

Rohin Koshi &
Eian Vizzini
ecs188
12/9/2007

Privacy Concerns with RFID

Radio Frequency Identification (RFID) is a type of wireless identification system. The system consists of a low cost RFID reader and an ultra low cost tag which reports its identification or location data upon proper request from the reader. The tag consists of a digital memory chip, transponder, and antenna which are typically powered by the external RFID reader source without wires. These RFID tags that have no internal power source are the most inexpensive and are called "passive tags." The smallest tags range around 0.15mm x 0.15mm and are thinner than a sheet of paper. Typical read distances range from around 10 centimeters to tens of meters.¹ Passive tags currently cost around 5 cents per tag; the average price per passive tag is steadily declining.²

RFID has been used in tracking and access applications since the 1980s.³ They have been incorporated into products, animals, and even people for various purposes. The general uses of RFID have been organized into four main categories: EAS (Electronic Article Surveillance) systems, Portable Data Capture systems, Networked systems, and Positioning systems.⁴ They have been improving the efficiency of inventory tracking and management, passports, transportation payments, automobiles, beer-keg tracking, animal identification, libraries, and patient identification. With all of these uses, one should consider any possible downsides.

Consumer privacy experts and some politicians are debating over potential privacy abuses from the ever increasing use of RFID tags by major corporations such as Wal-Mart and METRO Future Store. There is currently no regulation of RFID technology protecting consumers from abuse of this technology. The only way for an average consumer to know if a product contains an RFID tag is to see the tag with their own eyes or a tiny ½ inch by ½ inch EPC label on a limited number of products. Unfortunately, manufacturers are getting very clever as to hiding tags in the products they produce. One such technique is to hide the RFID tags in between cardboard and paper layers. The government, along with major corporations, have the potential to track people's movements and purchases without our knowledge or consent.

Another type of consideration one may have when discussing the privacy abuses of RFID is that of lawfulness of actions involving RFID. Since privacy is such an important issue to people, certain measures have been taken in Congress to facilitate the right of privacy to people in our country (through tort law/the fourth amendment), which we will briefly analyze, after covering some virtues of privacy.

¹ Umeda, T.; Yoshida, H.; Sekine, S.; Fujita, Y.; Suzuki, T.; Otaka, S. *A 950-MHz rectifier circuit for sensor network tags with 10-m distance* Solid-State Circuits, IEEE Journal of Volume 41, Issue 1, Jan. 2006 Page(s): 35 - 41

² Hara, Yoshiko. *Hitachi advances paper-thin RFID chip*. EE Times.
<http://www.eetimes.com/news/design/showArticle.jhtml?articleID=179100286>

³ Carter, CMC. *RFID Credit Card Report*.
http://www.rfidbuzz.com/news/2006/rfid_credit_card_report.html

⁴ EPIC. *Radio Frequency Identification Systems Privacy Page*. <http://www.epic.org/privacy/rfid/> Updated Sept. 5, 2007

We value privacy for many reasons, but there are two main virtues that lend themselves well to the idea of privacy support. Security is one such reason, or virtue. What exactly is security?

“Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security.”⁵

We, as humans, instinctively dislike things like danger or loss, and therefore we greatly value safety. The RFID can make security breaches easier in multiple ways. First, RFID chips can be infected by viruses by hackers.⁶ Second, Gillette photographed images of people taking razors off the shelf of a store that contained RFID tags, using RFID tags as the basis for beginning photographs⁷, and this can be identified as a personal user security breach.

Another important virtue of privacy is anonymity. First, a definition:

“**Anonymity** is derived from the Greek word **ἄνωνυμία**, meaning "without a name" or "namelessness". In colloquial use, the term typically refers to a person, and often means that the personal identity, or personally identifiable information of that person is not known.”⁸

We seek to be nameless in our society. From watching others, it can be said that we don't generally want to have information about ourselves leaked to the public, but yet this is possible with RFID. One good example is the possibility of implementing the RFID in money (allowing money to be counted and deterring counterfeit behavior) at the cost of the anonymity we usually associate with cash.⁹ As an example, the information retrieved from RFID may contain data that is stored in a database and can be used to generate a set of statistics that could generically describe the actions of some individual.¹⁰

While these virtues give us motivation for thinking in the way of keeping our privacies, there is existing policy that offers some guarantee on our rights to privacy. There are general and specific right guarantees we have given to us by legislation. Starting with the most general, the Universal Declaration of Human Rights prescribes that no one should be subject to prejudicial interference with privacy, family, home or correspondence. It further states that everyone should be protected by law against such interferences.¹¹

In *United States v. Knotts*, 460 U.S. 276 (1983), it was determined that it was not a fourth amendment violation to track a person via a beeper placed in his/her car. On the

⁵ Public Domain Authors, *Security*. <http://en.wikipedia.org/wiki/Security>

⁶ Naraine, Ryan. *Dutch Researches create RFID Malware*. <http://www.eweek.com/article2/0,1895,1938391,00.asp>

⁷ Dickson, Ed. *Fraud, Phishing and Financial Misdeeds*. <http://fraudwar.blogspot.com/2005/10/rfid-abuse-in-private-sector.html>

⁸ Public Domain Authors, *Anonymity*. <http://en.wikipedia.org/wiki/Anonymity>

⁹ Granneman, Scott. *RFID Chips are Here*. <http://www.securityfocus.com/columnists/169>

¹⁰ Undisclosed Author, *First RFID Database*. <http://www.databasejournal.com/news/article.php/3351521>

¹¹ Universal Declaration of Human Rights, Article 12

flip side, the federal court has determined that tracking someone within their home is a violation of the Fourth Amendment. *United States v. Karo*, 468 U.S. 705 (1984).¹² From this we can deduce that the public and private system has a differing association with RFID prosecutions / law. In other recent cases, Wisconsin recently introduced a ban on forcible implantation of RFID.¹³ This shows the recent involvement by state governments to prevent the introduction of the RFID into the human culture.

Two corporations experimenting with RFID recently informed a U.S. House subcommittee that U.S. law enforcing privacy rules for RFID isn't necessary.¹⁴ While the culture of law is favored by the government, corporations don't really seem to be very interested in law restricting the use of the RFID (for the obvious reason that it will be beneficial for them).

Recently, in 2006, the Identity Information Protection Act of 2006 was passed by the California Senate. The law safeguards personal data. However, when sent to California governor Schwarzenegger, it was vetoed due to a similar interest with corporations that Schwarzenegger openly admitted. Despite this corporate mindset presented by our governor, we as citizens deserve to be protected from technological invasions of privacy posed by RFID.

The kind of information contained in an RFID tag is unlike that of a typical barcode currently used on almost all packaged products. As an example, a barcode of a specific product in New York is identical to that of the same product in California. With RFID, each tag contains unique dynamic information pertaining to that product such as: date of production, place of purchase, manufacturer information, and after-sale servicing history. This unique tag can be tied to the purchaser through a registration system such as the shopping card used at many grocery stores today. Once this tag is identified with its consumer, RFID readers have the capability to collect further data on the consumer such as date of purchase, frequency of shopping at a particular store, other purchases, shopping behavior, etc. The company then has the capability to tie this information to your name, phone number, email address, address, etc. and then sell this information to advertising companies or whoever would be interested or direct advertisements to you as you walk through their store.

Within the past year, payment card companies have been putting RFID tags inside the credit and debit cards they provide for their customers. There are now tens of millions of cards containing them in the US. With off-shelf-hardware and only modest technical skills, a card reader and cloning device can be constructed. This would be able to obtain information from the tags off credit cards such as: cardholder name, card number, expiration date, and type. After this information is recovered the device can then be used to carry out transactions just as the original card could.¹⁵

¹²Solove, Daniel. *The New RFID Chip*.

http://www.concurringopinions.com/archives/2007/02/the_new_rfid_ch.html

¹³ Songini, Mark. *Wisconsin Law Bars Forced Implants*.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111542>

¹⁴ Gross, Grant. *RFID Users Say No Privacy Law Needed*.

http://www.infoworld.com/article/04/07/14/HNrfidusers_1.html

¹⁵ Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu1, Ari

Juels, and Tom O'Hare. *RFID Payment Card Vulnerabilities*

Technical Report. http://www.nytimes.com/packages/pdf/business/20061023_CARD/techreport.pdf

While there are many possible risks to our privacy introduced by the RFID, consumers still have options to protect their privacy rights that are already in existence other than through use of legislation. One way to do so is to join the Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN), a group that has coined the term “spychips” in reference to RFID tags. CASPIAN is headed by RFID and Consumer Privacy Experts Katherine Albrecht and Liz McIntyre. They proposed federal legislation called the “RFID Right to Know Act of 2003” which mandated labeling of RFID-enabled products and consumer privacy protections.¹⁶ They state that the problem is that consumers currently have no way of knowing if these tags could be in your home. As we wait for the law to catch up with technology, CASPIAN as well as other organizations are testing and proposing methods consumers can currently use to yield immediate protection.

Several Engineers and Computer Scientists proposed what they called the “Smart Tag” approach to block tags for consumer privacy. These blocking tags act as a passive jammer that “simulates the full spectrum of possible serial numbers for tags, thereby obscuring the serial numbers of other tags.”¹⁷ This smart tag approach uses cryptographic methods that are challenging to design. The blocker tag is designed to simulate a full set of 2^k possible RFID tag serial numbers. When a reader queries tags in the vicinity of the blocker tag, the blocker tag outputs both a 0 and a 1 bit signal at the same time which may require 2 antennas. This requires the reader to recurse on all nodes and if the reader was given enough time and processing power it would output the entire 2^k spectrum of serial numbers. The designers of this blocker tag suggest that it can be made for as little as 10 cents. When carried by the consumer, a blocker tag induces a physical region of privacy radially about its position where an RFID reader would be incapable of singling out a tag. The downside to this blocker tag technology is its potential malicious use. If carried by a person with malicious intent, it could be used to disrupt business operations or to help penetrate petty theft by shielding merchandise from inventory control-mechanisms.¹⁷ These blocking tags would most likely cost about the same as a standard RFID tag of a few cents and hence provide an economical way of protecting your privacy.

The most straight-forward way to protect consumer privacy from RFID tags is called the “Kill Tag” approach. The idea is to kill the RFID tags before they are placed in the hands of consumers. RFID tags can be programmed so that if they receive a specific code they will essentially disable themselves from operating forever. Also, if an RFID tag is seen it can be disabled by disconnecting the antenna from its microchip using a knife or scissors. The chip is easy to spot as all the antenna’s wire’s converge to the chip’s location. A group of engineers designed and tested what they call an implementation of the “Clipped Tag.” This approach is a form of the Kill Tag approach in that the RFID tag’s functionality is limited at the time of purchase. In this case, the RFID tag is kept visible with perforations on either side of the microchip in order to allow the removal of the antenna after purchase. This group of engineers tested their design with Marnlen RfiD, a leading manufacturer of RFID labels, and it proved to

¹⁶ Davidson, Zoe. *RFID Right to Know Act of 2003*. <http://www.spychips.com/right-to-know-bill.html>

¹⁷ Juels, Ari; Rivest, Ronald; Szydlo, Michael. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*. <http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf>

significantly reduce the range from 10m to only 2cm¹⁸, thereby increasing the consumer's privacy. The tag isn't fully disabled in order it to be used later for returns, recalls, or recycling. This "Clipped Tag" approach could be a feasible compromise between manufacturers and consumers.

RFID may well have implications into several of our existing notions of privacy rights, based on the four main categories above that we use commonly today in tort law across many courtrooms in the nation. We see that the intrusion of solitude via electronic means is definitely occurring in this case. The public disclosure, false light claim, and appropriation of the users information can ALL stem from the initial extraction of the user's sensitive data. By better understanding the constitutional implications of privacy rights, we can hope to do what is best for our citizens and government while meeting the fine line between privacy rights and commercial necessity (to implement RFIDs for profit purposes).

Word Count: 2,083

¹⁸ Moskowitz, Paul A.; Lauris, Andris; Morris, Stephen S.; *A Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag*. Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on 19-23 March 2007 Page(s):348 - 351