

(Figure 1) Source: www.SpyChips.com

This is a picture of an RFID tag in a Gillette razor packaging.

Radio Frequency Identification (RFID)

The purpose of this paper is to inform businesses and governments who plan to incorporate Radio Frequency Identification (RFID) systems into their work about the potential security and privacy vulnerabilities associated with the technology. I will also persuade them to regulate the use of this technology in a manner to better protect privacy and security of the general population. RFID technology can offer many advantages to manufacturers and the government. Manufacturers can use this equipment to better supply consumers by having more



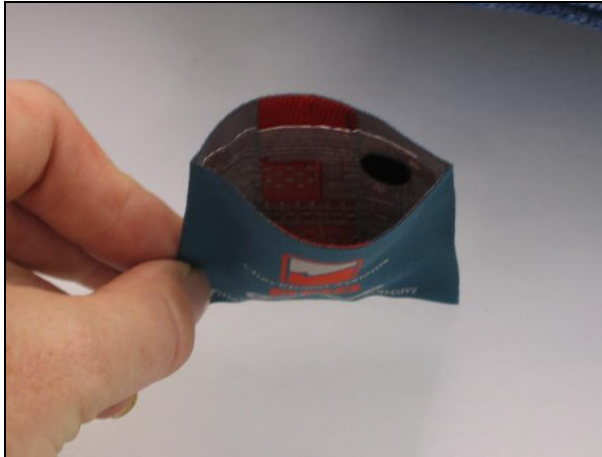
(Figure 2) Source: www.SpyChips.com

This is a picture of an RFID clothing label made by Checkpoint sewn into a Champion jacket.

detailed information on the products sold. The government could use this technology to aid in anti-counterfeiting technology and assist with accurate reading of biometric data. However, while this same technology can aid the manufacturers and government, it also poses a threat to the general population. RFID could easily be used as tracking devices for everything on the planet, even humans. This may sound farfetched, but this is actually the plan of some large companies. Proper precautions need to be

taken by the organizations implementing this technology to ensure the safety and privacy of the public.

To understand the threats that this technology can produce, a general understanding of it



(Figure 3) Source: www.SpyChips.com

This is a close-up view of the same tag shown in Figure 2.

is required. Radio Frequency Identification

systems are exactly what they say they are.

They are systems that use radio frequencies to

read identification data. Data is stored on

specially made devices called “transponders”,

also known as “tags”. These tags come in two

types: *active* and *passive*. Active tags are tags

that include a power supply such as a battery.

Passive tags, on the other hand, do not require a local power source. (Figure 4) Tags are as large

as needed and can be half as small as a grain of sand. (14 Albrecht) Passive tags are small

enough to be placed on store-bought products and can even be woven into clothing. (Figures 2

and 3) (19 Albrecht) Each tag has two parts, a microchip and an antenna. The antennas, usually

flat and maze-looking, can be seen on the back of barcode stickers in retail stores. The

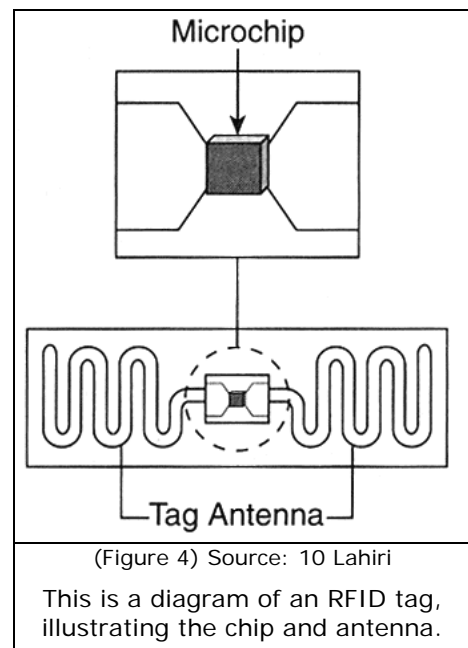
microchip is located somewhere along the maze of the antenna and is what stores the

information. Retailers that have already implemented RFID tags include Wal-Mart, Best Buy,

and Target. (7 Albrecht)

The other important part of any RFID system is the tag “reader”. The reader broadcasts a radio wave which the tag’s antenna receives. The antenna amplifies the waves and powers the microchip. The chip then broadcasts back the information on it, which can be text or a unique ID number. Since this technology utilizes radio frequency, a direct light of sight is not needed between the reader and the tag. The size of readers can be as large as needed to as small as a handheld device. RFID readers are similar to the antitheft readers that can be seen at the doorways of many stores. (Figure 5) These antitheft systems are similar to RFID, but the main difference is that they do not store information; thus they do not create a privacy threat. (78 Lahiri)

The technology of RFID itself is not new. In fact, versions of this idea have been around since World War II. During World War II, the British, Japanese, Germans, and Americans all were using Radar which informed them of incoming aircraft. However, this system did not distinguish between returning allies’ and approaching enemies’ aircraft. To overcome this obstacle, the German pilots would roll the aircraft, in turn altering the signal sent back to the radar. Essentially, this is the same idea of the RFID technology. But in 1973, a man by the name of Charles Walton patented a passive RFID tag that could unlock a door without a key. A reader near the door read a signal from the RFID card he had created, and when it read an authorized number, the door unlocked. This was the beginning of the RFID tags that we know today. (“The History of RFID”)



If the technology has been around since the 1930's, then what's all the fuss about? Though the technology is not new, the proposed uses of RFID is what is gaining the media's recent attention. Businesses, especially manufacturers and retailers, plan to use RFID tags to more or less replace barcodes. This would be done to more easily and efficiently track inventory. Since some RFID tags are writable, meaning a reader could write data to the tag, the tags could be updated with information such as location and time while it moves through the supply chain. While this can be very useful for manufacturers to track products, it also creates privacy concerns. If the tag is still enabled once the product leaves the store, it can be tracked while in the consumer's possession and even all the way to the landfill. (Figure 6) (67 Lahiri)

Businesses such as Wal-Mart and Procter & Gamble plan to put RFID tags into everything they possibly can. (33 Albrecht)



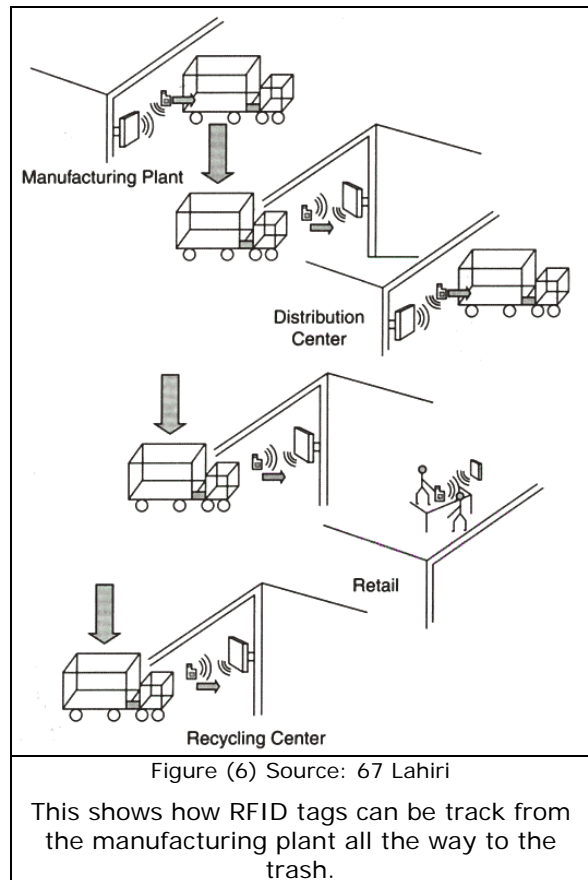
(Figure 5) Source:
<http://www2.cpttm.org.mo/cyberlab/rfid/intro.html.en>
This is an RFID reader that would be installed at an entrance/exit of a store.

A numbering system has been created that can utilize over $8E28$ (also thought of as 80 thousand trillion trillion) unique id numbers, which is claimed to be more than enough to track every manmade physical product for the next thousand years. (26 Albrecht) This means that every soda can, pack of gum, and needle could have its very own personal identification number to track it around the globe. This means that it is possible for each and every product ever made to have its own website. As the product moves through the supply chain, information about it can be stored

in a database and then linked to the internet. The internet can query the databases for the unique

ID, and return results of where it originated, everywhere it's been and at what times, where and when it was purchased, and even bank accounts that were linked when the product was purchased.

The fact that RFID tags can be read even without a direct line of sight to the ID tag is itself a risk. A reader can read a *passive* tag up to 30 feet away with the current technology. (9 Lahiri) The most common *active* tags can send signals up to about a mile. But active RFID tags that are used to track animals in the ocean can transmit data even to low orbiting satellites. Furthermore, like most technology, improvements will be made on the current devices and allow them to read from much further distances. This could be dangerous in a situation such as the following example. As you leave the store with all your holiday gifts in hand, every



item you just bought contains an RFID tag that contains product information. A man sitting in a car nearby equipped with a reader can read all of the items in your bags to see if you're gifts are worth trying to steal. The fact that tags can be read without actually being seen is not at all safe.

Another reason RFID poses a threat to personal privacy is that no information stored in RFID tags are encrypted. This means that if RFID tags are used as passports or driving licenses, information such as full name, date of birth, place of birth, and age could all be stored in a tag, unencrypted. When near a reader, the tag would broadcast this personal information through the

air in all directions, which is clearly a bad idea. Even if encryption is introduced to the tags, it is only a matter of time before the encryption is reverse engineered. This means that no personal data should ever be stored on RFID tags.

On the other hand, some claim that RFID tags are safe because tags would usually only contain and broadcast a unique id number and not personal information. This may sound harmless, but in reality, this could be similar to broadcasting a credit card or social security number. For example, giving away your credit card number to a stranger is generally not a good idea. It's not because the number itself has personal information in it, but it is what you can do with that number. If you have someone else's credit card number, you can find out where the owner lives, at the least, and maybe even make purchases with it. Similarly, the RFID tag may not contain personal or vital information, but this id can be linked to databases that give a detailed log of everything about the tag, such as everywhere it has been. Therefore, the claim that RFID tags are safe for the reason that they only store a unique identification number is more than optimistic.

Along with already mentioned negative effects that RFID technology can cause to society when not properly regulated, the technology itself has limitations. Some examples of these limitations are that tag reading can be restricted by the surroundings and materials near the equipment. Materials and objects are categorized by RF lucent and RF absorbent. A material is referred to as RF-opaque if it blocks or scatters RF waves. RF-lucent materials let the waves pass through without affecting them. Problems may arise in the supply chain if packaging is made of materials like metal foils, which are RF-opaque. (60 Lahiri) This could limit the areas of usage for the tags. It would be difficult to read tags that are placed in products that require

metal packaging. If RFID is going to be used more and more, then flaws like these need to be worked out along with the privacy invasion threats.

The idea of implementing RFID technology does not have to be discarded all together, but we do have to create certain restrictions and limitations of its use. I would like to propose certain guidelines that would help regulate the use of this technology that could otherwise be detrimental to society. If RFID tags are placed on products sold at stores, not only should the consumer deserve the right to be informed that the product contains the tag, but also the tag should be deactivated or removed at the point of sale. Like mentioned before, if tags are not removed from the product or packaging, they can stay attached until they reach the landfill. This needs to be prevented to ensure that product tracking will not take place in the consumers' possession outside of the supply chain. There is no reason for manufacturers to monitor people in this way to justify keeping the tag in the product after point of sale. Humanity has been able to make trades for thousands of years without gathering insurmountable private data about their customers. What's the need to do that now?

I also suggest that a tag reader must clearly inform all persons of a tag reading beforehand so that there is no secretive tag reading. For example, all tag readers placed at the entry and exit points of a store must clearly label what they are, what they are doing, and what the information is used for. Without this stipulation, stores can secretly read information without his/her consent; which could lead to spying on individual persons inside of a retail store.

As future uses of RFID technology are fought, the very same technology is in use today. Knowledge of the current technology is possibly the biggest reason new implementations of RFID systems are being opposed: because it is proven to work. Television and radio ads today are advertising for RFID in the form of chip implants for pets. A company by the name Home

Again ID sales RFID chip implants to veterinarians. These tags are implanted into pets to uniquely identify and track them. Over three million pets have been chipped with HomeAgain, and over 270,000 pets have been recovered. This is a perfect example of how powerful and useful this technology can be. At the same time, however, it also demonstrates its negative potential. If a dog can be located and tracked so easily as to recover a pet every 7 minutes (HomeAgain.com), imagine implanting RFID chips into humans. To prove that tracking humans through RFID has not only been thought of but also, IBM inventors filed a patent entitled “Identification and tracking of persons using RFID-Tagged Items.” – Patent Application #20020165758.

In conclusion, RFID technology can be useful for manufacturers, retailers, and even the consumers. But more importantly, we need to work out the problems before applying this technology everywhere in our lives. RFID could help businesses, but if they don’t make it seem like a good safe idea to the public, they could be making matters worse for themselves in the long run. The businesses are hiding these uses of the technology thus making the consumers skeptical. Instead, if the companies work out all of the privacy issues and have the consumers comfortable with the technology before implementing it, both consumers and manufacturers alike will benefit without the unfavorable effects to society.

Works Cited:

- Albrecht, Katherine and Liz McIntyre. Spychips. Nashville: Nelson Current, 2005.
- Lahiri, Sandip. RFID Sourcebook. New York: IBM Press, 2005.
- Balkovich, Edward et al. Do You Know If Your Boss Knows Where You Are? Pittsburgh, PA: RAND, 2005.
- “RFID Update – RFID Passport Controversy Heats Up.” April 1st, 2005. RFID Update. 21, 2005 <<http://www.rfidupdate.com/articles/index.php?id=839>>
- James, Louis. “Tech Central Station – Big Brother in Your Shopping Cart?” July 23, 2004. Tech Central Station. November 21, 2005 <<http://www.techcentralstation.com/072304B.html>>
- “RFID Position Statement”. 14 Nov. 2003. Spychips.com. 1 Dec. 2005. <http://www.spychips.com/jointrfid_position_paper.html>
- “EFF: Position Statement on the Use of RFID on Consumer Products”. 14 Nov. 2003. Electronic Frontier Foundation. 2 Dec. 2005. <http://www.eff.org/Privacy/Surveillance/RFID/rfid_position_statement.php>
- “The History of RFID”. RFID Journal. 3 Dec. 2005. <<http://www.rfidjournal.com/article/articleview/1338/1/129/>>
- “RFID”. Wikipedia.org 6 Dec. 2005<<http://en.wikipedia.org/wiki/Rfid>>
- “HomeAgainID.com”. 6 Dec. 2005. Home Again. 6 Dec. 2005. <<http://www.homeagainid.com>>
- “RFID: The Early Years”. 27 Sep. 2002. The Eagle’s Nest. 4 Dec. 2005. <<http://members.surfbest.net/eaglesnest/rfidhist.htm>>
- “Rfid Technology: What The Future Holds For Commerce, Security, And The Consumer” 14 July, 2004. < http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f:95455.pdf >