

RFID and Consumer Tracking

Sam Napp, Anthony Chiulli, John Bialk

“We don’t regard ourselves as ‘Big Brother’. We’re more like a friendly uncle or aunt watching over you.”¹²

Introduction

In recent years, the demand for Radio Frequency Identification (RFID) technology has skyrocketed. Since 2005 the demand for RFID chips has outstripped manufacturer’s ability to produce them. This excess demand can be attributed to the cost savings and productivity benefits associated with RFID. Wal-Mart alone expects to save \$407 million annually with pallet-level tagging and would likely see that amount increase to \$7.6 billion annually by putting an RFID tag in every item.¹³ RFID’s ability to manage the supply chain, reduce theft and streamline the checkout process is unprecedented. Retailers want this technology now and most experts believe that it will be pervasive within a decade.

Oppositely, consumers have approached this new technology timidly. Aside from the promises of increased efficiency and productivity there are some real dangers lurking within RFID technology. RFID chips are small, unobtrusive and can be read from distance.¹³ There is no real way for a consumer to know if they purchase a product equipped with a RFID tag. Consumers fear that they may end up walking around carrying computer chips that stealthily track their movements and spending habits.

Further complicating the matter is the adoption of the Electronic Product Code (EPC). This is a standardized numerical sequence that will allow all readers to identify the product being scanned. Not only does this code identify the manufacturing company and product type, but also the 96-bit code is long enough to uniquely identify every product ever made.¹³ Combine this with the prevalence of RFID readers in the retail market and the suggestion of RFID readers in traffic lights and we have an environment that is ideal for tracking citizens.

Tracking Issues Raised by RFID

When privacy advocates discuss RFID, they frequently focus on consumer privacy. They are concerned that RFID technology will allow stores to collect information on consumer shopping habits and use this information to create consumer profiles and influence purchasing decisions. This is a real and valid concern, but it is not the only issue associated with RFID technology. An equally important and often overlooked point is the impact of RFID on location privacy. Fundamentally, RFID tags are a tracking technology and they are equally effective at tracking supply shipments and consumers wearing RFID enabled products. In order to highlight the dangers of RFID enabled tracking this paper will present the abuses of suppositional data tracking and skimming. We contend that these physical tracking techniques lead to injustice and are fundamentally immoral.

Items such as shoes or ID cards equipped with RFID, (As of 2005, the United States has been issuing passports which contain an RFID chip and there is serious talk of putting RFID chips into drivers licenses)¹³ which are likely to be carried at all times, are ideal candidates for physically tracking a person. Whenever a person crosses a RFID scanner their shoes or ID card would register. Thus making it a simple task to build detailed records of where a person has been, what time it was, what items they were carrying, and who they were with.

Suppositional data tracking uses databases to compile this information and analyze it to infer things about the person being tracked. Data trackers may seek to determine what physical afflictions a person has (based on what they were carrying, where they were shopping, or how long it took them to get around) or any love affairs they might be involved in (based on who they were with, where they went, and what time it was). This information could then be used against a person's will for determining insurance premiums or for fringe behavior such as blackmail and stalking.

The most frightening aspect of this "tracking" is that it is all supposition. RFID provides no proof of a person's actions, only hints and small pieces of data, which must be interpreted by imperfect humans. This lack of perfection allows for mistakes. Yet the person who is being monitored has no ability to view or modify the information that is collected, thus compromising the individual's ability to shape their own identity, as well as intruding on their privacy. Imagine being framed for murder simply because your shoes and wallet were out of your site for a night and you have no alibi because you were alone and asleep. A frightening thought.

Another disturbing scenario involving RFID tracking is skimming. Skimming is defined as reading RFID chips without the knowledge of the holder.¹³ By implementing RFID chips in passports and national ID cards it would be a simple task for kidnappers, pickpockets and terrorists to determine the nationality of a person traveling abroad. In a busy marketplace, it would not be difficult to bring a hidden reader within the necessary read range of the RFID chips. Once a person's identity has been established, his or her value as a target can more easily be established.¹³ In this way RFID enabled passports are actually increasing the likelihood of foul play while abroad.

A similar and equally disturbing scenario could occur within the United States. Imagine that businesses or government officials were to "skim" the attendees of a religious ceremony or political rally. These attendees might find themselves added to terrorist watch lists simply for exercising their first amendment rights. Skimming also expands the likelihood of prejudice and bias. It might turn out that an employee attends a rally which is in opposition to views held by his boss. Based on information provided by skimming the crowd the boss may decide to punish the employee by denying them promotions or simply firing them.¹³

Both suppositional data gathering and skimming are behaviors that seem creepy and even potentially dangerous. As alluded to earlier, these behaviors come about by knowing the location and identity of a person. We contend that even though the person being tracked is in a public space they have an expectation of location privacy. We will argue this case using the Subjective Freedom Argument and the Social Contract Theory. Through these arguments we will seek to demonstrate that suppositional data gathering and skimming are morally wrong and ethically corrupt.

Subjective Freedom Argument

One way to think about the conflict between RFID technology and freedom is to imagine that RFID will enable the monitoring of all citizens in public settings such that one will never, or will rarely, be able to escape being tracked. This is the "Friendly Aunt or Uncle" scenario in which RFID readers are stationed at every intersection and linked through a central computer system. In this scenario the government would be able to monitor individuals and recreate their actions in such a way as to make laws fully enforceable. Laws that are fully, or nearly fully enforceable would result in an eclipse of a person's freedom because they are denied the ability to make autonomous decisions, that are themselves ways of generating morality.¹²

This view is called the Subjective Freedom Argument and finds its foundation in Kant. According to him there are two kinds of laws: Heteronomous Law (law as it is enforced from the outside) and Autonomous Law (law as one arrives at it, self-law).¹² According to Kant, when one follows Heteronomous Law they are acting according to duty because the law is imposed from the outside. Oppositely, when one follows Autonomous Law they are acting by appeal to the categorical imperative and thus their actions are contributing to the creation of a moral system.¹² Thus, the subjective agency is not the passive experience of being bumped around by rules and laws, but rather an agent's active participation in the determination of ends and means to those ends.¹²

As an example of this lets imagine a man, Mr. A, who is considering having an affair. In the world described above the laws are highly enforceable and there is a strong likelihood that Mr. A will be caught. In this scenario Mr. A no longer asks himself whether it is ethical that he cheat on his wife, but rather he asks himself whether cheating on his wife is worth the penalty that he will surely incur.¹² In this world, operationalism acts in place of ethical deliberation and a person's freedom to act according to the categorical imperative is impaired. Mr. A's ability to participate ethical deliberation has been truncated because he is not free to consider both courses of action. In this world individuals are not free to entertain the possibility of acting wrongly and thus they cannot seriously ask the critical question of whether a particular action complies with their autonomous law.¹² Thus to return to Mr. A he would be denied the ability to reach a decision on whether or not infidelity is morally wrong and thus he would be disallowed from following his own autonomous law.

Thus based on the argument above we contend that it is necessary to allow individuals some privacy of location, even when in the public sphere, because failure to do so denies citizens the ability to follow the categorical imperative.¹² According to Kant not following the categorical imperative is the definition of immoral.¹² To return to RFID we see that it is RFID's ability to pinpoint an individual's location and recreate their actions that prevents individual from considering improper actions or acting wrongly. Thus, we as users have a duty to protect and value our location privacy.

Social Contract Argument

The Social Contract Theory supposes that a moral system comes into being by virtue of contractual agreements between individuals. Morality in this theory is based on the assumption that rational people will only agree to accept social contracts that are for their mutual benefit and on the condition that others follow the same set of rules.¹⁴

When a person walks into a store they have numerous social contracts with the storeowner. Some examples of these social contracts are customers are allowed to enter the store and purchase goods, but are expected to tender legal currency and refrain from stealing. Some important contracts that relate to RFID are customers have a right to know what information is being collected about them, have the ability to prevent or object to data collection, and storeowners have a right to know about transactions that have taken place in their establishment.¹⁵

When a storeowner collects data from RFID tags on products at the point of sale, he is not breaking any agreements.¹⁵ At this point the storeowner and customer have equal rights to information about the transaction. However, if a storeowner or other user collects data from other store's RFID tags or RFID tags on products from previous transactions, they are breaking a social contract. In this situation the storeowner is violating the social contract because the customer has been forced into a contract that is not mutually beneficial. Currently, there is no law that requires retailers to notify consumers when RFID tags are being used or read. Thus it is likely that consumers are unaware they are being tracked and the customer's right to object to data collection has been violated. In this scenario the storeowner is setting up new contracts that are not mutually beneficial and thus immoral.

Protecting Privacy

The location based privacy threat occurs when RFID tags remain active once a consumer leaves a store. Now imagine millions of RFID readers strategically placed in airports, bus stations, subways, and highways. It is this long-term tracking and monitoring ability that poses a significant threat to individual privacy. As the technology of RFID continues to permeate our society, legislators and consumer advocacy groups are demanding options for consumers and guidelines for retailers to protect personal privacy. Simply these options can be boiled down into three fundamental solutions: tag killing, tag blocking and increased legislation.

Tag Killing

One method to protect consumers from RFID tracking is tag killing. In this scenario RFID tags have a built-in “kill command” which disables the functionality of the tag after consumers purchase a product.¹⁵ Tag killing allows for a high degree of consumer privacy protection at negligible cost. However, there are some concerns with this solution. One is that retail stores would set up killer kiosks, in which it is the consumer’s responsibility to “opt in” to the kill program.

This scenario has a number of potential drawbacks. First the disabling process is performed manually by millions of individual consumers, leaving human error as an ever-present possibility.¹⁶ Another draw back is that there may only be a limited number of these killer kiosks in stores, leading to lines and preventing consumers from killing tags due to the inconvenience. Related to this point is the idea that retailers may give consumers incentives not to kill the tags. An example of these incentives could be loyalty discounts given when a consumer returns to the store with five of the retailer’s active tags.¹⁶ The final concern with the tag killing solution is that tags could be killed in a temporary manor by using a software lock. If this were the case there would be nothing to prevent stores from “waking up” tags and using these resurrected tags to track consumers.

Blocker Tag

Another method citizens can utilize to protect themselves from location privacy is using blocker tags. A blocker tag is a jamming mechanism that fools RFID readers upon scanning. When carried by a consumer, blocker tags impair RFID readers by simulating many ordinary RFID tags simultaneously.¹⁷ Blocker tags can also block selectively by simulating only designated ID codes, such as those issued by a particular manufacturer. Although the blocker tag is implemented cheaply (requiring no alterations to the tag), the extent to which user privacy is protected is limited.¹⁷ Consumers cannot confirm the blocker tags are actually working and thus cannot conclude their privacy is being protected. Another reason their protection is limited is it puts the burden on consumers to purchase blocker tags, and carry them on their persons at all times. Consumers might thus be uneasy about the privacy protection afforded to their data.

Legislation

Currently, there is no law requiring a label on products to indicate that an RFID chip is inside.¹⁸ Nor is there any federal or state laws that specifically prohibit or restrict the use of RFID.¹⁸ Even though U.S. citizens have an inferred right to privacy through the Bill of Rights, they are still unprotected from RFID tracking. Current legal doctrine, as decided by the Supreme Court, holds that there is little or no expectation of privacy in public places.¹⁹ Thus as the law currently stands, anytime a person leaves home they enter the public sphere. While in the public sphere it is legally acceptable for government and business to obtain and document information on the individual. Due to the fact that the majority of information gathering, including RFID tracking, is done in the public sphere, citizens do not receive any protection from these new technologies.

This lack of protection needs to be remedied. With the rapid increase in technology it is time for the courts to re-examine some of their previous interpretations. One piece of legislation which could be relevant to RFID technology is the *Electronic Communications Privacy Act* of 1986.¹⁹ This law prohibits the interception of information communicated by electronic means. According to the U.S. Code, electronic communications "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."¹⁹ In the future, this law could easily be re-interpreted in such a way that data collection via another company's RFID chips is illegal.

The issue of RFID technology is too substantial for reinterpretation alone. In order to effectively govern this technology we must begin drafting new laws. Even now Congress is answering this challenge by formulating new RFID legislation. On February 23, 2007 the Washington State House Committee on Technology, Energy & Communications, passed House Bill 1031 and sent it to the Rules Committee for a second hearing.²⁰ This is important because House Bill 1031:

Requires that a person selling or issuing an electronic communication device that has not been disabled, deactivated, or removed at the point of sale or issuance, provide notice to the consumer and label the device.

Requires that a person selling or issuing an electronic communication device must use industry accepted best standards to secure the device.

Prohibits a person from remotely scanning or reading an electronic communication device to identify a consumer without obtaining consent from the consumer and creates civil penalties.²⁰

If this bill becomes law, then it would be a major victory for personal privacy and a step towards responsible governance of RFID technology. Still, this law is not a Federal law and there is a great deal of work left to be done to ensure RFID does not intrude on the privacy of United States citizens.

Conclusion

This paper does not seek to condemn RFID technology nor prevent its acceptance into society. RFID's ability to monitor the supply chain and enhance industry performance with fast and accurate product data is unrivaled. However, when left uncontrolled this technology can be used to track individuals and compromise their privacy of location. Therefore, we conclude that RFID technology must be regulated with federally mandated laws that follow a RFID Bill of Rights and set standards for retailers.

Due to the novelty of RFID, current legislation does not effectively protect personal privacy. One solution is to create a new set of laws that follow the spirit of Garfinkle's RFID Bill of Rights.²¹ This Bill of Rights purposes that consumers have:

- The right to know if a product contains an RFID tag.
- The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
- The right to use RFID enabled services without RFID tags.
- The right to access a RFID tag's stored data.
- The right to know when, where and why an RFID tag is being read.²¹

House Bill 1031 was based on many of these principles, but does not go far enough to fully protect citizens. In the future, federally mandated laws must adhere to these principles in order to ensure that individuals are able to control their exposure to RFID tracking and protect their privacy.

Further, future laws should place the responsibility on retailers to protect citizens. Consumers should have access to protective technology, such as blocker tags, but it should not be their only line of defense. By placing primary responsibility with retailers, we ensure that all

citizens are protected and those who are concerned have access to multiple layers of protection. Proposed requirements for retailers include placing RFID tags on products in a visible and easily removable fashion, providing free tag killing services during checkout, and making RFID readers highly visible to citizens.²¹ These simple requirements are a minor inconvenience to retailers and will dramatically increase citizen's privacy and comfort with RFID.

It is up to us, as U.S. citizens, to control technology and blend it into our lives in a way that doesn't diminish our quality of life. As Thomas Jefferson said,

*"Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with the change of circumstance, institutions must advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy as civilized society to remain ever under the regimen of their barbarous ancestors."*²²

With RFID technology the human mind has again made a discovery that eclipses the reach of society's laws and institutions. It is now our duty to create new laws that set standards for retailers and provide citizen's with the protection of a RFID Bill of Rights. By doing this we will clothe our new society in a suit of laws that is well tailored to our technological progress.

Works Cited

- [1] "RFID Journal Frequently Asked Question." RFID Journal the World's RFID Authority. 2007. 28 Feb. 2007 Available at: <http://www.rfidjournal.com/faq>>.
- [2] H. T. Tavani, Ethics & Technology, 2nd ed. , Hoboken, New Jersey: John Wiley & Sons, Inc., 2007
- [3] Albrecht, Katherine. "RFID: Tracking Everything, Everywhere." C.a.S.P.I.a.N. 11 Aug. 2003. C.A.S.P.I.A.N. 10 Apr. 2007 Available at: <http://www.nocards.org/AutoID/overview.shtml>>.
- [4] "Metro Group Future Store Initiative." METRO Group. 20 Nov. 2006. 28 Feb. 2007 Available at: http://www.future-store.org/servlet/PB/menu/1007055_12/1134638479848.html
- [5] M. H. Bosworth, "Loyalty Cards: Reward or Threat?" [Online Document] July 11th, 2005. [March 25, 2007] Available at: http://www.consumeraffairs.com/news04/2005/loyalty_cards.html
- [6] "Grocery Store Loyalty Card Use is Strong Despite Privacy Concerns." [Online Document] December 28th, 2004. [March 26, 2007] Available at: <http://www.rfidnews.org/news/2004/12/28/grocery-store-loyalty-card-use-is-strong-despite-privacy-concerns/>
- [7] "RFID and Consumers: Understanding Their Mindset." Capgemini. 12 Jan. 2007. Capgemini; consulting, technology, outsourcing. 10 Apr. 2007 Available at: <http://www.us.capgemini.com>
- [8] C. Cobbs, "Data-Hungry Retailers Snoop Like Spies." RedOrbit. 30 May 2006. 2 Apr. 2007 Available at: http://www.redorbit.com/news/technology/519528/datahungry_retailers_snoop_like_spies/index.html?source=r_technology
- [9] J. McQuivey, "RFID and Consumer Demand." RFID Journal. 2 Apr. 2007 Available at: <http://www.rfidjournal.com/article/articleview/1097/1/82/>
- [10] D. Levy, "A Vision for RFID in-Store Consumer Observational Research." RFID News and RFID Operations. 20 Oct. 2003. 2 Apr. 2007 Available at: <http://www.rfidnews.org/weblog/2003/10/20/sponsored-feature-a-vision-for-rfid-instore-consumer-observational-research/>.
- [11] B. Givens, "Implementing RFID Responsibly." Privacy Rights. 21 Jan. 2004. 2 Apr. 2007 Available at: <http://www.privacyrights.org/ar/FTC-RFIDTestimony.htm>
- [12] Hale, "Identity Crisis: Face Recognition Technology and Freedom of the Will." Ethics Place & Environment 8.2 (2005): 141-158.
- [13] V. Lockton, and R. Rosenberg, "RFID: The Next Serious Threat to Privacy." Ethics and Information Technology 7 2005: 221-231.
- [14] H. Tavani, Ethics and Technology. New York: John Wiley& Sons Inc, 2007. 137

- [15] B. Keifenheim, "An Ethical Evaluation of Radio Frequency Identification" University of Minnesota . [Online Document] March 8, 2007. Available at: http://www.tc.umn.edu/~keif0007/Ethical_Evaluation/
- [16] "Radio Frequency Identification (RFID) Systems." Electronic Privacy Information Center. 27 Feb. 2007. 3 Mar. 2007 Available at: <http://www.epic.org/privacy/rfid/>.
- [17] "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations." Privacy Rights Clearinghouse. 20 Nov. 2003. 3 Mar. 2007
- [18] "HB 1031 Bill Analysis." Washington State House of Representatives. 10 Jan. 2007. [Online Document] 6 March 2007 Available at: <http://www.leg.wa.gov/pub/billinfo/200708/Pdf/Bill%20Reports/House/1031.HBA%2007.pdf>
- [19] R. L. Miller and G. Jentz, A. Business Law Today: Seventh Edition. Mason, OH: The Thomson Corporation, 2006.
- [20] J. Morris and Z. Hudgins, "House Bill 1031: Bill Anaysis" Washington State House of Representatives. [Online Document]. March 7, 2007. Available at: <http://www.leg.wa.gov/pub/billinfo/2007-08/Pdf/Bill%20Reports/House/1031.HBR.pdf>
- [21] V. Lockton, & R. Rosenberg, "RFID: The Next Serious Threat to Privacy." Ethics and Information Technology 7 (2005): 221-231.
- [22] M. Williamson, U.S. Department of Peace. Citizenship Primer. 11 April 2007. Available at: <http://www.thepeacealliance.org/content/view/22/146/>