JISSec 4(1) 2008

Journal of
Information System
Security

www.jissec.org

Mitigating Consumer Perceptions of Privacy and Security Risks with the Use of Residual RFID Technologies through Governmental Trust

Andrew S. Jensen[1]
Joseph A. Cazier[2]
Dinesh S. Dave[3]

Department of Computer Science
College of Computing and Informatics
University of North Carolina at Charlotte
Charlotte, North Carolina[1]
Department of Computer Information Systems
John A. Walker College of Business
Appalachian State University
Boone, North Carolina [2, 3]

Abstract

Many organizations are adopting radio frequency identification (RFID) technologies. These technologies can provide many benefits to the organizations that use them. However, many of these RFID tags remain active after the consumers purchase them. We call these RFID tags, placed in a product for one purpose and left in the product after it has served that purpose, Residual RFIDs. Residual RFID technology can have many positive and negative affects on consumers, business, and society. In this study, we outline

An earlier research in progress version of this paper was presented at the AMCIS conference held in August 2007

some of the likely advantages and disadvantages of Residual RFID from the consumer perspective, then follow up with an in-depth survey of consumer perceptions. In the survey, we attempt to ascertain how consumers will react to the pending implementation of Residual RFID technologies on a mass scale. Specifically, we explore how consumers' perceptions of trust, privacy risk likelihood and privacy risk harm impact their intentions to use the technology, particularly as it pertains to the perceived role of government in the regulation of RFID and the protection of consumer privacy.

Keywords: Government, Privacy, Privacy Risk, Security Risk, RFID, Residual RFID, Technology Adoption..

Introduction

In the near future, almost every product manufactured, bought and/or sold will have a small tag that can remotely and uniquely identify that individual item. Any person or business with an appropriate scanner may determine the item type, price, place of origin, place of purchase, etc., by reading small radio frequency identification (RFID) tags. In fact, it is projected that the current overall RFID market, approximately a $3 billion enterprise with several million tags in circulation today, will grow by more than 800 percent to over $25 billion with tens of trillions of tags in circulation by 2015 (Wyld 2006).

RFID tags are currently being deployed in the supply chains of many organizations. These tags have the potential to bring many benefits to the organizations that use them. However, many of these tags remain after they leave the organization, broadcasting their identities and histories to anyone with a scanner and link to the proper database. These left over tags, installed to help the supply chain, but not removed once they have lived out their intended purpose, are referred to as Residual RFIDs.

The two different types of RFID tags, active and passive, offer their own differing benefits and liabilities to consumers. Active RFID tags are driven by a power source, typically a small battery. These tags are capable of broadcasting their own signal over varying distances, depending upon the potency of the battery and range of the frequency. Although useful only for the duration of their power source, these tags may be extremely important in certain military and other applications, but may offer only limited practicality for consumer use, as the cost to produce such tags would render them prohibitive in a consumer environment.

Passive tags have no power source and are relatively inexpensive to produce. These economical tags are those that are most likely to be found on consumer goods. Lacking a power source, these tags are incapable of broadcasting their own signal. Initially, this sounds like a benefit in terms of consumer privacy, but the lack of a power source effectively makes these tags nearly immortal in consumer terms. They are activated only when scanned or read by a RFID scanning device.

Such activation may occur at a retail location, airport security checkpoint, bus terminal, restaurant, mall, or as the result of a handheld scanner that could be used unobtrusively at any time or place. Active tags have limited life span, but passive tags are forever. These passive tags, still able to be scanned but no longer providing a retail or consumer benefit, are the tags that become Residual RFID tags.

The adoption of RFID technologies is on the rise in retail and other industries. Mandates by Wal-Mart, Target Corp. and Albertson's in the United States, Metro Group in Germany, and Carrefour in France have pushed the use of RFID in retailing, while governmental regulations on the traceability of food in the United States and Europe have pushed RFID into food production. RFID is also being used in security systems, healthcare, livestock tracking, parcel and parts tracking, casinos, U.S. toll roads (think EZ-Pass), law enforcement, and the U.S. Department of Defense (Attaran 2006).

Whether we like it or not, RFID technology is already a part of our lives. Many of its applications have little to no effect on the general consumer (i.e. What can the consumer say about RFID in military applications for the DOD?), but the integration of this technology into other aspects of consumers' lives raises certain concerns.

While the focus on RFID has been on the benefits that accrue to corporations and supply chains through this technology, many organizations have not adequately considered the impact of Residual RFID technology on consumers, business and society. The ultimate purpose of RFID technology is to provide retailers and suppliers with the ability, in time, to track any item remotely and uniquely at the individual level. The impact of this ability, both positive and negative, on consumers in our society will be enormous.

Of particular concern is the threat to individual privacy such technology raises. Consumers have called upon the developers and users of RFID technology to implement precautions to limit the privacy risk issues, while others call upon the government to legislate the implementation and use of the technology. While such legislation may eventually prove effective, the question remains as to whether it will ultimately satisfy consumers to the degree that they feel comfortable with the privacy risks associated with Residual RFID. Consumers may ask themselves:

- Will the government make every effort to protect my privacy from RFID abuse?
- Will the government tell the truth about the risks I may encounter with RFID?
- Can I trust the government to protect me from RFID abuse?

Consumers' perceptions of trust, privacy risk likelihood and privacy risk harm will impact their intentions to use RFID technology, particularly in regards to the perceived role of government in the regulation of RFID and the protection of consumer privacy.

In this paper we begin with a discussion of prior research regarding RFID, discussing benefits and liabilities for consumers as well as business supply chains, and the impact of privacy risk on technology adoptions. We then discuss the basis for our research, specifically the impact that perceived risk likelihood, perceived harm and overall trust have on the consumer's decision to use a given technology. This is followed by a discussion of our data collection method, consisting primarily of an in-depth survey of consumer perceptions regarding the potential mass-scale adoption of RFID technologies. Finally, we present the results of our findings and evaluate the validity of our hypotheses.

Literature review

RFID in the Supply Chain

There is a huge need for improvements to the business process that will enable suppliers and retailers to cut costs, reduce inventory, improve order forecast, improve asset management, and provide higher customer satisfaction (Attaran 2006). These needed improvements may potentially be met through the implementation of RFID technology.

Supply chain automation is probably the single greatest and most attractive factor behind the development of RFID technology. RFID is currently being used for tracking assets in offices, labs, warehouses, pallets, and containers in the supply chain. Through RFID, suppliers are able to determine the location of a pallet, track its journey through the supply chain, and make instantaneous routing decisions (Attaran 2006). Additionally, RFID technology has distinct advantages over the barcode technology. According to Juels (2005), an RFID tag provides a unique serial number that distinguishes among many millions of identically produced products. RFID tags are readable without line-of-sight contact and without precise positioning; as a result, RFID readers can scan tags at very high rates.

Implementation of RFID requires a significant investment, and the return on investment is directly associated with the improvements it enables. The challenge for information technology experts is to determine how to integrate RFID with existing supply chain management, customer relationship management, and enterprise resource planning applications within existing systems (Attaran 2006).

Residual RFID Benefits

The benefits of RFID technology for business and government have been well-documented. The benefits of RFID technology for consumers, however, are often overlooked. Yet it is imperative that consumers understand that there are legitimate consumer benefits through the use of the technology. Without realizable consumer benefit to counteract the perceived risks associated with RFID, retailers will find it difficult to maintain a solid customer base in the face of the perceived security and privacy risks.

RFID developers have sought to limit the perceived risk by trying to educate consumers as to the positive benefits of RFID and providing privacy policies to explain what data is being collected and how it's being used (Eckfeldt 2005). It is a difficult task for retailers and RFID developers to limit the risk of privacy invasion for consumers. The problems are many and complex. It is much easier and more effective to improve the perceived value consumers receive through RFID by offering them better prices, service, and/or experience (Eckfeldt 2005).

It has been suggested (Eckfeldt 2005) that RFID-based technologies provide value to consumers in three basic ways:

1. Peace of mind
2. Consumer convenience
3. Improved service

The consumer benefits of RFID technology can be seen through many existing applications. There are additional benefits that come through Residual RFID as well. Since RFID technology is designed to enhance the productivity and efficiency of the supply chain, its usefulness, in theory, ends when the product to which the RFID is assigned leaves the supply chain and enters the consumer domain. RFIDs that have completed their job in the supply chain are Residual RFIDs. Yet, they still may offer certain benefits for consumers. Examples of these benefits can easily be evaluated under Eckfeldt's headings.

Peace of Mind

Eckfeldt (2005) explains that the RFID application with the greatest success in terms of adoption and proliferation involves security. It is interesting to note that the very ability that has been the source of so much public outcry against the technologyit's potential ability to positively identify and track individualsis also one of its greatest consumer assets. This ability is what has caused RFID to find its way into security systems around the globe. The perceived value here is that consumers know that only authorized peoplepersons for which they have at least an element of trusthave access to the sensitive data collected by such systems. When tracking lacks any obvious security benefit for consumers and delivers only marketing information for retailers, the risk/reward equation does not add up for consumers (Eckfeldt 2005).

Law enforcement can use Residual RFID technology to easily track stolen goods. The use of RFID scanners by police investigators may significantly enhance such tracking procedures, enabling faster recovery of stolen property and ultimately even deterring such crimes.

Consumer Convenience

The EZ-Pass toll-collection system is a perfect example of successful RFID adoption by consumers (Eckfeldt 2005). Consider the convenience benefit: a consumer has the choice to stop, roll down the car window, get out the money, hand it to the toll-collector, get the change and receipt, put it in the ashtray, roll up the window, and start driving again, or this same consumer may simply approach the EZ-Pass entry point with the RFID-equipped pass on the dash and drive right through with barely a reduction in speed. Despite the fact that the scanner in such systems creates a precise time log and can be used to map the consumer's travels, the perceived convenience benefit for daily commuters is likely to be greater than the perceived privacy risk such documentation poses.

Residual RFIDs can also greatly simplify the process of returning retail goods. Products with embedded RFID tags can potentially be returned without a receipt, and aid both the consumer and the retailer in streamlining customer services. The future use of RFID may also include ease of checkout, in that consumers could checkout merchandise by rolling shopping carts past point-of-sale terminals. These terminals would automatically compute the total amount and perhaps even charge RFID-enabled payment devices. Another possible application of RFID technology in the customer relationships management arena includes interactive objects (Juels, 2005). Consumers could interact with RFID-tagged objects through their mobile phones, for example.

Improved Service

Certain high-end fashion retailers are beginning to use RFID-based systems to improve the overall customer service and consumer shopping experience. Casinos, such as the Wynn Las Vegas resort, are using RFID to fight fraud and give guests easy access to house credit. Delta Air Lines uses RFID tracking systems to ensure that baggage arrives on time at the appropriate destinations. The net result of all these solutions is a tangible consumer benefit (Eckfeldt 2005). Who can argue with a more pleasurable shopping experience, improved guest treatment and security, or never having to deal with lost luggage again?

Insurance companies may be able to quickly catalog complete inventories of a person's belongings for home insurance purposes. Rather than relying on the lengthy process of hand-written lists and estimated replacement costs, agents may simply scan a home and record and catalog the results based upon the RFIDs present in the home.

Liabilities of Residual RFID for Consumers

While consumers may realize legitimate benefits from Residual RFID, the liabilities cannot be ignored. Spiekermann and Ziekow (2005) suggest that five immediate and key threats of RFID technology are:

1. Unauthorized assessment of one's belongings by others
2. Tracking of persons via their objects
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for their objects

The most obvious violation is perhaps the first listed by Spiekermann and Ziekow (2005). They suggest that “by scanning inventories of flats and houses or baggage at airports promising targets for theft or burglary might be identified” (Spiekermann and Ziekow 2005, p. 3). They also suggest that individuals may be tracked by others through the objects they carry (Spiekermann and Ziekow 2005). The offending party may be an individual, organization, or government.

In addition, businesses could potentially target individuals with personalized advertising in-store or out based upon objects they carry. While businesses may desire such efficiency in advertising, many consumers may view such efforts as intrusive.

The identification and retrieving of social networks is another potential violation. According to Spiekermann and Ziekow (2005), through the use of data mining techniques, additional information can be gained from registered [RFID] tracks. Analyzing information about movement can be used to deduce social links between persons. While this may be of potential interest for governmental agencies in the context of law enforcement (Spiekermann and Ziekow 2005), there is also the potential for abuse and criminal intent.

Technology paternalism refers to a fear expressed in focus groups of uncontrolled autonomous action of machines that cannot be overruled by object owners (Spiekermann and Ziekow 2005). RFID fits into this idea quite well. Spiekermann and Ziekow suggest that “RFID has the potential to overrule or punish people instantly for a myriad minor incidents of misconduct and by this intrude heavily on peoples' life” (Spiekermann and Ziekow 2005, p. 8).

The scenario that people might be held responsible for objects they own or owned has frequently been cited in press articles to criticize RFID technology (Spiekermann and Ziekow 2005). While in some respects this may be very beneficial (i.e. objects used in the commission of a crime may be easily traced to their owners) it could also prove quite intrusive (objects used in the commission of a crime may have been stolen, for example).

These are only a few of the many potential liabilities that are currently being discussed regarding RFID technology. As the technology gains more and more attention, additional concerns continue to be raised. The prevalence of these concerns and the perceived risk to consumers these concerns generate have a direct affect on consumers' willingness to purchase goods containing RFID technology.

Impact of Privacy Risk on Technology Adoptions

Featherman et al. (2006) investigated whether consumer perceptions of artificiality increase perceptions of e-services (web-delivered services) risk, which has been shown to reduce consumer acceptance in a variety of online settings. Their results support the contention that e-services of less risky e-services categories will be perceived as more authentic and less likely to use. Therefore, e-service providers must carefully assess their respective categories and plan accordingly. The study further suggested that an e-service provider operating in a risky category may consider to invest more resources to develop an interface that projects a higher degree of authenticity. Additionally, vendors may display in-depth security information on separate pages accessible to those consumers with an affinity to read it, and simple catchy graphics for more novice system users.

Cazier et al. (2007) state that privacy risk factors are found to negatively influence consumer intentions. While theirs was a study regarding e-commerce and privacy risk in a web environment, the principle from our point of view remains the same. If a consumer perceives a particular privacy or security risk as a result of Residual RFID, that perception could profoundly affect that consumer's intention to purchase a particular product carrying a RFID tag or engage in commerce with a retailer that utilizes RFID technology. Juels (2005) surveyed technical research on the issue of privacy and security for RFID. The majority of the articles in the survey explore security and privacy as a relationship between RFID tags and readers.

It has been stated that information technology is "morally neutral" in that it can be employed for both positive and negative uses (Conca, et al. 2005, p. 167). Some of these uses have already been explored in previous paragraphs, and while there are legitimate benefits to the use of Residual RFID, the privacy risks are significant enough to warrant consumer concern. This is not an unreasonable response. Privacy concerns rate among the highest of the risks that Americans fear most (Garfinkel et al. 2002). In fact, most Americans believe they are more likely to be a victim of a cyber attack than a physical crime (IBM 2006).

Dinev and Hart (2006) studied the balance between privacy risk beliefs and confidence and enticement beliefs that influence the intention to provide personal information necessary to conduct transactions on the Internet. The authors developed and tested a model that incorporated contrary factors representing elements of a “privacy calculus.” The study provided insights into the argument pertaining to privacy paradox as studied by Sweat (2000) that consumer behavior contradicts consumer preference. The finding of study further suggested that the factors perceived privacy risk and privacy concerns were found to be related to the willingness to provide personal information to conduct transactions on the Internet.

Hoffman et al. (1999) find that when users perceive an online environment to be risky, they are less likely to purchase online. One of the greatest reasons for this type of consumer behavior is the fact that many consumers are not fully aware of how their private data is being used and processed in an online environment (Raab and Bennett 1998). Residual RFID, however, offers a completely new environment with which consumers are likely to be unfamiliar. Organizations' privacy practices regarding RFID may not be readily available, and even if they are, simple consumer ignorance of the technology may cause significant numbers of consumers to be completely unaware of how their purchasing habits and private information may be used by a given organization.

It should also be noted that when people perceive risks, they change their behaviors accordingly, often by performing a risk benefit calculation that assists them in deciding whether they should or should not disclose private information (Milne and Culnan 2004). But in the case of RFID, that choice to disclose or not disclose may not be available. Whether it is the retailer's scanning of purchased goods or the illicit scanning by would-be thieves, consumer purchases will be tracked, catalogued, and evaluated for further action.

Theory

The formation of our hypotheses regarding consumer behavior is based upon three mitigating factors:

1. the perceived likelihood of a privacy breach occurring,
2. the perceived harm such a privacy breach might incur, and
3. the level of trust a consumer feels toward the government's ability to control and regulate the use and/or abuse of RFID technology.

The first two factors, perceived event likelihood and perceived harm, are critical components of our theory regarding consumer behavior and together comprise what we identify as consumer privacy risk. This model follows the suggestion of Cazier et al. (2007), that the two elements that comprise consumer privacy risk are perceived privacy risk likelihood (the probability of an event occurring) and perceived privacy risk harm (the amount of loss a consumer may sustain from such an occurrence). Risk is then calculated as the probability of an event occurring multiplied by the loss or amount of harm that could be done if that loss is realized (Straub and Welke 1998). These elements, combined with trust, will directly influence consumer behavior regarding RFID adoption and use.

Perceived Event Likelihood

Risk likelihood is the perception of probability that a privacy breach will occur (Cazier et al. 2007). Most people, upon perceiving that an action they are about to take involves a certain amount of risk; subsequently re-evaluate the decision to carry on with the intended action. This applies to consumer purchasing as well. Most consumers evaluate the probability of risk to their privacy every time they engage in an online transaction. Certain factors, such as an organization's security policy or encryption standards, may influence the consumer's decision regarding whether to engage in a business transaction with that organization.

Perceived Potential Harm

Risk harm is the perception of the level of damage that would occur in the event of a privacy breach (Cazier et al. 2007). When determining consumer behavior, the potential for harm must be factored alongside the potential of a privacy breach to occur. For one consumer, the potential harm that may occur in the event of a privacy breach may be relatively small, and therefore a minimal factor in that person's intent to purchase, but for another consumer, the potential harm may be very great, significant enough to be a deterring factor in that person's intent to purchase. The potential occurrence of a privacy breach and the potential harm that may occur as a result of that breach may be negated or significantly diminished by the trust a consumer has in the organization with which the consumer intends to do business.

Trust as a Mitigating Factor

Trust has been defined as the “willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform particular actions important to the trustor, irrespective of the ability to monitor or control the other party” (Mayer et al. 1995, p. 712).

The willingness of a party to be vulnerable is a key component of trust. In a business-to-consumer (B2C) setting, customers are more vulnerable than in a face-to-face setting (Cazier et al. 2006). This is critical in the RFID environment.

Cazier (2007) expounds on the theory proposed by Mayer et al. (1995), regarding the three dimensions of trust, which are defined as ability, benevolence and integrity, by testing and validating their impact on behavioral intentions. We propose that the elements of perceived risk likelihood and perceived risk harm must be factored independently into the behavior model to obtain a more accurate prediction of consumer behavior (see Figure 1 below).

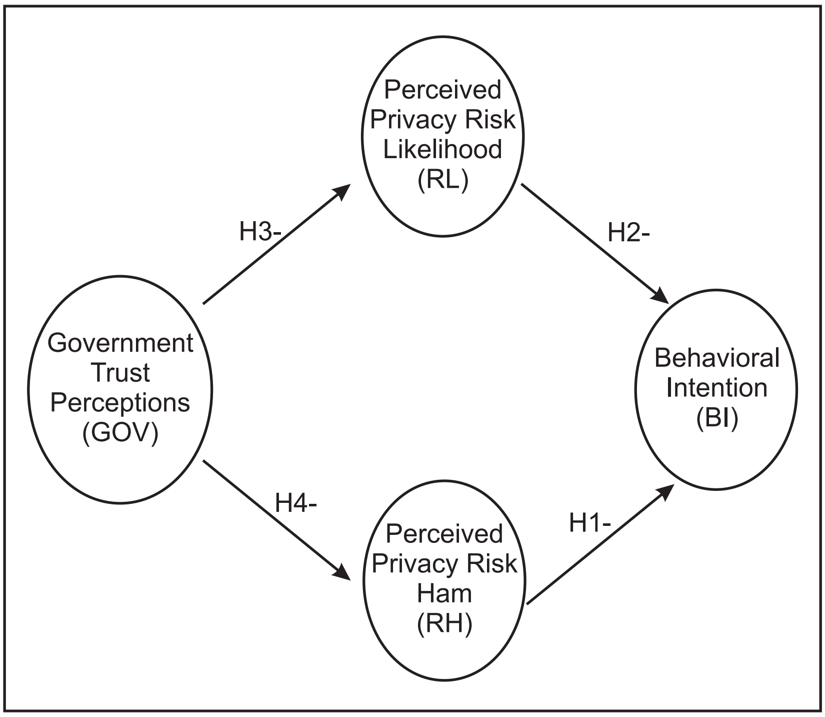

Figure 1. Research model

All social exchange involves some risk. When an individual trusts a person or organization, then it is more likely that he or she will be willing to take risks with them (Cazier 2006).

The act of purchasing goods from organizations employing RFID technology may easily be likened to online transactions. When customers place an order online, they are frequently asked to reveal personal or financial information to the vendor, which can potentially be used by criminals to commit identity fraud. In order to engage in online transactions, clients need to trust vendors enough to be willing to put themselves in such a vulnerable position (Cazier et al. 2006). A similar situation now exists in the world of RFID technology. Consumers will be required to put their trust in organizations that use this technology, trusting that the personal information gained as a result of RFID will not be used in a way that compromises their privacy or security. However, consumers must also trust that steps will be taken to ensure their protection from other violations made possible by the use of this technology, whether these protective steps come from the organizations themselves or from the governments of the nations in which they live.

Hypotheses

Based upon the factors we have previously discussed, we have composed four hypotheses that we test through a survey instrument designed to assess the perceptions and usage intentions of individuals toward organizations and products that employ Residual RFID technology.

We propose that perception of privacy risk will directly influence consumer acceptance of RFID technology. We anticipate that consumers' perceptions of privacy risk in regards to the potential for harm as well as the likelihood of a privacy breach occurring will have a negative impact on their intentions to accept Residual RFID technology. We also anticipate that consumer perceptions of trust in government's ability to protect consumer privacy will reduce their perceptions of perceived privacy risk likelihood as well as perceived privacy risk harm.

H1: Consumer perceptions of the potential for harm due to privacy risk will have a negative impact on their intentions to accept Residual RFID technology.

H2: Consumer perceptions of the likelihood of a privacy breach occurring will have a negative impact on their intentions to accept Residual RFID technology.

H3: Consumer trust in the government will reduce their perceptions of perceived privacy risk likelihood.

H4: Consumer trust in the government will reduce their perceptions of perceived privacy risk harm.

Methodology

The research methodology was conducted using a survey instrument, based upon previously validated scales where possible, that assesses the perceptions and usage intentions of individuals toward organizations and products that employ Residual RFID technology. Respondents are given a brief written summary of the technology and some of the likely positive and negative impacts on consumers. In addition to the written summary, respondents in the pilot studies were given a web address and encouraged to listen to a short news story presenting both positive and negative views of Residual RFID technology as heard on National Public Radio (NPR).

This NPR news story provides a brief synopsis of RFID technology, how it works, its benefits and potential liabilities. Specifically, it discusses how RFID may be used to reduce waste and lost inventory in retail supply chains, as well as possible consumer benefits. It also addresses issues raised by consumer privacy advocacy groups who are concerned about the potential privacy threat posed by individually tagged consumer items. Finally, the story discusses proposed means for dealing with and remedying the potential privacy risks, from legislation to “anti-RFID” blocker tags (Abramson 2004).

Scale Development and Pilot Studies

In the interest of research accuracy and applicability, we selected questions for the survey instrument from previously validated instruments where possible, adapting them to meet the criteria of our survey. For this the risk likelihood and risk harm questions were adapted from Cazier et al. (2007), where they did a similar study looking at these variables and their impact on the adoption of technology for a university information system. The questions in the Cazier et al. (2007) paper were loosely based upon work by Featherman et al. (2006) and Dinev and Hart (2006), then tested and validated to meet the study objectives.

The trust questions were inspired by McKnight et al. (2002), which looked at trust in an e-commerce system, but had to be significantly adjusted to meet the government and RFID context. These questions were also influenced and adapted from Battacherjee (2002), where the author developed trust scales for an online firm. These were also significantly adapted for the government and RFID context to give an overall view of trust. The questions on behavioral intentions are new and were developed to measure the types behaviors that industry and researchers would be most interested in and are typical of this type of research.

All of the scales were then subjected to scale validation through pilot studies. The first pilot study had 96 respondents and was used to solicit feedback on the scales and see how well it flowed and how much base knowledge the average person had regarding RFID. In the first pilot study we found that a majority of our respondents did not have a deep understanding of the risk and rewards possible for consumers through RFID technology. Therefore we prepared a short written summary about the technology for a second pilot study to make sure that each respondent had at least a base level understanding of some plausible benefits and potential liabilities resulting from full scale adoptions of RFID technologies for the consumer, as opposed to focusing on only business impacts.

This summary was designed to be as unbiased as possible and was modeled after some of the information presented in the NPR news clip by Abramson (2004) as well as similar ideas from the authors. This tutorial can be found in Appendix A. In addition, a link was included for the second pilot study to the NPR news story, which was conducted online, and respondents were encouraged to listen to it.

This second pilot study had 189 respondents, most of them undergraduate business students. We used this data to test our scales by running a factor analysis on the data and testing preliminary results, which were consistent with our finding in the final survey. We made some minor modifications to the wording of some questions for clarity based on the factor analysis and reliability scales for the final instrument. However, we found that only about 29% of respondents listened to the NPR story. This lead to a concern that there may be some bias introduced between those that listened to the story and those that did not. For this reason the final survey was conducted with the written summary of RFID technology, but not with the NPR news clip, so that all respondents would be given the same base level of knowledge. The final survey was geared toward non-students and had 320 respondents (see Table 2 for specific demographics data).

Data Collection

The research methodology was conducted using a survey instrument, based on previously validated scales where possible, that assessed the perceptions and usage intentions of individuals toward organizations and products that develop and/or employ Residual RFID technology. While there has been some popular press about Residual RFID technologies, such as the report by Abramson (2004) on National Public Radio (NPR), the implications of Residual RFID technologies may not have fully entered the consciousness of the average consumer. Since mass adoption of these technologies is imminent, it is important to understand how consumers do and will react to mass Residual RFID adoption. Therefore, a brief education piece instructing subjects regarding the fundamental principles of Residual RFID technology was presented to each subject prior to completing the survey.

Scale Validation and Reliability

The survey instrument was constructed using questions from several validated existing surveys. Modifications were made to questions where necessary to coincide with the nature of RFID technology. All items in the survey were measured on a 7-point Likert scale, with endpoints labeled “Very Strongly Disagree” / “Almost Impossible” / “No Harm At All” (Value =1) and “Very Strongly Agree” / “Almost Certain” / “Severe Harm” (Value = 7) as dictated by the form in which the item was stated. Data collected during the study was stored in a database for later statistical analysis.

Four significant factors cleanly loaded in the model, as shown in Table 1. All alpha values are .8 or higher, factor loadings are routinely high as well. This analysis demonstrates that there are four clear factors, all of which load cleanly on the latent constructs we are attempting to measure. Results were analyzed using LISREL version 8.2 for structural equation modelling.

Factor / Alpha	Items	Description	Mean	Std. Dev.	Factor Loadings*			
					1	2	3	4
GOV	GOV1	The government will make every effort to protect my privacy from RFID abuse.	3.70	1.282	.635	-.084	.093	.094
α = .83	GOV2	The government will tell the truth about the risks I may encounter with RFID.	3.72	1.208	.928	.075	-.075	-.066
	GOV3	I trust the government to protect me from RFID abuse.	3.73	1.259	.784	-.024	.004	.090
RL	RL1	How likely is it that someone will use Residual RFID to steal your personal information?	4.93	1.209	-.015	.730	.139	.064
α = .91	RL2	How likely is it that your personal information will be stolen as a result of Residual RFID?	4.73	1.120	.039	.895	.002	-.061
	RL3	How likely is it that your privacy will be violated as a result of Residual RFID?	4.86	1.150	-.026	.970	-.053	.013
RH	RH1	How much harm could be done to you if someone broke into RFID databases containing your private personal information?	5.53	1.131	.049	-.041	.958	-.070
α = .92	RH2	How much harm could be done to you if an organization that employs RFID abused your information?	5.53	1.125	.007	.061	.883	.009
	RH3	How much harm could be done if consumers' personal information is stolen because of RFID?	5.67	1.200	-.063	.030	.815	.046
BI	BI1	I would prefer to purchase products from retailers that use RFID.	3.87	1.189	.096	-.007	.014	.760
α = .86	BI2	I would actively seek out products that use RFID.	3.48	1.206	-.036	.003	-.025	.825
	BI3	If given the choice between a RFID product and a non-RFID product, I would choose the product that uses RFID.	3.66	1.187	.030	.018	-.012	.692

** Extraction Method: Maximum Likelihood. Rotation Method: Promax with Kaiser Normalization. a Rotation converged in 5 iterations.*

Table 1: Rotated Factor Matrix, Cronbach Alpha and Descriptive Statistics

Results

As shown in Table 2, our sample consisted of 320 likely consumers of products with embedded Residual RFID tags. Approximately 53% of the subjects were female, 47% male. While the mean age, collected in categories, was in the upper 20, lower 30 range, we had a wide range of age groups from under 20 to over 70. To obtain the greatest possible dispersion of consumers, including those with and without technology familiarity, the research was conducted using a paper-based format as opposed to an online medium.

Respondents were encouraged to participate in the research study by entering a drawing for a gift certificate from any one of five restaurants.

The income of the respondents to the survey varied widely, from zero income university students to corporate executives, though most incomes were in the range of $20,000 to $50,000 annually. Respondents' familiarity with technology in general varied as well, from those comparatively unfamiliar to experts in various fields, with most respondents indicating they were at least somewhat familiar with technology. Many indicated at least some familiarity with RFID as well. It should be noted that approximately a third of the respondents were university students. Although they were not the primary target audience, they do represent a significant population that will be interacting with Residual RFID technology throughout their lives.

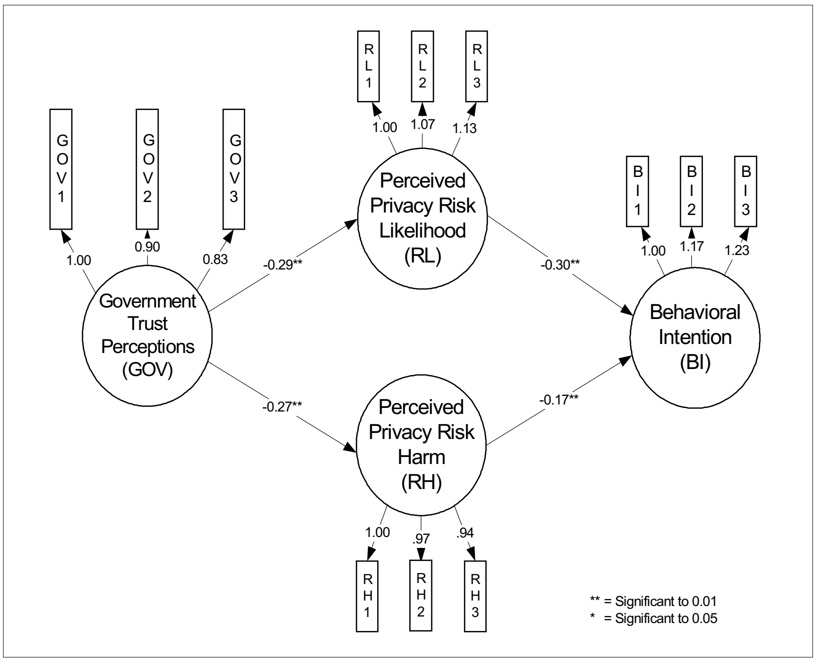

Figure 2. Results - Government trust perceptions, risk likelihood, risk harm

	N	Mean	Std. Dev	Percent Distribution						
Gender	320	0.47	0.5							
	N	Mean	Std. Dev	< 20	20-29	30-39	40-49	50-59	60-69	>70
Age	320	2.65	1.424	12.8%	57.2%	3.4%	1.6%	10.9%	2.8%	1.6%
	N	Mean	Std. Dev	<20%	20-40K	4060K	6-080K	80-100K	100-120K	>120K
Income	296	2.84	2.117	42.9%	12.2%	14.5%	7.4%	6.8%	4.1%	12.2%
	N	Mean	Std. Dev	No Knowledge	Very Unfamiliar	Somewhat familiar	Undecided	Somewhat Familiar	Very Familiar	Expert
Tech Familiarity	319	4.27	1.482	6.2%	9.4%	16.3%	6.3%	45-6%	14.7%	1.6%
	307	3.08	1.75	29.0%	Ried Familiarity 14.7%	16.0%	6.8%	26.7%	6.8%	0.0%

Table 2 : Demographics

Based upon the results presented in Table 1 and Figure 2 above, we can conclusively say that all four of our hypotheses are validated. Privacy risk likelihood and privacy risk harm both have direct and negative impacts on consumers' intentions to use products with Residual RFIDs. Likewise, trust in government's ability to protect consumers from abuse and misuse alleviates said risks. All relationships portrayed in Figure 2 are supported and significant. Figure 2 and Table 3 present the path coefficients and the strength of the path for each hypothesis. All paths are supported at the .05 significance level, supporting our hypotheses. Likewise the overall fit of the model, described in Table 4, supports the complete model. The overall model, therefore, has a good fit.

		Effect	Supported
H1	Consumer perceptions of the potential for harm due to privacy risk will have a negative impact on their intentions to accept Residual RFID technology.	-0.17**	Yes
H2	Consumer perceptions of the likelihood of a privacy breach occurring will have a negative impact on their intentions to accept Residual RFID technology.	-0.30**	Yes
H3	Consumer trust in the government will reduce their perceptions of perceived privacy risk likelihood.	-0.29**	Yes
H4	Consumer trust in the government will reduce their perceptions of perceived privacy risk harm.	-0.27**	Yes

** = Significant to 0.01 * = Significant to 0.05

Table 3: Hypotheses Summary

Measure	Abbreviation	Fit Statistics Fit Disabled Tags
Chi-square	X^2	326.52
Degrees of freedom	Df	50
Discrepancy/df	/df	6.53
Incremental fit index	IFI	0.90
Comparative fit index	CFI	0.90
Root mean square error of approximation	RMSEA	0.12

Table 4: Fit Statistics for Research Model

Discussion and Conclusions

The study identified four significant factors. The first factor was Trust in the Government, next factor was Perceived Risk Likelihood, the third factor was Perceived Risk Harm, and the last factor was the Behavioural Intention to Use Products with Residual RFID Tags. These factors significantly impact each other as hypothesized in the model as depicted in Figure 2. The consumer perceptions of the likelihood of a privacy abuse occurring showed a strong negative impact on their willingness to use product with residual RFID tags. In addition, the level of harm consumers believed could happen to them in the event of abuse also had a strong negative impact on their willingness to use products with residual RFID tags.

Figure 2 demonstrates that consumers' perceptions of privacy risk likelihood have a direct and negative impact on their intentions to use products with Residual RFIDs. Likewise, consumers' perceptions of privacy risk harm have a direct and negative impact on their intentions to use products with Residual RFIDs. The magnitude of risk likelihood (-.30) is nearly double that of risk harm (-.17), suggesting that this may be a fruitful area to address in future research. While it may also be true that risk harm is becoming more difficult to mitigate under the constructs of our current information society, it is nevertheless becoming increasingly important to do so, regardless of how challenging the problem may be. In contrast, the magnitude of the effect of governmental trust on privacy risk (-.29) is almost identical to the effect on privacy risk harm (-.27). Those consumers who trust the government to act in the their best interests — that is, protect them from abuse, tell the truth about the risks associated with RFID technology, and make every effort to protect consumer privacy — have lower degrees of risk likelihood and risk harm perceptions than other consumers and are therefore, according to the model presented, more likely to use and adopt RFID technologies.

Consumers expect the government to be integrally involved in the legislation and regulation of technology, particularly where privacy and security are concerned. By building trust with consumers, government has the ability to mitigate the risks associated with the adoption of RFID technologies and to act as a third party to overcome those risk perceptions. Without positive governmental involvement, consumers are more likely to be impacted by the inherit privacy and security risks associated with the technology.

The study also showed that the government may have the ability to mitigate the effect of these risk perception taking appropriate steps to protect privacy from abuse through residual RFID tags. Those respondents that believed that the government will tell the truth about the risk they may encounter with residual RFID tags were more likely to accept the products. Also, the respondents who believed the government will take steps to protect the consumers were more likely to use the products in spite of the risk.

Without the mitigations government can provide, there is still a significant risk of consumer backlash based on the perceptions of privacy and security risk likelihood and harm. Therefore, breaking risk into its components of risk harm and risk likelihood shows it is a theoretically and empirically supported approach to conceptualize overall risk concerns in future studies.

Some of the initiatives that the government could undertake include the following: controlling the dissemination of RFID reading equipment, enforcing strict penalties for the abuse of this technology and setting standards of behaviour for a company's use of this technology. However, in the USA what we really need to be effective is to move past Congress passing patchwork legislation to a comprehensive view of privacy in general similar to that adopted in Europe. Not that we need to adopt the same standards, but that we adopt and agree to live by a set of principles that guide specific types of actions on a broad scale for multiple technological platforms rather then a piecemeal approach with different rules for different technologies. This would likely give consumers a better understanding of what to expect across a range of technologies and lead to a greater degree of trust that their rights, as defined by those principles, would be respected.

Finally, industry could greatly benefit through government intervention in protecting consumers from these potential risks. This would allow businesses to fully adopt RFID tags throughout their entire supply chain including their use after consumers have purchased the products; allowing businesses to achieve more of the potential benefits of this technology.

The potential benefits include better customer relationship management (CRM), more efficient reverse logistics, a more personalized marketing and service approach, improving inventory shrinkage and management, improving quality using information pertaining to the entire product life cycle, etc.

Limitations & future research

This study looks at general trust in the government and its ability to ensure that the risks are contained. Future studies might consider the effect of general trust in individuals as opposed to governmental bodies, while other studies might extend this stream of research by looking at specific actions that either the government or a coalition of governments could take and how consumers might react to such actions. Studies might also include consumer perceptions regarding political viewpoints and which of the several domestic parties might best be equipped to contain the risks associated with Residual RFID technologies. The inclusion of questions that ask respondents how often they shop at specific places (some known to use RFIDs and other non-RFID organizations) will be helpful in demonstrating a difference between behavioral intention and actual performance. Whatever the motivation or direction, it is clear that positive governmental involvement is the key to alleviating consumer perceptions of privacy risk likelihood and privacy risk harm, and is a field of study to be explored further.

References

Abramson, L. (2004), “Radio Frequency IDs”, National Public Radio (NPR), Morning Edition, 26 March 2004. <http://www.npr.org/templates/story/story.php?storyId=1792847>

Attaran, M. (2006), “RFID pays off .” Industrial Engineer, 38 (9): 46.

Battacherjee, A. (2002), “Individual Trust in Online Firms: Scale Development and Initial Test”, Journal of Management Information Systems, 19 (1): 213-243.

Cazier, J. A. (2006), Value Congruence and Trust Online: Their Impact on Privacy and Price Premiums, Cambria Press, Youngstown, New York.

Cazier, J. A. (2007), “Projecting Values Online: An E-Tailing Goldmine?”, International Journal of Electronic Marketing and Retailing, 1 (3): 217-235.

Cazier, J. A., Shao, B. B. M. and St. Louis, R. D. (2006), “E-business differentiation through value-based trust”, Information and Management, 43: 718-727.

Cazier, J. A., Wilson, E. and Medlin, B. D. (2007), “The Role of Privacy Risk in IT Acceptance: An Empirical Study” forthcoming in International Journal of Information Security and Privacy.

Conca, C., Medlin, D. and Dave, D. (2005), “Technology-based security threats: taxonomy of sources, targets and a process model of alleviation,” International Journal Information Technology Management, 4 (2) 166-177.

Dinev, T. and Hart, P. (2006), “An Extended Privacy Calculus Model for E-Commerce Transactions”, Information Systems Research, 17 (1) 61-80.

Eckfeldt, B. (2005), “What Does RFID do for the Consumer?”, Communications of the ACM, 48 (9): 77-79.

Featherman, M. S., Valacich, J. S. and Wells, J. D. (2006), “Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters”, Information Systems Journal, 16: 107-134.

Garfinkel, R., Gopal, R. and Goes, P. (2002), “Privacy Protection of Binary Confidential Data Against Deterministic, Stochastic, and Insider Threat”, Management Science, 48 (6): 749-764.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999), “Building consumer trust online”, Communications of the ACM, 42 (4): 80-86.

IBM (2006), 'IBM Survey: Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime: Changing Nature of Crime Leads to Significant Behavior-Changes', IBM.com, 27 January 2006.

Juels, A. (2005), “RFID Security and Privacy: A Research Survey”, RSA Laboratories, 1-19.

Mayer, R. C., Davis, J. H, and Schoorman, F. D. (1995), “An integrative model of organizational trust,” Academy of Management Review, 30 (3): 709-734.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002), “Developing and Validating Trust Measures for e-Commerce: An Integrative Typology,” Information Systems Research, 13 (3): 334359.

Milne, G. R. and Culnan, M. J. (2004), “Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices”, Journal of Interactive Marketing, 18 (3): 15-29.

Raab, C. D., and Bennett, C. J. (1998), “The Distribution of Privacy Risks: Who Needs Protection?” The Information Society, 14: 263-274.

Spiekermann, S. and Ziekow, H. (2005), “RFID: A 7-Point Plan to Ensure Privacy”, Thirteenth European Conference on Information Systems, Regensburg, Germany, May 26-28.

Straub, D. W. and Welke, R. J. (1998), “Coping with systems risk: Security planning models for management decision making,” MIS Quarterly, 22 (4): 441-469.

Sweat, J. (2000), “Privacy Paradox: Constomers Want Control and Coupons,” Informationweek, April 2000, 781: 52.

Wyld, D. C. (2006), “RFID 101: the next big thing for management,” Management Research News, 29 (4): 154.

Appendix A Survey Introduction

Many experts predict that in the future, nearly every product manufactured, bought and/or sold will have a tiny tag that can remotely and uniquely identify that individual item. Any person or business with a scanner may be able to know the item type, price, where it was made, sold, purchased and resold by reading a small RFID tag.

Radio frequency identification (RFID) tags are currently being deployed in the supply chains of many organizations. These tags have the potential to bring many benefits to organizations that use them. However, many of these tags can remain active after they leave the organization, broadcasting their identities and histories to anyone with a scanner and link to the proper database. These left over tags, installed to help the supply chain, but not removed after the purchase, are referred to as residual RFIDS.

In the future, residual RFID tags have a tremendous amount of potential to both help and harm consumers. A few examples are listed below.

Possible Benefits

- Residual RFID tags may make it possible to return items without a receipt.
- Residual RFID tags may make it easier to track and find stolen goods.
- Residual RFID tags may make it easier to track and fulfil warranties and repairs.

Possible Liabilities

- Companies could scan for residual RFID tags in order to target marketing to individuals.
- Thieves could scan for residual RFID tags in order to case out potential victims.
- Residual RFID tags could give out a tremendous amount of private information about individuals.

Appendix B - Survey Questions

Please read each of the following questions and respond by checking the box beneath the answer that best matches your opinion or situation.

	Under 20	20 - 29	30 - 39	40 - 49	50 - 59	50 - 69	70+
1. Please select your age:							
	Male	Female					
2. Gender							
	Under $20,000	$20,000 - $39,999	$40,000 - $59,999	$60,000 - $79,999	$80,000 - $99,999	$100,000 - $119,999	$120,000+
3. Please select your annual household income:							
	No Knowledge	Very Unfamiliar	Somewhat Unfamiliar	Undecided	Somewhat Familiar	Very Familiar	Expert
4. In general, how would you rate your familiarity with information technologies?							
5. How familiar are you with RFID?							

		Very Strongly Disagree	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Very Strongly Agree
6.	The government will make every effort to protect my privacy from RFID abuse.							
7.	The government will tell the truth about the risks I may encounter with RFID.							
8.	I trust the government to protect me from RFID abuse.							
9.	I would prefer to purchase products from retailers that use RFID.							
10.	I would actively seek out products that use RFID.							
11.	If given the choice between a RFID product and a non-RFID product, I would choose the product that uses RFID.							

	Nearly Impossible	Very Unlikely	Unlikely	Neutral	Likely	Very Likely	Almost Certain
12. How likely is it that someone will use residual RFID to steal your personal information?							
13. How likely is it that your personal information will be stolen as a result of residual RFID?							
14. How likely is it that your privacy will be violated as a result of residual RFID?							
	No Harm At All	Very Little Harm	Little Harm	Undecided	Some Harm	Much Harm	Severe Harm
15. How much harm could be done to you if someone broke into RFID databases containing your private personal information?							
16. How much harm could be done to you if an organization that employs RFID abused your information?							
17. How much harm could be done if consumers' personal information is stolen because of RFID?							

Author Biographies

Andrew S. Jensen is a PhD student in the Department of Computer Science at the University of North Carolina at Charlotte. He currently works in the Charlotte Visualization Center, where his research interests include high-resolution display systems, textual analytics and RFID security applications. His research has been presented at the Southeast Institute for Operations Research and the Management Sciences and the Americas Conference for Information Systems.

Joseph A. Cazier is an Assistant Professor in the Department of Computer Information Systems at Appalachian State University. He has a keen interest in information ethics, trust and security and conducts research in this area. He is also very interested in international technology issues, has lived in Europe and South America and is bilingual (English/Spanish). He has published in journals such as Information Systems Security, EDPACS - the EDP Audit, Control, and Security Newsletter, International Journal of Networking and Virtual Organisations, International Journal of Electronic Marketing and Retailing, International Journal of Information Security and Privacy, and the International Journal of Healthcare Information Systems and Informatics.

Dinesh S. Dave is a professor in the Department of Computer Information Systems at Appalachian State University. He served as a director of the Center for Business Research in the John A. Walker College of Business. His teaching, research, and consulting activities have been in production and operations management, quantitative methods and techniques, business statistics, and information technology. He has published in journals such as Decision Sciences, International Journal of Business Performance Management, International Journal of Management, International Journal of Computer Applications in Technology, International Journal of Information Technology Management, Computers & Industrial Engineering, Journal of Applied Business Research, Information & Management, Communication of the ACM, International Journal of Production Economics, Journal of Computer Information Systems, Journal of Health Marketing Quarterly, Tourism Economics, and others.