The police have named him as a suspect because they were able to access information stored in the Wal-Mart central database that shows that he purchased a bat as well as trash bags in an area in which he does not regularly visit. Coincidentally, both items were used in the crime. The time frame of the purchases makes him a prime suspect and he has no alibi because he drove to the game by himself and came home by himself. Knowing the full scenario, this information clearly does not prove guilt but to an investigator who is only looking at known facts, it can look very suspicious and could even lead to a situation where guilt is predetermined based on facts such as these, thus resulting in a wrongful trial simply because of circumstantial evidence. As illustrated in this scenario, sometimes, too much data can actually be a bad thing and can lead to false positives.

Accessibility is an increasing ethical concern in today's information age and it is one that requires companies to individually decide where they stand on privacy and ethical issues. Even though a practice may be legal and financially beneficial to a company, it may not be an ethically

sound choice. The use of RFIDs can be implemented in a way that is ethically responsible but the temptation to use them to their full potential will most likely be too overwhelming for businesses to turn down due to an immense amount of pressure to remain competitive in their industry. Companies today tend to put the desire for customer information first with the ethics of their practices being a distant second.

Customers Need to Have Input

One of the main problems with the use of RFID technology in retail stores is that it does not allow the consumer to choose whether or not the technology can be used. This violates an individual's privacy because it does not allow them the ability to keep desired information strictly to themselves.

Scenario: RFID Technology Aids Divorce

Take for instance a man who goes to Victoria's Secret and purchases some women's lingerie. He then goes to a grocery store and purchases a pack of condoms, in both cases, entering and leaving the stores quickly, allowing the automated system to charge him via his store-issued ID card that links directly to his bank account. The items he purchased were tagged with RFID tags and he did not have the ability to disable those tags because they are the property of the store until he completes his purchase. The man then proceeds to drive down the tollway to his mistresses' house on the other side of town where he uses the newly purchased items.

A week later, the man's wife grows curious when she starts receiving several advertisements for lingerie and condoms that are addressed to her husband. She then goes online and checks her E-ZPass account that shows that her husband's car was scanned at an automated tollbooth across town a week earlier when he said he was working late. His wife quickly puts it all together and subsequently files for divorce. Though the man in this example most likely deserves what is coming to him as he has committed adultery, he still has the right to keep any information about himself, such as his purchasing decisions, a secret if he wishes to do so.

Ethics Versus Profit

Businesses place a great deal of value on the demographical information that they purchase about the consumers in their market; so why is it that they do not put any effort into understanding how sensitive their customers are to the unethical practices used to acquire that information? A large portion of a consumer's purchasing decisions are based on their personality type. Knowing that customers are concerned about the privacy of their information or the methods that a business uses to obtain that information could be a valuable marketing tool as well. Unfortunately, the value of the information that is obtained about consumer purchasing habits through ethically questionable methods often outweigh the consequences associated with the methods used to obtain that information.

RFIDs Don't Die

In all of the examples thus far, it has been assumed that the RFID tags that have been used in the given scenarios are disabled once the product leaves the store. One of the most disturbing facts about RFID tags, however, is that they do not actually disable themselves at any point. As a matter of fact, an RFID will continue to broadcast its signal until its power dies which can be several years into the future. With tags being produced as small as a grain of sand, it is entirely feasible that tags would be placed on every single item we purchase from our food to the clothes on our backs. In many cases, the chips could be virtually undetectable if the consumer were not informed of its presence. The tag may just be the dot to the "i" on the Gucci sunglasses or Timberland backpack. Manufacturers intend to market the continual broadcasting of an RFID tag as a benefit to the consumer, saying that they can purchase scanners for their own homes that will allow them to track all their own items within their house. When people go to the grocery store, they will be able to bring their groceries home and place them in their smart fridge that will instantly inventory the food once it is within the reading range of the scanner. The refrigerator will then be able to print out an inventory list at the push of a button or, with a little input from the user, a shopping list of the items that are low or no longer in inventory.

As for clothing, people no longer have to hunt through the house for their favorite blouse. With scanners located all over the house, they can quickly check their computer or Palm Pilot and tell whether that blouse is sitting in their closet or if it is downstairs in the laundry room. But if a person's scanners can pick up the RFID signals, what is stopping someone else outside their home from picking it up? What about the neighbors, who also have RFID scanners in their homes, they will be able to tell what items all of their neighbors have purchased and keep in their homes. It would certainly be an invasion of privacy if a person were to physically come into someone's home and go through their dresser drawers, but would it be considered an invasion privacy if they had the ability to go through someone's drawers without ever leaving their bedroom?

Our definition of privacy would suggest that the method does not matter: this act would still be an invasion of one's personal privacy. Even though the act would be legal, it would be unethical in practice. Along those same lines however, many upstanding citizens would be unlikely to physically steal anything even if they knew they would not be caught. These same people, however, might not think twice about downloading an MP3 track over a peer-to-peer file-sharing network. Somehow, the ability to do something unethical or even illegal from the comfort of one's own home somehow makes people convince themselves that it is not wrong to do so. If RFIDs are able to be picked up by scanners other than those belonging to their owner, people will not hesitate to try to pick up their signal and they may even enjoy the challenge of trying to figure out what their neighbors' interests and purchasing habits are.

Considering the accessibility of information, imagine if the police had records of all the RFIDs that were used to tag alcoholic beverages for a particular liquor store. They could then set up a checkpoint where

they automatically pull over every car passing by that has alcohol in it without knowing or caring if the alcohol were opened or not. This would most likely not be an illegal practice but it certainly involves profiling based on whether or not someone purchases alcohol and it definitely invades one's privacy.

Security of information is another issue when considering RFID technology. With the potential to have tags on items that are linked to an individual's financial information such as credit cards, how can one keep others from picking up this information and reproducing it? Even the strongest encryption can be broken and this technology would be a new method for thieves and hackers to test their skills and find a way to reproduce someone else's RFID such as their Visa card. With identity theft rising at such rapid rates already, it seems ludicrous to introduce a new technology that could actually have such adverse effects. Once the RFID's unique code has been learned and is able to be reproduced, it would be very easy for someone other than the owner to use that ID to wrongfully purchase items using an unknowing victim's credit. The methods for ensuring that RFID technologies are secure are still in development at this time but this will clearly be an issue that must be addressed if this technology is ever to be used to its full potential.

Mexico Considers Tracking People

It was mentioned earlier that the Mexican Government is considering implanting children with RFID chips in order to help crack down on the astronomical kidnapping rate. The implementation of such a system would be an enormous undertaking as it would involve not only putting the chip itself in every individual child, but it would also require that RFID scanners be placed all over the country in order for the system to be effective. This would be the first system in the world that would actually have the capability of tracking a person's every move. This would be a clear violation of the child's privacy because the chips would be installed at birth and would not have the ability to be turned off. The extent of Mexico's plans for this system are unknown but the likely scenario would be for a child to keep the chip in place until they become an adult, at which time they can decide to have it removed.

It may seem that under these circumstances, it is perfectly reasonable to sacrifice a child's privacy in order to ensure their safety. The problem however is that children in Mexico are not kidnapped to be held for ransom; rather, they are kidnapped because their organs are worth a great deal on the black market. Given this motive, the implementation of a nation-wide RFID tagging system in children would only encourage a captor to quickly mutilate its victim in order to physically remove the tracking device from their body. The most widely argued point about implanting an RFID chip into a child is the matter surrounding the element of choice. Will the children be allowed to decide if they want to be tracked or not? Removing these chips will be costly and many may not be able to afford it. Thus, this creates the ultimate dilemma: the children may not want the chip inside them once they grow up but cannot afford to take it out, therefore having to live with a decision that was made for them.

Adverse Health Effects

Why wouldn't someone want an RFID chip inside him or her? Beside the fact that it may be an invasion of privacy, there are many health concerns that have been disregarded when considering the installation of a chip into someone's body. Though the FDA has approved the "VeriChip" implant, an RFID chip that is read with the "VeriChip" freestanding scanners, they have also reported the harmful effects of injecting the chip into one's flesh. Why would the FDA approve a product that can cause such harm? Harm including "'adverse tissue reaction,' 'migration of the implanted transponder,' 'failure of implanted transponder,' 'electrical hazards' and 'magnetic resonance imaging [MRI] incompatibility'" (FDA Letter 2004).

Ethical Concerns

The questions on an ethical level about whether RFIDs should be implemented are indeed tough because there are two sides to the argument. The powerful ideals of both sides have valid points, depending on what angle the dilemma is being looked at. There is an issue of right-versus-right at hand rather than simply taking a deontological approach in saying that there is an absolute set of rules already to say what is right. There are three main ethical theories that may help in the decision process of whether RFIDs are good for our society and may help in figuring out which right may indeed be right: ends-based thinking, rule-based thinking, and care-based thinking.

Does the implementation of RFID chips produce the greatest good for the greatest number of people – an ends-based thinking approach? The benefit of implementing these chips may dwarf the ethical concerns that are raised due to the influence and decision-making power that large manufacturing companies have. It is scary to think that consumers may ultimately not have a choice as to whether or not the implementation of RFIDs will give a larger benefit to society. Consumers are living with the decision of companies to go ahead and implement RFID chips – having no say at all as to whether or not the implementation of RFID chips produces the greatest good for the greatest amount of people and whether that matters at all. The issue of ends-based thinking has been overlooked without consideration. This has therefore led many organizations, such as CASPIAN, to become so outraged that they have even suggested to consumers to "pulverize," in CASPIAN's own words, any RFID that they may see. This animosity toward RFIDs could have been avoided if companies would have used an ethical approach such as the one proposed by the article "The Ethical Systems Analyst."

This article states, in summary, that the first step in an ethical analysis approach is to "identify the stakeholders in the situation who possess ethical perspectives" and then to move onward to find out if the possible conflicts that these people may feel are relevant and then use a conflict resolution tool to work through these problems.

Have the many companies that have implemented RFID technology thought about Kant's rule-based thinking approach? This approach simply states to "follow only the principle that you want everyone else to follow." Organizations are attempting to pave the path for the rest of us to follow without getting any input from consumers –

taking initiative as to what we “ought to do” rather than what might be best for society as a whole. It is possible that the use of RFID technology does benefit society, but it should be society that decides the boundaries of the technology’s implementation, not the large corporations who stand to gain far more than consumers.

When considering the use of RFID chips in children, the golden rule of “do to others what you would like them to do to you” should be used – a care-based thinking approach. Though many parents would love to know where their child is at all times, would these same parents want someone else, perhaps their very own parents, to know where they were at all times? Perhaps some would not mind. Then there are those who would argue that it is an invasion of their privacy. Even as a company decides to implement RFIDs onto their products, they need to understand the privacy implications that will apply to them as individual consumers. Sometimes this is hard to do given the monetary benefit of installing these chips from an organizational, bottom line, standpoint.

Conclusion

No matter which theory best helps in determining the “right” choice, it is clear that RFID technology comes with social implications; Implications that have lead groups such as CASPIAN to resist the implementation of RFIDs because they feel that they present too many unethical effects. As technology keeps advancing, society keeps a watchful eye. In order to maintain an ethical balance between convenience, efficiency and privacy, consumers must question new technologies and understand their potential impact before allowing technological advancements to be adopted and implemented in everyday life. RFID chips should not be treated any differently. Instead of sidestepping the issue of privacy, we need to give it great consideration for the betterment of society. There are many benefits to RFID tags: they allow pet owners to find their lost pet, marathon runners to accurately monitor their race times and businesses to identify and track their assets quickly and accurately among other things. In the grand scheme of things, these benefits may not outweigh the obtrusiveness of privacy that accompanies them.

Works Cited

- Adelman, Sid, and Dyche, Jill, and Hackathorn, Richard, and Imhoff, Claudia, and Loftis, Lisa. “Experts Perspective.” *Business Intelligence Journal*. (2004).
- Chiesa, Mario, et.al. 4 March 2002. “RFID: A week long survey on the technology and its potential.” 21 Nov 2004. <http://people.interaction-ivrea.it/c.noessel/RFID/RFID_research.pdf>
- Corder, Steve, Watson, Heather, and Wood-Harper, A.T., and Wood, J.R.G. “How We Profess: The Ethical Systems Analyst.” *Communications of the ACM*. March 1996, Vol 39 No. 3.
- Gilbert, Alorie. “Theme park takes visitors to RFID-land.” 14 September 2004. ZDNet. 21 Nov 2004. <<http://news.zdnet.com/2100-9584-5366509.html>>
- Kidder, Rushworth M. “How Good People Make Tough Choices: Resolving the Dilemmas of Ethical Living.” 1996. Institute for

- Global Ethics. 21 Nov 2004. <<http://www.globalethics.org/pub/toughchoices.html>>
- "Ethical Dilemmas" 2004. Jewish Association For Business Ethics. 12 Nov 2004. <<http://www.jabe.org/ethical-profiling-index.htm>>
- "FDA Letter Raises Questions about VeriChip Safety, Data Security." 19 Oct 2004. *Spychips*. 21 November 2004. <<http://www.spychips.com/reports/verichip-fda.html>>
- "How RFID Will Help Mommy Find Johnny; Florida theme park uses SafeTzone application to help visitors locate other members of their group." *Information Week*. NA, September 15, 2004. ISSN: 8750-6874.
- "In Brief: McDonald's to Use MC Radio Chip System." 23 Aug 2004. Bloomberg News. 21 November 2004. <<http://proquest.umi.com/pqdweb?index=1&did=000000684631401&SrchMode=1&sid=3&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1099263912&clientId=56281>>
- "Privacy and Human Rights 2003: Threats to Privacy." *Privacy International*. 21 Nov 2004. <<http://www.privacyinternational.org/survey/phr2003/threats.htm#Radio-Frequency%20Identification>>
- "RFID gets skin-deep alternative." 4 August 2004. Silicon.com. 21 Nov 2004. <<http://networks.silicon.com/lans/0,39024663,39122871,00.htm>>