RFID Tagging and Human Identification

Jeremy Kieser

University of Wisconsin - Eau Claire

September 18, 2010

RFID Tagging and Human Identification

As humanity develops new technological advances, we need to ensure that they are used appropriately and safely. Often we release a new technology into the world with a particular intent, but it ends up taking on a completely new function. Potential positive and negative purposes are unforeseeable and can quickly change the nature of young ideas. Nuclear energy was not fully understood before we were using it for weaponry and energy alike. Originally intended for merely sending electronic mail, the internet has now grown in functionality and cultural impact to rival any other invention in human history. The trends of the digital age have made privacy concerns an essential priority for people who have confidential information. Radio frequency identification (RFID) technology has been introduced to the market and has been integrated into many systems, but the full ramifications are still unknown. In this paper, I will discuss the history, usage, and ethics of RFID technology.

1. History

RFID transponders[1] (also known as tags) have only been in use for about 40 years, but the history that made the technology possible stretches back over 100 years. In the nineteenth century, physics pioneers Michael Faraday, James Maxwell, and Heinrich Hertz discovered the fundamental properties and functions of electromagnetic energy. This knowledge became the precursor of radio technology, which led to a revolution in communications around the world. As engineers began to develop radar technology in the 1920's, a primitive version of RFID under a different name made its initial appearance. During the Second World War, British air bases implemented Identification:

[1] Short for transmitter-responder.

Friend or Foe (IFF), which became the grandfather system for modern RFID. According to this method, a radio signal was sent out to aircraft approaching a base. If the crew responded with the correct key, the craft was "friendly." With this new technique, air bases could effectively and consistently identify whether an incoming plane was an ally or not; however, it was not until 1948 that the true work of RFID began.

Harry Stockman was one of many innovators who worked on early RFID technology. His paper, "Communication by Means of Reflected Power," outlined the core of its theory and implementation. The foundation was set, but it would take another 30 years before his ideas would be developed into more practical applications. Modern innovations, such as the transistor, the integrated circuit, the microprocessor, and the development of communication networks necessary for RFID had not been invented yet, and so it would have to wait (Landt 2001).

The 1960's saw the initial boom of RFID as the tags became commercially widespread. The first tags were only one bit in capacity and could only have their presence detected, but they were the first examples of Electronic Article Surveillance[2] (EAS), which still proves useful even today. In the 1970's tags were developed and used for animal identification. Over the next decade, RFID usage spread worldwide as many countries adopted the new technology. The greatest uses in the US were for tracking inventory while shipping, personnel access, and to a lesser extent, for livestock inventory. Short-range systems for locating animals and collecting fees on toll roads were the greatest uses in European countries. The 1990's saw the worldwide implementation of RFID in electronic toll road collection (Landt 2001).

[2] Electronic article surveillance (EAS) is a technological method for preventing theft from retail stores or libraries.

2. Current Technology

Current RFID transponders are comprised of two parts: an antenna and an integrated circuit to store information on the tag. Tags can be further categorized into passive and active. Passive tags are not powered independently, but are “awakened” by incoming radio waves. An incoming electromagnetic wave induces a small current in the tag’s antenna, powering its circuit. The most common responding method is backscatter, which is a reflection of the initial signal that results in a weaker, modulated response signal. This type of tag generally has a storage capacity of up to 1KB, enough for about 1000 ASCII characters or 500 Unicode characters and has a read range of about 1 meter ("Radio-frequency identification"). In contrast, active tags have their own power source and transmit their own signal upon activation. These types of tags have the advantages of longer read ranges (8 to 10 meters) and have a higher bandwidth for transfer; however, they do have the disadvantage of requiring larger containers and a power source (often batteries), thus resulting in greater cost ("The History of RFID Technology - RFID Journal."). There is also a third, less common type called semi-passive, which relies on an external signal for communication, but utilizes a battery for circuitry functions.

Tags range in size anywhere from a few millimeters to several centimeters wide. Generally, passive tags are smaller than their active counterparts since they require no power source. The world’s smallest tags have been reduced in size to a mere .05 mm x .05 mm (Sankei 2007). They have been aptly dubbed “powder” tags and have the potential to be inserted into currency to deter counterfeiting. However, attaching tags to products is meaningless unless there is a device to identify them. Such “readers” can be handheld or stationary and are obtained readily with a simple internet search. This detail creates other potential problems that will be discussed in the chip security section. The frequency of the signal sent out by the reader often depends on the application of the tag. For example, 125 KHz, 915 MHz, and 433 MHz or 2.45 GHz frequencies are used for animal identification, inventory control, and active tags in highway toll road collection respectively (Heurich).

3. Current Applications

Current applications of RFID vary widely and are expanding. One of the most common uses is inventory management. The old method of assigning each product a UPC barcode does not allow for physical tracking of each individual item. The RFID version of the UPC, referred to as the electronic product code (EPC), has this capability. Distributers can tag items and have them monitored at various points along their route to ensure prompt and reliable delivery. Retail stores use the technology for security as well as for inventory purposes. Electronic readers are stationed at the exits of stores, which read any passing chip on any tagged item that goes through them. If the tag has been deactivated in the system by an additional reader at the cash register, the alarm does not sound. However, if the tag has not been marked as purchased, the system sounds an alarm to indicate that a potentially unpaid item is leaving the store.

The European Union has also implemented tags in euro notes higher than 20€ to deter counterfeiters (Albrecht). By tracking the flow of currency, governments have not only made it harder to launder money, but have also removed anonymity from cash transactions. Opponents of the new anti-counterfeit system have resorted to microwaving their bills in an effort to retain privacy. The technology has also found a place in cross-country races. Competitors wear the tags, which pass through readers at measured distances along the race and at the finish line. This type of timing allows for greater precision for interval and final times. The automotive industry has been using tags for quite a while as well. Frequent toll-road drivers now have the option of paying tolls electronically by mounting a tag in their cars, which is read as they pass through checkpoints along a toll road. iPass subscribers in Illinois have been using this system for more than ten years and number in the millions. In 2005 E-ZPass, a similar toll collection system in Maryland and Virginia, became compatible with the Illinois system ("Radio-frequency identification"). Mass transit authorities around the globe are also taking advantage of this convenience. New York, London, Amsterdam, and countless other cities are adding tags to tickets to speed paying for and using services.

RFID is only one among many ways to use electromagnetic waves as a means of communication. Bluetooth, wireless internet (Wi-Fi), GPS, and cellular phones also employ this technology, but the distinguishing lines between each application are not always clear. For years, parole officers have used tracking ankle bracelets to monitor individuals under house arrest. These devices send a radio frequency signal to a receiver in the house. One might consider this an example of RFID, but it is not, as the tracking device is the initiator and is often used in conjunction with GPS signals. Other examples, such as animal migration and population tracking, are not as easily placed into one category. A good rule of thumb to help determine which category a technology best falls under is whether it sends signals independently. If it does, it is most likely not RFID and is one or a combination of other communication methods.

4. Human Implantation

RFID implants have been used subdermally in animals and, more recently, in humans. Concerned pet owners have been using the technology since the early 90’s; however, the extension of implants to humans has not occurred without controversy. Professor Kevin Warwick of the University of Reading (UK) became the first human to host an RFID tag in his body ("Scientists test first human cyborg"). The test lasted only nine days, but he managed to control various electronic devices in his workplace, including the lights, doors, and his computer. There were many individuals who questioned his motives, however, and even some who dismissed it as merely a publicity stunt. Six years later, VeriChip, a large RFID marketer, was granted approval by the Food and Drug Administration to use its device (a subdermal RFID tag) in humans; however, this action created several controversies. Placement of the device is simple and relatively safe: a rice-sized capsule is inserted through a tiny needle under the skin, often in the hand or the arm. Having access to the information contained within the chip is controversial because it raises concerns about medical privacy. Proponents of the device often point out the advantage of storing vital medical information for use when a patient is unconscious or otherwise unable to give information. Users of the device would be able to link the tags to a security network, allowing personnel to access secure facilities. The potential risks of using the device can be seen in the following letter from the FDA to Digital Angel Corporation (parent company of VeriChip):

> The potential risks to health associated with the device are: adverse tissue reaction; migration of implanted transponder; compromised information security; failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick. The special controls

> document aids in mitigating the risks by identifying performance and safety testing, and appropriate labeling.
>
> ...
>
> As a result of this order, you may immediately market this device, subject to the general control provisions of the Act and the special controls identified in this order. (Tillman 2004)

One criticism of this excerpt from the FDA letter is that it merely lists the risks without ranking the dangers or citing their respective occurrence rates. Adverse effects that are rare or relatively benign, such as migration of the transponder, are listed with others that may be harmful or life-changing (for example, compromised information security).

5. Security Measures

Historically, implementing digital security measures has been an ongoing battle between those who encrypt sensitive or vital information and those who attempt to decrypt it. For every security measure installed, there seems to be a calculated effort to crack it. A simple Google search for RFID hacks will yield thousands of pages on how to perform legally gray actions. Most tags do not have any encryption methods at all, so that the only deterrent to possible criminal activity is lack of physical proximity to the tags. Even tags with sensitive or private information, like the medical information on those distributed by VeriChip, have no security measures to secure the stored 16-digit identification (ID) number. The American Medical Association has recognized this problem, declaring that only ID numbers linked to secure data bases be stored and that "physicians should support research into the safety, efficacy, and potential non-medical uses of RFID devices in human beings" (Sade).

Biometric passports are among one of the few devices that actually utilize some encryption, but it is still not effective. In 2006, an employee of DN-Systems, an international consulting firm in the field of information security, was able to write software to successfully read and copy biometric information on a British passport to a faked passport (Sterling 2006). The data transmission between the chip and reader uses military grade encryption, but the fatal mistake here was using non-secret information that was human readable in the passport to create a secret key. This was none other than the passport number, date of birth and expiration date. A hacker who gained access to this information, for example, by shoulder surfing, would be able not only to reproduce it, but also to edit it. In defense of the system, the Home Office (the UK equivalent to Homeland Security) said, "By the time you have accessed the information on the chip, you have already seen it on the passport" (Sterling 2006). However, this greatly underestimates the danger of tag cloning. Sterling compares this to "installing a solid steel front door to your house and then putting the key under the mat." With the electronic version of a passport, one could forge a copy of it and travel under the identity of another person.

Another danger is posed by EPC (electronic product code) clouds. Such clouds do not yet exist but by reading all the tags on persons entering and leaving the store, a store owner or a store manager could determine their customers' purchasing habits. Even without a name, they would still be able to create profiles that could identify individuals coming into and going out of their stores. These profiles, dubbed "EPC clouds" would have the capacity to update a database as new characteristics are added to or dropped from the reference set (Hansen 2009). EPC cloud tracking also would have the capacity to monitor transactions that take place outside a store. If a unique EPC is tied to a particular cloud, but is identified in another one, it is probable that some type of interaction has occurred. Analyzing many instances of exchanges would create social network patterns that represent families, schools, and workplaces. These kinds of data could add further to the ever-increasing demand for data mining. Business retailers, even relatively small ones, would have the capacity to gain access to consumers' purchasing information. Adding encryption techniques to already deployed tags is not a viable option for protection either since the memory capacity of such inexpensive tags is so low that installing security measures that would actually fit could be broken easily by brute force attack. Tags that are fitted with encryption techniques often cost about $5 each, which may not be cost-effective for products where the company cannot afford to pass on the expense to the consumer ("Radio-frequency identification"). However, the infrastructure necessary to track enough data points and interactions to make the system functional and meaningful is distant at best.

6. Ethics of Human Implantation

With RFID technology defined, we can look at the ethical implications of human identification. One common justification is that it would ensure that people's medical information would be available to medical personnel quickly and reliably, particularly in emergency situations. Often when people are being rushed to the ER, they cannot recall vital information about their medical history, medications, allergies, or even basic hereditary conditions. However, the benefits of this technology are greatly outweighed by the weaknesses. Ensuring the accuracy of medical records once a patient is in the hospital is difficult. Current systems are not seamless and incorrect data often leads to delays in reaching a diagnosis or medical errors, an occurrence that can be fatal if overlooked. Having control over who has access to one's personal information is becoming more difficult in this digital age. The standards for how long information should be held, who has access to it, and what type of information should be kept vary widely.

Another possible negative aspect of RFID lies within tagged currency. The possibility of privacy loss due to tracked bills has not been fully assessed and depends on whether countries continue to implement the tags.

Using an act utilitarian perspective, one must weigh the net effect for all parties involved. Were RFID technology to be implemented as is, the beneficial effects would include ease of tracking for corporations, increased security for retailers, and safety for those who might need emergency medical treatment. The RFID Research Center at the University of Arkansas found that “RFID-enabled stores were 63% more effective in replenishing out-of-stocks than the control stores” (Kuchinskas 2005). However, the negative aspects are more difficult to quantify. Clandestine monitoring of individuals and the marketing of that information could have a wide range of results, varying from minor inconveniences due to unwanted advertisements to loss of life due to a contract killer purchasing location data. Adopting a rule utilitarian perspective, one must reflect on what potential universal rule is being considered. In this case, the rule is that companies should be optimizing efficiency, regardless of whether it is safe for all intended users. If this rule were generalized, consumers would have no protection against fraudulent corporations. Clearly, universalizing this rule would not produce the greatest happiness. Therefore, the act is wrong. Taking a Kantian viewpoint, one must consider the motives behind the action, not considering the result. In order to increase effectiveness and security, people who install the tags disregard the possibility that the end user’s privacy may not be fully secure. Hence, they treat others as a means to an end, and so the action is wrong.

I agree that releasing a product that is not fully secure is wrong; nevertheless, I predict that, while the capability will exist for mass-produced, encrypted tags in five years or less, the change in infrastructure to accommodate these new tags will only come with an exposure of large numbers of people to theft or breach of privacy. The general public is usually satisfied with current innovations and their security until it is discovered that they are grossly ineffective. Therefore, the responsibility for arousing public awareness of RFID inadequacy falls to those who create the tags and to those in the field of information security. RFID producers should be required to inform potential clients explicitly about the level of security of their product. Consumers could then make an informed decision whether to utilize the product. It should be mentioned that there are other technologies in widespread use that have similar or worse security (e.g., Bluetooth, smart phones) that have not spawned distrust in electronic devices. It is probable that RFID will find a similar acceptance in our technology usage. Its use in business applications is most likely to remain innocuous and produce no harm. The idea of an EPC cloud tracking the habits of consumers is implausible at best and would require an infrastructure change to facilitate it. This does not remove the burden of vigilance from the public, as they must also keep the dangers in check by staying informed about them.

Appendix A: Comparison of RFID and Other Wireless Communication Methods

	GPS	Cellular Signal	WiFi
Cost ($ per unit)	60+	20+	9
Range (m)	20,000,000	3000	32-95
Data transfer Speed	40 kb	Up to 9.6kbps (2G) Up to 384kbps (3G)	54 Mbps
Freq Range	1.57542 GHz, 1.2276 GHz	824-849, 869-894, 896-901, 935-940	2.4 GHz
	Bluetooth	RFID	
Cost ($ per unit)	3	.05 - .25 (passive) up to 5	
Range (m)	10-100	2 (passive) 30-100 (active)	
Data transfer Speed	3Mbps	8 kbps (passive) up to 3Mbps (active)	
Freq Range	2.402-2.480 GHz	(LF: 125–134.2 kHz and 140–148.5 kHz) (HF: 13.56 MHz)	

Table compiled with information from Foley, Michael.

Works Cited

Albrecht, Katherine. "Auto-ID: The worst thing that ever happened to consumer privacy." *CASPIAN - Consumers Against Supermarket Privacy Invasion and*. Web. 12 Nov. 2009. <http://www.nocards.org/AutoID/overview.shtml>.

Data Privacy and Integrity Advisory Committee. Rep. no. 2006-02. Department of Homeland Security. Web. 12 Nov. 2009.

Foley, Michael. "Compare with Other Technologies." The Official Bluetooth® Technology Info Site. Bluetooth.com. Web. 15 Sept. 2010. <http://www.bluetooth.com/English/Technology/Works/Pages/Compare.aspx>.

Hansen, Markus, and Sebastian Meissner. "Identification and Tracking of Individuals and Social Networks using the EPC on RFID Tags." N. pag. *IEEE Xplore*. Web. 1 Nov. 2009.

Hayles, N. Katherine. "RFID: Human Agency and Meaning in Information-Intensive Environments." *Theory, Culture & Society* 26.2 (2009): 47-72. Print.

Heurich, James. "RFID, Inc. Radio Frequency Identification Products." *RFID, Inc. Radio Frequency Identification Products....!* Web. 09 Dec. 2009. <http://www.rfidinc.com/tutorial.html>.

Kuchinskas, Susan. "Study Sees RFID Savings For Wal-Mart." *InternetNews Realtime News for IT Managers*. 19 Oct. 2005. Web. 10 Dec. 2009. <http://www.internetnews.com/wireless/article.php/3557356>.

Landt, Jeremy. "Shrouds of Time: The history of RFID." *Association for Automatic Identification and Mobility* (2001): 3-7. Rpt. in Print. Print.

"Radio-frequency identification" *Wikipedia, the free encyclopedia*. Web. 12 Nov. 2009. <http://en.wikipedia.org/wiki/Radio-frequency_identification>.

Sade, Robert M. *Radio Frequency ID Devices in Humans*. Rep. no. 5-A-07. Print.

Sankei, Fuji. "Hitachi develops RFID powder :::." *Pink Tentacle*. 14 Feb. 2007. Web. 09 Dec. 2009. <http://pinktentacle.com/2007/02/hitachi-develops-rfid-powder/>.

"Scientists test first human cyborg." *CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News*. 22 Mar. 2002. Web. 10 Dec. 2009. <http://archives.cnn.com/2002/TECH/science/03/22/human.cyborg/>.

Sieberg, Daniel. "Is RFID tracking you?" *CNN.com - Breaking News*. Web. 12 Nov. 2009. <http://www.cnn.com/2006/TECH/07/10/rfid/index.html>.

Smith, Joshua, and Kenneth Fishkin. "RFID-BASED TECHNIQUES FOR HUMAN-ACTIVITY DETECTION." *COMMUNICATIONS OF THE ACM* 48.9 (2005): 39-44. Print.

Sterling, Bruce. "Arphid Watch: Find Own Foot, Aim Hastily, Pull Trigger | Beyond The Beyond." *Wired News*. 17 Nov. 2006. Web. 12 Nov. 2009. <http://www.wired.com/beyond_the_beyond/2006/11/arphid_watch_fi/>.

"The History of RFID Technology - RFID Journal." *RFID Journal - Technology News & Features*. Web. 12 Nov. 2009. <http://www.rfidjournal.com/article/articleview/1338/1/129/>.

Tillman, Donna-Bea. "Food and Drug Administration: Evaluation of Automatic Class III Designation." Letter to James Santelli, Vice President of Digital Angel Corporation. 12 Oct. 2004. MS. Rockville, MD.