December 2006

Consumer Beliefs about Radio Frequency Identification (RFID) Systems

Jeffrey Stanton
Syracuse University School of Information Studies

Consumer Beliefs about Radio Frequency Identification (RFID) Systems

Jeffrey M. Stanton
Syracuse University School of Information Studies
jmstanto@syr.edu

ABSTRACT

The most widely publicized privacy concern about Radio Frequency Identification (RFID) systems revolves around the inclusion of RFID tags in consumer goods, with the concomitant fear that parties other than the consumer will be able to detect the presence and location of a tagged object. The author used a conceptual framework developed by Mick and Fournier (1998) to understand consumer reactions to RFID technology. Results of a survey of a random sample of N=60 U.S. respondents showed that consumers have little knowledge of RFID technology. About half expressed concerns for privacy related to RFID. Elements of the framework predicted these concerns. Those who were better informed about RFID were also more likely to express concerns about freedom and dependency related to the technology.

Keywords

Radio frequency identification, RFID, consumer attitudes, consumer beliefs.

INTRODUCTION

Radio frequency identification (RFID) systems promise to move the world one step closer to the so-called "Internet of Things." In this vision, objects in the physical world will become as accessible by information systems as data already are (ITU, 2005). When information systems can reliably learn about the presence – and optionally the status – of objects at particular locations in the physical world, a remarkable new range of capabilities become feasible. For applications in supply chain management, transportation, commercial services, security, military, and other areas RFID promises to deliver improvements in flexibility, efficiency, and productivity that far outstrip those provided by barcodes and other mature object identification systems (Engels et al., 2001).

Security and privacy implications arise from at least four characteristics of RFID technologies – reading at a distance, rewritability, on board processing, and sensing – but the implications differ depending upon the circumstances of the RFID application. The most widely publicized privacy concern revolves around the inclusion of RFID tags in consumer goods, with the concomitant fear that parties other than the consumer will be able to detect the presence and location of the tagged object (e.g., Juels, Rivest, & Szydlo, 2003). In a nutshell, this could be described as the "Victoria's Secret Problem": If consumer goods such as underwear contain RFID tags, then a malicious party with an RFID reader can find out the make, style, and color of your skivvies without asking your permission. Although it is possible to imagine a scenario in which these concerns would become problematic, for the most part both physics and economics conspire against this recipe for unauthorized intrusion (Garfinkel, 2002). An RFID system that combined a long distance read range, small tags robust enough to go through the wash, and an inexpensive, portable reader widely adopted and deployed by snoopers is difficult to conceive.

This dismissal is not the end of the story, however. At the broadest conceptual level, RFID tags are no different than any other mobile computing device, and we have enough experience with PDAs, laptops, cellular phones, and other mobile computing devices to know that security and privacy concerns with these devices are both complex and difficult to anticipate at design time. We can anticipate that future standardizations and economies of scale in manufacturing will make full featured active RFID tags commonplace. Active tags overcome many of the distance and capacity limitations of passive tags. Upcoming advances in battery technology may also enhance the feasibility and operational lifetime of active tags.

Once programmable tags become cheap and ubiquitous, creative individuals and firms will find thousands of unanticipated applications for them. As these applications proliferate, the opportunity for valuable data stored on tags to go astray will also multiply. In addition, as more and more RFID applications are deployed, the likelihood of finding an inexpensive RFID reader as a common household device will also increase. Consumers can already purchase toys for their children that contain both RFID tags and readers. Major credit card companies are already marketing quick payment cards that contain RFID technology, while other firms have developed payment terminals for consumers to use on their own personal computers. If

we imagine a billion tiny cellular phones – each no bigger than a fingernail, and each containing small collections of interesting data – and we imagine attaching these transponders to virtually every object of any significance in our daily lives, then we can begin to think about the privacy and security issues related to RFID (Sarma, Weis, & Engels, 2003; Weis, 2003).

In this paper, I extend the existing literature on consumer reactions to RFID (e.g., Günther & Spiekermann, 2005), by assessing the knowledge and beliefs of a sample of U.S. consumers with respect to RFID technologies. Whereas previous research descriptively reported consumer opinions about RFID, the present paper examines the relationship of objective knowledge of the technology to subjective concerns about privacy. Furthermore, the paper conducts this examination within the context of a theoretical perspective designed to explore the paradoxes of new technology from a consumer perspective.

THEORETICAL PERSPECTIVE

Mick and Fournier (1998) developed a conceptual framework for understanding consumer reactions to new technology focusing on anxiety and stress. These researchers used grounded theory and an in-depth data collection to focus on eight paradoxes of new technology that consumers face. Using these paradoxes as a central feature of their conceptual framework provided a powerful method of understanding the subtleties of how consumers react to new technologies. Most technologies that are introduced to consumers have benefits that the technology is expected to bring. Few if any new technologies that are introduced to consumers have intentionally negative features built in, although many technologies eventually show unintended side effects, some of which are perceived negatively. A contemporary example of this is the cellular phone. While these phones provide substantial convenience benefits for consumers, their indiscriminate use in public places has upset some people's standards for appropriate behavior. Additionally, the use of cellular phones while driving appears to enhance the likelihood of causing or being involved in an accident.

In this light, every new technology represents to the consumer a unique blend of opportunities and threats. Mick and Fournier's paradoxes represent the tensions between these opportunities and threats. Table 1 identifies the eight paradoxes and describes briefly how radio frequency identification (RFID) systems map onto these paradoxes. Parenthesized material in Table 1 refers to older technologies that exemplify the same paradox.

Paradox	**Interpretation for RFID**
Control vs. Chaos	…whether the use of RFID tags in consumer products will make life more orderly or create new kinds of disorganization/chaos.
Freedom vs. Dependency	…whether RFID tags in consumer products will people more dependent on technology or less dependent on technology.
New/Obsolete	…when RFID comes into common everyday use, will it already be outmoded (e.g., 8-track tapes), or will the technology keep evolving into more advanced forms.
Competence vs. Incompetence	…whether RFID in general use will make people feel incompetent about the technology (e.g., older people and VCR programming) or competent to deal with the technology.
Efficiency vs. Inefficiency	…whether the use of RFID tags in consumer products will save the consumer effort (e.g., bar codes and scanning cash registers), or will cost the consumer greater effort.
Fulfills Needs vs. Creates Needs	…whether RFID fulfills an existing need or if it is a solution in search of a problem.
Assimilation vs. Isolation	…whether RFID technology will tend to bring people socially closer together (e.g., flash mobs) or will tend to isolate them from the social world around them (e.g., iPods).
Engaging vs. Disengaging	…whether RFID will prompt people to become more engaged and active in the world (e.g., GPS) or more disengaged and passive (e.g., cable television).

Table 1. Eight Paradoxes from Mick & Fournier

Table 1 makes evident the fact that some of these paradoxes are more relevant to currently understood applications of RFID technology than others. For example, RFID clearly has implications for the efficiency versus inefficiency paradox, assuming that current plans for the technology – such as smart scanning of shopping cart contents – come to fruition. In contrast, it is more difficult to see how currently envisioned applications of RFID would have significant implications for the engaging versus disengaging paradox. Note, however, that such assumptions can turn out to be notoriously incorrect because of the rapidity with which the applications of a technology evolve. Just a few years ago, few consumers would have envisioned that a child's doll would have come equipped with RFID-tagged accessories and RFID readers built into the body of the doll. Such applications may have unseen implications for any of the eight paradoxes described in Table 1.

Mick and Fournier's (1998) conceptual framework assumes that the paradoxes of new technology are not resolvable per se – in other words there is, for example, no right answer on whether RFID will create or alleviate chaos – but that consumers engage different strategies for coping with the paradoxes and some consumers do so more successfully than others. Taking an older example alluded to in Table 1, the arcane programming interfaces for setting up recording on early models of VCRs had a legendary befuddling effect, particularly on older consumers. Many older consumers resolved this paradox by simply ignoring the recording interface, by seeking programming help from younger people, or by opting to purchase or upgrade to models that offered on screen programming "wizards." Further, despite the feelings of incompetence that may have been caused by the arcane programming interfaces, many consumers nonetheless purchased VCRs because of the other benefits. Note, however, that other technologies have notably failed to succeed in the face of these paradoxes – 8-track analog tape cassettes, the :CueCat barcode scanner, Kodak disc cameras, Philips CDI-I technology, Microsoft Bob, the Iomega Clik! Drive, DIVX/Flexplay/ez-D pay per view DVDs, the Segway personal transportation device, and Sony's HiFD floppy disk drive are among the hundreds of consumer technology products that failed to provide sufficient benefits in the face of various barriers to consumer adoption.

With respect to RFID technology the most commonly cited and discussed concern about the technology pertains to whether it will impinge upon the privacy of consumers' goods that are tagged with RFID (e.g., Grafinkel, 2002). Most definitions of privacy pertain to control and freedom – control over one's personal information and freedom from intrusion by external authority – and thus I hypothesize that Mick & Fournier's paradoxes pertaining to control versus chaos and freedom versus dependency are most likely to demonstrate relations to consumer's privacy concerns. In general, however, it seems likely that members of the U.S. public have inaccurate conceptions of the capabilities and functions of RFID systems (an issue that can be explored with data). Given this possibility, I expect that those who are most troubled by control and freedom concerns will also have the least knowledge of RFID systems.

METHOD

Using the StudyResponse panelist response system, I surveyed a random sample of 200 U.S. citizens. From this sample, N=60 individuals actually provided completed surveys for a response rate of 30%. These data should be considered preliminary, as the small sample places important limits on statistical power that make detection of the predicted effects more difficult. Respondents were 64% women and 87% Caucasian with an average age of 32 years. The survey comprised 13 closed-ended questions and one open-ended question and the average completion time was approximately six minutes.

The survey opened with a single question about prior experience and knowledge of RFID technology, with responses on a six point scale ranging between "I had not heard of RFID prior to taking this survey" and "I'm an expert because I've worked on RFID myself." This question was placed on the first page of the survey by itself to avoid contamination from later material.

In recognition of the likelihood that many consumers would have had limited exposure to RFID technology, a brief explanation was provided on the second page of the survey prior to further questioning:

> *Please read the short paragraph below very carefully:*
>
> *Radio Frequency Identification (RFID) is a new technology already in use by some retailers. Within a few years RFID will replace bar codes. Small computer chips, called RFID tags, are attached to product containers or inserted into the products themselves (example: clothes). Using a reader device, a retail worker or other person can activate the RFID tag from a distance, causing it to send back the information it contains using radio waves. The reader receives this information and sends it to a computer. The radio waves used in RFID systems work properly even if they pass through cloth, plastic, wood, paper, or cardboard, but not through metal. Soon, RFID tags will probably be built into or attached to many consumer goods such as clothes, toys, appliances, food, cellphones, CDs, DVDs, and many other items.*

Note that this explanation contains only factual material, presented in simple, non-biased language. The specific capabilities of RFID systems are not described, because objective knowledge of RFID was assessed in the next three questions. In the

first of these three, the survey asked, "Given everything you know about RFID, what is your best estimate of the present cost of one RFID tag? Think about this question in terms of what a major retailer must pay, per tag, when buying the tags in bulk today." This question was designed to assess the consumer's knowledge of how ubiquitous and pervasive RFID technology is. At this writing, articles in RFID trade magazines typically refer to the possibility of obtaining a suitable return on investment by tagging individual, high-value items with tags that cost $0.30 apiece, a price that it is feasible to obtain for high volume applications. The six response options available to survey respondents ranged from less than $0.01 per tag to more than $10.00 per tag and were described in increasing powers of ten to cover a wide range so as not to bias the respondent with respect to the answer most likely to be correct.

In the second of the three knowledge questions, the survey asked, "Given everything you know about RFID, what is your best estimate of how far away (the maximum distance) a typical RFID reader device can be from the tag and still get an accurate report of the information on the tag?" This question was designed to assess the consumer's knowledge of the practical distances at which RFID scanning can occur. Although there is no theoretical limit on the read range of active tags (assuming an arbitrary power source and antenna configuration), the passive tags that are affordable for the tagging of consumer goods are limited to either a few centimeters for near field (low frequency) applications, or a few meters for far field (high frequency) applications. Note that some far field applications have been tested at much longer distances, but tag cost and reader configurations make long distance applications unlikely in consumer good's tagging, at least for the near future. The six options available to survey respondents ranged from a distance of less than one inch or 2.5 centimeters to a distance of more than 100 feet or 30 meters and were described in increasing powers of ten to cover a wide range so as not to bias the respondent with respect to the answer most likely to be correct.

In the last of the three knowledge questions, respondents were asked to place checkmarks next to a set of capabilities that they believed RFID tags possessed. Table 2 lists these capabilities.

Capability Description
A tag can store information.
A tag can send information when activated by a reader.
A tag can send information at any time, even when not activated by a reader.
A reader can send new information to a tag, which the tag will then store.
A tag can report its location in a room to a reader.
A tag can report the temperature of the item it is attached to.
When two or more tags are right next to each other, a reader can find and get information from all of them.
A tag can be deactivated by the consumer.

Table 2. RFID Capabilities for Knowledge Test

All eight items in the list in Table 2 are accurate descriptions of actual capabilities of existing RFID systems, although not all have been widely deployed outside the laboratory. The first two items were implied by the description on the second page of the survey, so we expected the majority of the respondents to get at least one or two items correct.

The next eight questions were forced choice items that allowed each respondent to express his or her beliefs about the eight paradoxes with respect to RFID technology. Item wordings followed the descriptions in Table 1. In each case there was a normatively more optimistic choice (e.g., "RFID systems will help make life more orderly.") and a more pessimistic choice (e.g., "RFID systems will lead to upheaval or disorder.").

The final two questions were a pair; both inquired about respondent beliefs concerning the privacy implications of RFID. The first question was closed ended and read as follows, "Given everything you know about RFID systems, how concerned are you about your personal privacy?" This question offered a five option response scale ranging from "Not concerned at all" to "Extremely concerned." Finally, an open ended question asked for a brief explanation of each respondent's answer to the closed ended privacy question.

RESULTS

I will begin the report of the results by providing a selection of the open ended responses about RFID and privacy offered by the survey respondents. A number of the verbatims were redundant with one another, and these have not been presented. Nonetheless, the roughly equal proportions of responses suggesting minimal concerns versus those expressing some concerns do accurately reflect the overall open ended data.

Open-Ended Responses Suggesting Minimal Concerns

I am not really concerned about my personal privacy since I do not have much to hide. RFID in terms of privacy issues will probably not affect me.

I am not at risk with RFID because I am not in a high-security position and do not have many assets.

Not quite concerned at all since I feel my information is secure.

Not really sure what it is and do not really care at this point in time.

I don't know enough about the product to understand how it could affect me personally. I won't be tagged personally so how could it affect my privacy?

Since I'm still not exactly sure how RFID works, I am not too terribly concerned. Especially since it has not been put into use yet.

As an engineer and professional manager, I welcome the technology inherent in RFID systems.

I think it will cut down on thefts. It will shorten lines in the stores. It will improve the workplace.

The benefits far outweigh my concerns. The uses are limitless, from anti-theft to lost pet ID. Although there are potential misuses, I don't consider these to be a viable, practical threat.

I am not at all concerned about my privacy. I think people have become a little crazy about businesses knowing their preferences. I find it helpful to have people offer me and make it easier to find what I want anyway.

I don't plan on stealing anything. I think RFID technology will make things much easier for retailers.

Open-Ended Responses Suggesting More than Minimal Concerns

I have more questions than there are answers being provided from consumer organizations I can trust. I understand the benefits of RFID to manufacturers and retailers; I do not understand why it is so important to consumers for our goods to be tracked.

If the tag is not deactivated, then can follow a person's living patterns after purchase.

It's a case of Big Brother. Even now, the federal government is tracking our movements in the disguise of national security. It will never end.

If you can invent something that will send info on the item, what's to stop anyone from inventing items that would transmit information on things that denote what your status is in society.

I don't need people knowing the types of products I buy, where I buy them, when I shop - I prefer a bit of anonymity in the world.

What was wrong with just scanning a bar-code? Now we're going to have more radio frequencies in the air to jam each other.

I am a born again Christian and this is a sign of the proving of the end times, when there is a mark needed for everyone to be able to make purchases. This is mentioned in revelations of the New Testament.

I am somewhat concerned because the RFID would be all over me. It would be on my clothes, food, etc. If I can be tracked by this or identified by this, this would MAJORLY control my privacy.

I am a modern person but this kind of technology is getting on my nerves. Pretty soon we will not have any privacy and personal space anymore.

Quantitative Analysis

The modal response (46.7% of all responses) on the question concerning prior experience and knowledge of RFID technologies was the lowest category, "I had not heard of RFID prior to taking this survey." Only 13 respondents (21.7%) reported responses of "I know a few things about how RFID works" or higher. No respondents chose the highest category ("I'm an expert because I've worked on RFID myself."). These results suggest that self reported beliefs about knowledge of RFID were quite low.

In estimating the current cost of RFID tags the mean value was $0.99 (standard deviation, 275.4). Note however that this was a deceptive measure of central tendency because of the powers of ten in the response scale. The modal response, with 55% of all respondents (n=33) was $0.10. Fully 81.7% of the sample believed that the cost of a tag was $0.10 or less, indicating a substantial underestimate of the actual current prices of tags used by retailers.

In the same vein, the mean estimated read distance for a typical tag was 10.6 meters (standard deviation, 13.3 meters). Again, this was a deceptive measure of central tendency because of the powers of ten in the response scale. The modal response, with 35% of all respondents, was 3 meters, a value that is not unreasonable for far field RFID applications in current use or planned for the near future. Note, however, that 31.7% of the sample believed that tags could routinely be read at distances of 30 meters or more, a capability that is rarely achieved outside of the laboratory or without the use of expensive active tags.

On the eight item test of knowledge, the mean number of items correct was 3.3 (standard deviation, 1.74). If achieving at least five out of eight correct would be considered a "passing score" then only 26.7% of the sample achieved a passing score. Interestingly, 10 respondents (16.7% of the sample) got only one item correct and that item was typically the assertion that "A tag can send information when activated by a reader." Most of these ten people failed to check the item that stated, "A tag can store information," evincing a fundamental misunderstanding of the nature of the reading process. Among these respondents, who were also likely to put themselves in the lowest knowledge category on the first self report question, it is likely that they did not understand that the analogy to barcodes extended to the storage of an actual numeric value within the tag.

On the paradox forced choice items, the average number of "optimistic" responses (e.g., more control, less chaos) was 4.44 (standard deviation, 2.1). Given that there were eight paradoxes, this value is quite near the middle, suggesting that the typical respondent had four areas where the paradox was not problematic for them and four where it was. The control and freedom paradoxes were the most extreme. Fully 70% (n=42) of the sample believed that RFID technology would increase their control and decrease their chaos. As the item stated, "RFID systems will help make life more orderly" was the option of choice. In contrast, however, 81.7% (n=49) believed that RFID would limit their freedom by making them more dependent on technology.

On the privacy question, which is treated as a dependent variable below, the mean response was 2.67 (standard deviation, 1.39) on a scale of 1 to 5. The modal response was the middle option, "Somewhat concerned: RFID may affect my privacy in the future." Overall, 53.3% of the sample was at least this concerned about RFID and privacy. This result suggests an almost even split between those who have concerns about RFID and those who do not.

I conducted two additional tests. First I correlated the summary of feelings about the paradoxes with privacy concerns. The correlation was -.40, $p<.05$. As I hypothesized, the more optimistic an individual was about the paradoxes, the less that person had concerns that RFID would adversely affect his or her privacy. To provide a finer level of detail on this analysis, I regressed the eight paradoxes on the privacy concerns and found that control/chaos and freedom/dependency were the most powerful predictors. In a trimmed model, the R-squared was .30, $F(2, 54)=11.3$, $p<.001$ (note that three cases were lost because of partial missing data). The beta weight on control/chaos was -.47, $p<.001$, signifying that those who were optimistic that RFID would reduce chaos were less likely to have concerns about privacy. Likewise, the beta weight on control/chaos was -.47, $p<.001$, signifying that those who were optimistic that RFID would decrease their dependence on technology less likely to have concerns about privacy.

In the second analysis I divided the sample first by responses on the control/chaos question and the freedom/dependency question. Then I compared means between the two groups on the knowledge variables from the beginning of the survey. No significant differences arose for the control/chaos grouping. In contrast, however, the freedom/dependency grouping yielded three out of four significant results, with the fourth having means in the same direction as the other three. People who were concerned about a loss of freedom reported more prior knowledge of RFID $t(56)=2.81$, $p<.01$. They also believed that RFID tags were more expensive ($1.17 versus $0.07 for the other group, $t[56]=2.57$, $p<.05$), and they were more likely to have scored higher on the test of knowledge (3.7 correct versus 2.0 correct for the other group, $t[56]=4.4$, $p<.001$). Notably, this result was contra-hypothesized. I expected that those with less accurate knowledge of RFID capabilities would be more likely to have concerns about freedom/dependency than those with more accurate knowledge, but the reverse was true.

DISCUSSION

Based on Mick & Fournier's (1998) conceptual framework of consumer reactions to new technology, I explored current knowledge and attitudes toward RFID technology. My interpretation of the conceptual framework posited that paradoxes of control versus chaos and freedom versus dependency are most likely to demonstrate relations to consumer's privacy concerns. The data suggested that this was true: Benefits of RFID for increasing orderliness in applications such as retail checkout seem to be weighed against the potential costs in increased dependency on the technology. As I assumed would be the case, members of the U.S. public have inaccurate conceptions of the capabilities and functions of RFID systems. Interestingly however, this knowledge connected to beliefs about the privacy implications of RFID in an unexpected way. Specifically, those who were *more* knowledgeable had greater concerns about the extent to which RFID might impinge on their freedom. Other individuals, who expressed lower beliefs in their knowledge of RFID, had unrealistically low estimates of the cost of tags (and therefore, one might assume, a higher belief in their ubiquity), and objectively knew less about the capabilities of the technology, were overall less likely to have concerns about freedom and dependency.

If this result can be replicated, it suggests some unexpected implications. On the face of things, it appears that ignorance is bliss: Consumers who know little about RFID are not worried about it. It would be dangerous, however, for RFID systems manufacturers, retailers, and other advocates of the technology to assume that this position would remain static. To assume that consumers will remain blissfully unaware and thus unconcerned about the implications of RFID is to risk a backlash if a significant privacy breach related to RFID occurs and is publicized. A more sensible, proactive stance would be to assume that knowledgeable consumers need to be told more about the privacy protections than can be built, or already are being built into the technology. In this way, manufacturers, retailers, and other advocates of RFID can please both the minority who have no privacy concerns as well as the majority who do.

CONCLUSION

The primary contribution of this study is to establish a baseline concerning consumer knowledge and beliefs, so that future efforts to inform the public about RFID systems can examine changes in beliefs with respect to the baseline. Data collected and reported in this study are preliminary. Replication and extension of these results is needed before they are used as the basis of any policy suggestions. Nonetheless, the application of a workable conceptual framework to understanding how and why people form beliefs about RFID technology and privacy holds promise for future research and application.

REFERENCES

1. Engels, D., J. Foley, J. Waldrop, S. Sarma, D. Brock. "The Networked Physical World: An Automated Identification Architecture," WIAPP, p. 76, Second IEEE Workshop on Internet Applications (wiapp '01), 2001.
2. Garfinkel, S. An RFID Bill of Rights. Technology Review, page 35, October 2002.
3. Günther, O. and Spiekermann, S. (2005). RFID and the Perception of Control: The Consumer's View. Communications of the ACM, 48 (9), 73-76.
4. International Telecommunications Union (ITU) (2005, November). Executive Summary: The Internet of Things. Geneva: Author.
5. Juels, A., R.L. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Atluri, editor, 8th ACM Conference on Computer and Communications Security, pages 103–111. ACM Press, 2003.
6. Mick, D. G., & Fournier, S. (1998). Paradoxes of technology: Consumer cognizance, emotions, and coping strategies. *Journal of Consumer Research, 25*, 123-143.
7. Sarma, S. E., S. A. Weis, and D.W. Engels. Radio-frequency-identification security risks and challenges. CryptoBytes, 6(1), 2003.
8. Weis, S.A. Radio-frequency identification security and privacy. Master's thesis, M.I.T. June 2003