The Impact of Consumer Perceptions of Information Privacy and Security Risks on the Adoption of Residual RFID Technologies

Joseph A. Cazier

Department of Computer Information Systems

Appalachian State University

cazierja@appstate.edu

Andrew S. Jensen

Department of Computer Science

University of North Carolina at Charlotte

Dinesh S. Dave

Department of Computer Information Systems

Appalachian State University

Abstract:

In today's global competitive environment, organizations face a variety of challenges. Continuous improvement in organizational efficiencies and improving the entire supply chain are necessary to stay competitive. Many organizations are adopting radio frequency identification technologies (RFID) as part of their information supply chains. These technologies provide many benefits to the organizations that use them. However, how these technologies affect the consumer and their willingness to adopt the technology is often overlooked.

Many of these RFID tags remain active after the consumers purchase them. These RFID tags, placed in a product for one purpose and left in the product after the tags have served their purpose, are Residual RFIDs. Residual RFID technology can have many positive and negative effects on consumers' willingness to buy and use products containing RFID, and thus, on the business's ability to sell products containing RFID. If consumers refuse to buy products with Residual RFID tags in them, the business harm is greater than the business benefit, regardless of any gain in supply chain efficiency.

In this study, we outline some of the advantages and disadvantages of Residual RFID from the consumer perspective, then follow up with an in depth survey and analysis of consumer perceptions. Using structural equation modeling (SEM) we demonstrate that consumers' perceptions of privacy risk likelihood and privacy risk harm negatively impact their intentions to use this technology. The implications of these findings need to be considered before the pending implementation of Residual RFID technologies in the supply chain on a mass scale.

Keywords: Privacy, Privacy Risk, Security Risk, RFID, Residual RFID, Technology Adoption, Secure Supply Chain.

This box will only be used for peer-reviewed papers.

I. INTRODUCTION

In the near future, almost every new product available to consumers will have a small tag that can remotely and uniquely identify that individual item. Any person or business with an appropriate scanner and information may determine the item type, price, place of origin, place of purchase, and other details about a given product by reading small radio frequency identification (RFID) tags. The current RFID market is approximately a $3 billion enterprise with several million tags in circulation. That market is projected to grow by more than 800 percent, to over $25 billion with tens of trillions of tags in circulation by 2015 [Wyld, 2006].

Many organizations are currently deploying RFID tags in their supply chains. While these tags have the potential to bring significant benefits to the organizations that use them, many of these tags remain in the product after they leave the organization, their identities and histories readily available 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 Residual RFIDs.

The two different types of RFID tags, active and passive, offer their own differing benefits and liabilities to consumers. A power source drives active RFID tags, making them capable of broadcasting their own signal over varying distances, depending upon the potency of their power source and range of their frequency. While these tags may be extremely useful in certain military and other applications, they offer only limited practicality for consumer use, as the cost to produce such tags renders them impractical in a consumer environment.

Passive tags have no power source and are relatively inexpensive to produce. These economical tags are most likely to be found in consumer goods. Lacking a power source, these tags are incapable of broadcasting their own signal. This lack of broadcast ability initially sounds like a benefit in terms of consumer privacy, but the lack of a power source 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 bus or train terminal, airport security checkpoint, retail location, restaurant, or even as the result of a handheld scanner used unobtrusively at any time or place. These passive tags, still present but no longer providing a realized retail benefit, are Residual RFID tags.

The adoption of RFID technologies is on the rise in many 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. 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 (e.g. EZ-Pass), law enforcement, and the U.S. Department of Defense [Attaran, 2006].

RFID technology is a part of our lives, whether we approve of the technology or not. Many of its applications have very little effect on the average consumer (e.g. what can the consumer say about RFID in military applications for the Department of Defense?), but the integration of this technology in other aspects of consumers' lives raises certain concerns.

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

The threat to individual privacy that such technology raises is of particular concern. Consumers have called upon the developers and users of RFID technology to implement precautions to limit the privacy risk issues. Others call upon government to legislate the implementation and use of the technology. In March 2008, the governor of Washington State signed into law a bill that declares the use of RFID technology to scan people's IDs without their knowledge or consent for fraudulent or other illegal purposes a class C felony [Gaudin, 2008]. Such legislation may eventually prove effective, but 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.

It is our suggestion that consumers' perceptions of privacy risk associated with RFID technology, as well as their perceptions of the technology's overall usefulness, will directly influence their intentions to adopt or accept the technology. We begin this paper with a discussion of prior research regarding RFID and its impact on consumers. We specifically address consumer benefits and liabilities (usefulness), as well as the impact of privacy risk on technology adoptions. We discuss the basis for our research, a desire to ascertain the perceptions and usage

intentions of individuals toward organizations and products that develop and/or employ Residual RFID technology, and the development of our hypotheses. We follow up with a discussion of our pilot studies and our data collection method, consisting primarily of an in-depth survey of consumer perceptions regarding the potential wide-scale adoption of RFID technologies. Finally, we present the results of our findings and evaluate the validity of our hypotheses. We were unable to find any similar studies looking at privacy risk harm and likelihood related to Residual RFID tags, indicating that this study makes an important new contribution to the literature.

II. THEORY DEVELOPMENT

Benefits of Residual RFID for Consumers

The benefits of RFID technology in business and governmental applications have been the focus of considerable research, as have the security and privacy risks associated with the technology for consumers. The benefits of RFID technology for consumers, however, are often overlooked. Yet it is imperative consumers understand that there are legitimate consumer benefits associated with the use of this 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 by providing privacy policies to explain what data is being collected and how it is being used [Eckfeldt, 2005]. It is a difficult task for retailers and RFID developers to limit the privacy risk for consumers. 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

Since the purpose of RFID technology in the supply chain is to enhance the productivity and efficiency of the supply chain, its usefulness, in theory, ends when the product to which a RFID tag is assigned leaves the supply chain and enters the consumer domain. Residual RFIDs, those that have completed their jobs in the supply chain, may still offer certain benefits for consumers beyond the retail experience. Examples of these benefits can be easily evaluated under Eckfeldt's headings.

Peace of Mind

Eckfeldt [2005] explains that the RFID applications with the greatest success in terms of adoption and proliferation involve security. It is interesting to note that the very ability that has been the source of so much public outcry against the technology—it's potential ability to positively identify and track individuals—is 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 people—persons for which they have at least an element of trust—have access to the sensitive data collected by such systems. When tracking lacks any obvious consumer security benefit and delivers only marketing information for retailers, the risk/reward equation does not add up for consumers [Eckfeldt, 2005].

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 could potentially 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 purchase merchandise by rolling shopping carts past point-of-sale terminals. These terminals would compute the total amount and perhaps even charge RFID-enabled payment devices. Another possible application of RFID technology in customer relationship management 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 overall customer service and the consumer shopping experience. Casinos, such as the Wynn Las Vegas resort, are using RFID to fight fraud and provide guests with easy access to house credit. Delta Air Lines uses RFID tracking systems to ensure that baggage arrives on time and 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?

In other applications, insurance companies may be able to quickly log complete inventories of a person's belongings for home insurance purposes. Rather than relying on the lengthy and inadequate process of hand-written lists and estimated replacement costs, agents might simply scan a home and catalog the results based upon the RFID tags 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, both in-store and out, based upon the 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. Through the use of data mining techniques, additional information can be gained from registered (RFID) tracks [Spiekermann and Ziekow, 2005]. Analysing 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' (lives)" [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 (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).

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 effect on consumers' willingness to purchase goods containing RFID technology.

Potential Solutions

Recognizing that while RFID-based supply chains provide convenience, efficiency, and productivity gains for businesses, Gao et al. [2004] point out that these systems also create new risks to security and privacy. The authors suggest an approach that deals with randomized read access control in order to prevent hostile tracking and man-in-the-middle attack. RFID tags pose a potentially widespread threat to consumer privacy. The RFID tag uniquely identifies each consumer product or item of merchandise and contains the manufacturer and product type as well, creating a potential privacy problem. Many researchers such as Juels et al. [2003], Juels and Pappu [2003], McCullaugh [2003], Sarma et al. [2002], Emigh [2004], Gao et al. [2004], Zhang and Li [2006], Karjoth and Moskowitz [2005], and Markelevich and Bell [2006] have all raised the privacy issue.

Juels et al. [2003] propose the use of "selective blocking" by "blocker tags" as a way of protecting consumers from unwanted scanning of RFID tags attached to items. The study conducted by Karjoth and Moskowitz [2005] focuses on technical solutions for consumer privacy in retail. The researchers propose to provide RFID tag structures that permit a consumer to disable a tag by mechanically altering the tag in such a way that inhibits the ability of a reader to interrogate the RFID tag by wireless means. The authors refer to this procedure as "clipped tags," where the body or chip separates from the head or antenna. Clipped tags offer a simple and practical privacy-enhancing techniques for RFID in retail, and deactivation can be performed in an easy, reliable, and verifiable way. The authors further suggest that if deactivation of the tag is performed by the consumer, then no special devices are needed by retailers.

Impact of Privacy Risk on Technology Adoptions

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 uses RFID technology.

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]. 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 concern 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].

Hoffman et al. [1999] showed 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 accessible, 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 of whether to disclose or not disclose information 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.

In 2004 Ernst and Young conducted a survey of 1000 internet users on a variety of questions related to RFID technology. The results of that study showed that only 23% of surveyed consumers had heard of RFID. Responses to the survey questions were quite favorable, at least until privacy issues were addressed [Juban and Wyld, 2004].

Table 1. Ernst and Young Survey [Juban and Wyld, 2004]		

Survey Question	Initial Response	After addressing privacy issues
Would definitely buy RFID enabled products	**55%**	29%
Would be somewhat willing to buy RFID enabled products	28%	26%
Would definitely NOT buy RFID enabled products	17%	**45%**

Note the change in response after privacy issues were introduced to the survey respondents. The results of the survey showed that the greatest concerns to consumers regarding RFID technology were related to consumer privacy and security [Juban and Wyld, 2004]. Such results indicate that the risk of a privacy breach might have a significant effect on consumers' willingness to adopt RFID technology.

Extending the Technology Acceptance Model (TAM)

We frame this paper as an extension of the Technology Acceptance Model (TAM) [Davis, Bagozzi, and Warshaw, 1989]. TAM is a derivation of the Theory of Reasoned Action (TRA) [Ajzen and Fishbein, 1980], customized for the prediction of IT adoption and use. TAM suggests that IT use can be predicted by its perceived usefulness (PU) and perceived ease of use (PEOU), mediated by a subject's behavioral intention (BI). All factors in the TAM equation, except IT use, are therefore measured as one's perceptions regarding one's beliefs and intentions.

In practice, TAM has proven to be both powerful and parsimonious [Cazier et al., 2007]. Lee, Kozar, and Larsen [2003], for example, report overwhelming support for the central relationships of TAM. Among the studies which assessed each specific relationship, 88% find PU influences BI, 71% find PEOU influences BI, 84% find PEOU influences PU, and 87% find BI influences IT use. In addition, Lee et al. describe 25 external factors that have been studied as contributors to TAM, ranging from measures of voluntariness of use to users' prior experiences with the technology [Cazier et al., 2007]. None of the external factors described in their study, however, addresses the security or privacy risks of technology use, which are of particular importance to consumers considering the acceptance of RFID technology.

It is important to note that although attitude was included in the initial development of TAM, most subsequent studies do not include an attitude measure [Lee et al., 2003], and one will not be considered here.

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

1) the perceived usefulness and ease of use of RFID technology as it relates to consumers

2) the perceived likelihood of a consumer privacy breach occurring as a result of RFID technology use

3) the perceived harm such a privacy breach might incur

Why TAM?

TAM is a well studied construct with a long history of use and application. This is one of the reasons why it makes sense to use TAM in this type of research. The reason it has a long history with so many studies associated with it is because it is a good model and provides useful predictive power in a variety of contexts. TAM therefore serves as a useful baseline for comparison to prior work and helps us to build on a cumulative tradition as encouraged by some of the earlier fathers of our discipline, such as Keen [1980].

This cumulative tradition and familiarity is especially important to this study because we are moving into a new context with a different type of technology and audience. Most of the early TAM research was applied in the context of a captive audience (i.e. employees) accepting an information system commissioned by the company they worked for. Later researchers expanded this to shed light on some of the voluntary systems, such as e-commerce, that provided intermittent use. However, this was a technology that consumers actively used.

We are now expanding this model again, to gauge consumer acceptance of a passive technology (Residual RFID tags) as opposed to an active technology, such as seeking out and searching a website. The expansion of this technology to a passive context, accepting a tracking technology into our daily lives without necessarily seeking it out, is an important new contribution to and from this model that helps establish a cumulative tradition and builds upon what is useful while still learning something new from it.

In addition, by examining both positive and negative utility, the model we use in this paper builds upon TAM in a way that goes beyond what most models have done in the past. Traditionally, TAM has explored numerous positive aspects of things that could be done to increase the chances of users accepting an information system. However, relatively few models have explored both positive and negative utility. Positive utility constructs discuss things that can be done to help people accept and use a system. Negative utility looks at elements in a system, the risks involved in their use, and how these elements affect people's acceptance and use of a system. This is especially important as many people are beginning to abandon completing tasks online that they once performed due to the risks involved in those transactions, such as the 18% of Americans who indicated they stopped banking online due to this anxiety [IBM, 2006]. This exploration of negative utility with TAM provides new insight while building upon prior work.

The use of TAM in this context makes a significant and innovative contribution by looking at both positive and negative utility, allowing us to weight the relative importance of each, and by expanding a proven model to a passive

as opposed to active user context. Even though it is an old and familiar tool, TAM can, in some cases, still provide new insight and value, as in this context.

Perceived Privacy Risk

Heijden et al. [2003] determined that "perceived risk" directly influences an individual's attitude toward making online purchases. In fact, according to their study, the effect of risk on attitude toward online purchasing is an order of magnitude greater than the effects of both perceived ease of use and perceived usefulness. The "perceived risk" referred to in their research, however, is of a more general nature than the privacy risk we propose in this paper. Our research makes a significant contribution by focusing on privacy risk, particularly as it pertains to the acceptance of RFID technologies.

Our research further supports the premise of TAM and expands it to include perceived privacy risk. Our model of privacy risk follows the suggestion of Kim and Leem [2005] that risk involves two elements: 1) the probability of an event occurring and 2) a loss amount. Our 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 might 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, in conjunction with TAM, will directly influence consumer behavior regarding RFID acceptance and use.

Featherman and Pavlou [2003] also draw upon the theory of perceived risk, defining privacy risk as the "potential loss of control over personal information." Their study identifies the importance of expanding TAM by looking at negative utility factors to produce more in-depth results. The inclusion of negative utility factors in the model can provide a more realistic and complete picture of technology acceptance [Cazier et al., 2007]. Perceived privacy risk, as it pertains to our study, is a negative utility factor, and is therefore an important contribution to existing literature.

Perceived Privacy Risk Likelihood

Drennan et al. [2006] state that perception of risk is fundamental to the understanding of consumer concerns about privacy and the relationship that exists among the factors of privacy, risk, and behavioral intentions. While their study focused on consumer behavior in an e-commerce environment, we contend that the same analysis applies to consumers and their behavior concerning RFID technologies.

Risk likelihood is the perception of the 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

11

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 Privacy Risk 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 occuring. 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.

Hypotheses

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

H1: Perceived ease of use will have a positive impact on the perceived usefulness of RFID technology

We propose that the perceived ease of use of RFID systems in association with consumer benefits will have a positive effect on consumers' perceptions of the usefulness of Residual RFID. Technology that is easy to use is more likely to be used and to be percieved as useful as people can better visualize how it will be used in their daily lives to fill a need. This has been one of the founding components of technology acceptance since the inception of the Technology Acceptance Model (TAM). For consumers, who have a choice to purchase and use a product, as opposed to those in a corporate setting who are mandated to use it, ease of use may be even more important than in some of the early TAM research with mandated use, or less recreational use that was required for their job function.
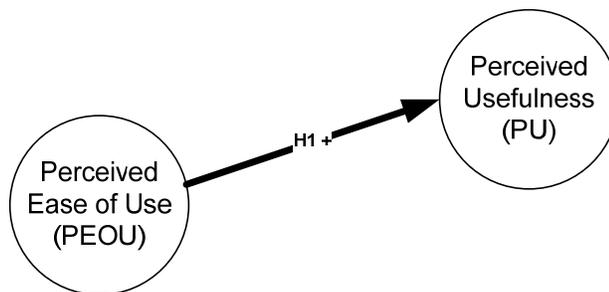

Figure 1: Model for H1

H2: Perceived usefulness will have a positive impact on intention to use products with RFID tags.

TAM also proposes that perceptions of the usefulness of Residual RFID will have a positive impact on consumers' intentions to accept the technology. If a technology is perceived to be useful, aiding consumers with tasks they must perform, they are more likely to want to use this technology. This link is also a hallmark of TAM included in the original Davis et al. [1989] study.
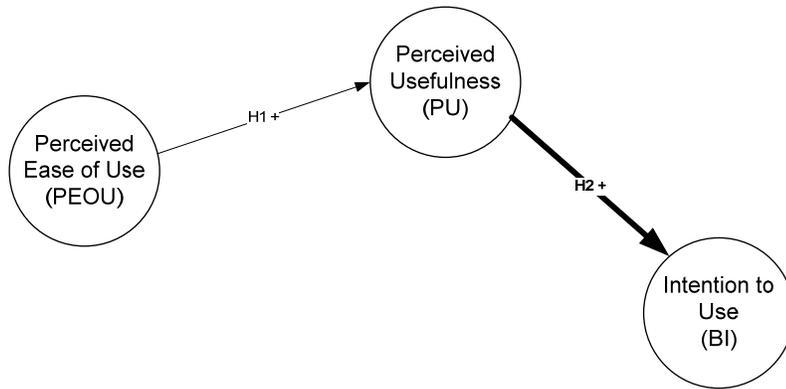
Figure 2: Model for H2

H3: Perceived ease of use will have a positive impact on intention to use products with RFID technology.

Likewise, we propose that the perceived ease of use of RFID systems in association with consumer benefits will have a positive impact on consumers' intentions to accept the technology. The more difficult a given technology is to use, the higher the level of cognitive or other effort is required. As effort level increases, consumer intentions to use the product drop as the expected benefit per unit of effort drops, making the effort/benefit payout less attractive.
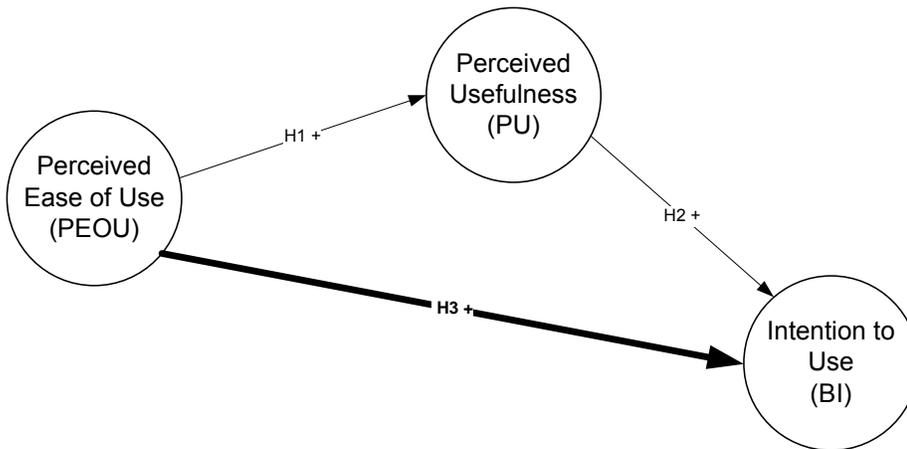
Figure 3: Model for H3

H4: Consumer perceptions of the potential for harm due to privacy risk will have a negative impact on their intentions to accept Residual RFID technology.

Risk is the probability of an event occurring multiplied by the loss or amount of harm that could occur if that loss is realized [Straub and Welke, 1998]. Our conceptualization of privacy risk follows the suggestion of Kim and Leem [2005] that risk involves two elements: the probability of an event occurring, which we denote as *perceived privacy*

risk likelihood, and a loss amount, which we denote as *perceived privacy risk harm*. Risk likelihood is the perception of probability that a privacy breach will occur. Risk harm is the perception of the level of damage that would occur in event of a privacy breach [Cazier et al., 2007].

Consumers' perceptions of privacy risk in regards to the potential for harm will have a negative impact on their intentions to accept Residual RFID technology. A number of researchers have studied monetary risks in online computing associated with e-commerce. Hoffman et al. [1999] find that when users perceived the online environment to be risky, they are less likely to purchase online. Labuschagne and Eloff write, "The major reason most people are still skeptical about electronic commerce is the perceived security risks associated with electronic transaction over the internet" [2000, pg 154]. Heijdenet al. [2003] found that the trust antecedent "perceived risk" directly influences an individual's attitude toward making online purchases.
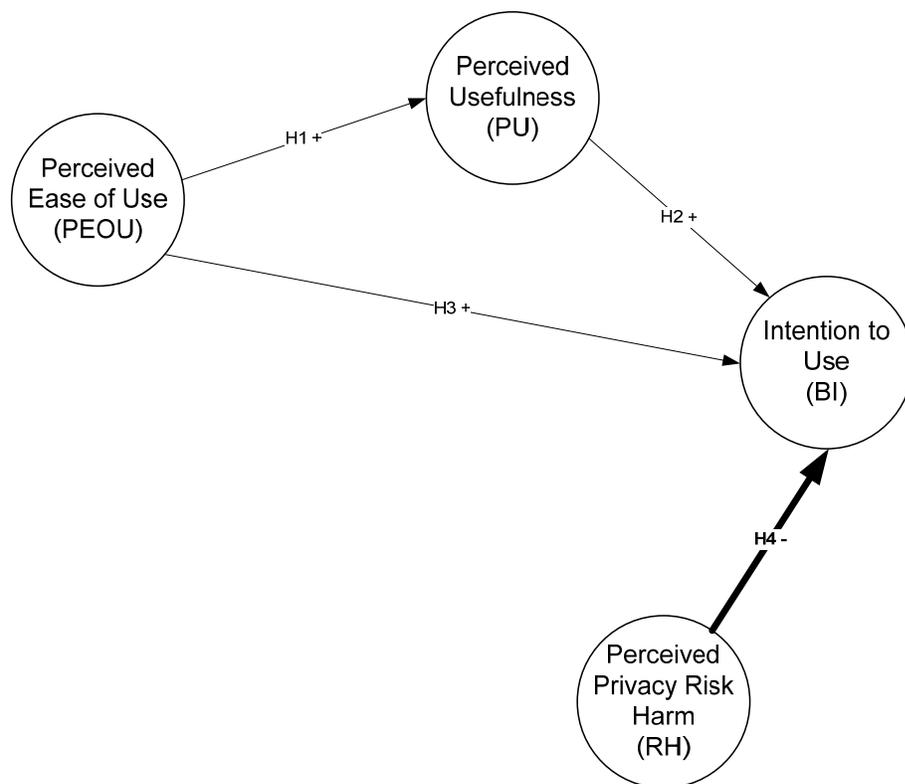

Figure 4: Model for H4

H5: Consumer perceptions of the likelihood of a privacy breach occurring will have a negative impact on their intentions to accept Residual RFID technology.

We propose that perceptions of privacy risk in regards to the likelihood of a privacy breach occurring will have a negative impact on consumers' intentions to accept Residual RFID technology. The greater the probability of a negative privacy event occuring, according to consumer perception, the more reluctant consumers will be to accept

this technology. Risk beliefs were found to have a very significant and direct impact on behavioral intentions [Malhotra et al. 2004], similar to those presented in our model.
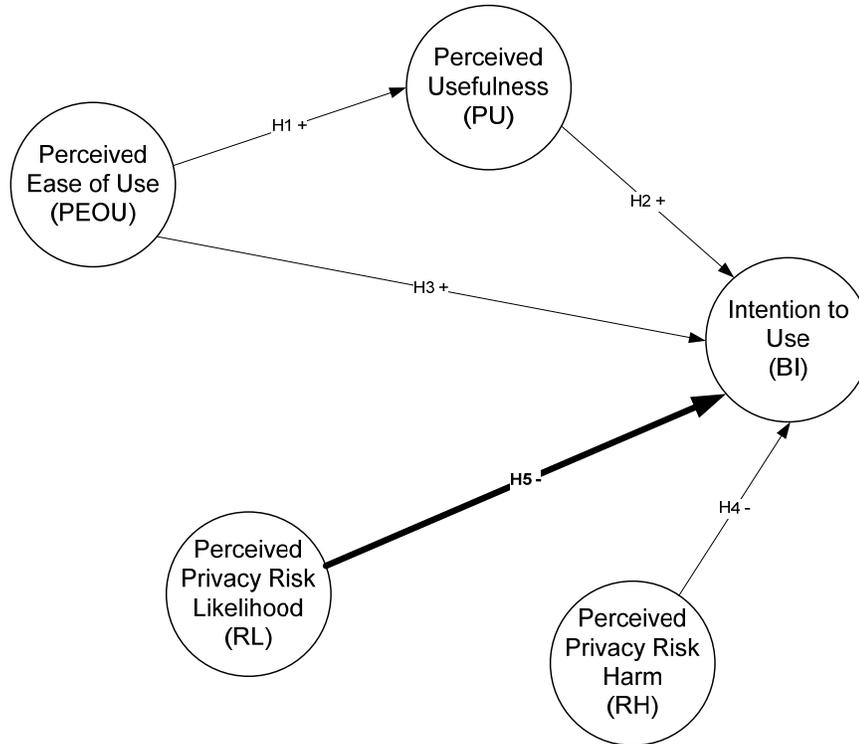

Figure 5: Model for H5

Hypotheses Summary

Our research model augments TAM with risk likelihood and risk harm (see Figure 1). Based on predominating findings in the TAM literature, we anticipate PEOU will have a positive effect on both PU and BI toward IT use, and we anticipate PU will have a positive effect on BI. We propose that perception of privacy risk will influence decisions toward RFID use. We anticipate BI toward RFID use will diminish where the perception of privacy risk is high and increase where the perception is low. In the present study, we operationalize privacy risk through its two elemental components, risk harm (RH) and risk likelihood (RL). We hypothesize that both factors will negatively influence BI.
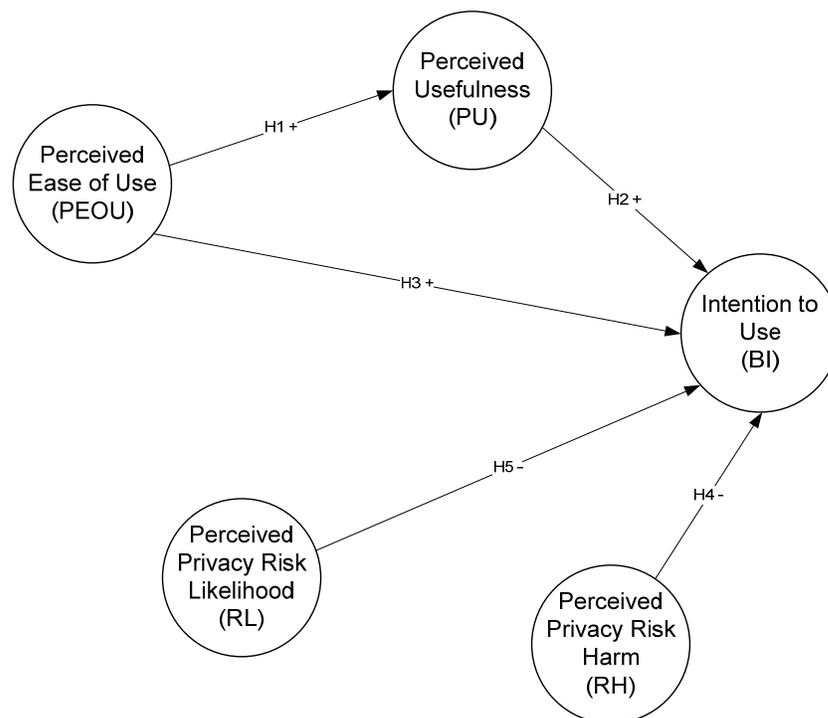
Figure 6: Model for all hypotheses combined

III. METHODOLOGY

We conducted the research methodology using a survey instrument 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 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, we presented a brief education piece to each subject prior to completing the survey, instructing subjects regarding the fundamental principles of Residual RFID technology. This survey introduction may be found at the start of appendix A.

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. In addition, we conducted two separate pilot studies in an effort to further validate and refine the selected questions before conducting the final survey and compiling the results.

Pilot Study

We first used an online version for a pilot study with a student sample. However, we were concerned about the generalilizability of this sample due to our student demographics and particularly their familiarity with technology compared to other consumers, especially older, less educated consumers that might be more of the typical Wal-Mart shopper (a company heavily pushing this technology).

To reach this audience, we developed a paper-based version of our instrument to try to capture this other demographic and allow those without easy computer access to respond. We accomplished this through a convenience sample where volunteers asked likely consumers of future products containing RFID to complete the survey from a variety of settings, and offered a prize through a drawing for one of the respondents. This method had the advantage of collecting a large sample of people of all demographics. However, this format does not give a traditional response rate that one might expect with a mail-in survey.

Our sample consisted of 320 likely consumers of products with embedded Residual RFID tags. All respondents were residents of the United States. Approximately 53% of the subjects were female, 47% male. While the mean age, collected in categories, was just under 30 years of age, we had a wide range of age groups from under 20 to over 70. Approximately 13% of the respondents were under 20, 57% of them were between 20 and 29, 3% were between 30 and 39, 12% were between 40 and 49, 11% were between 50 and 59, and 5% were over 60 years of age. Additionally, approximately 43% of the respondents' income was under $20,000, 12% earned between $20,000 and $39,999, 15% earned between $40,000 and $59,999, 7% earned between $60,000 and $79,999, 7% earned between $80,000 and $99,999, 4% earned between $100,000 and $119,999, and 12% earned $120,000 or greater.

The profession of the respondents included administrative assistant, accountant, healthcare, engineering, marketing and sales, management, manufacturing, computer and IT, graphic arts, entrepreneurship, academic, real estate, financial and banking, ministry, hospitality, and retired. Respondents' familiarity with RFID technologies provided interesting results. Approximately 29% of the respondents had absolutely no knowledge of the RFID technologies, 14% were very unfamiliar with these technologies, 16% were somewhat unfamiliar with these technologies, 7% had a neutral opinion of these technologies, 27% were somewhat familiar with these technologies, and 7% were very familiar with these technologies. None of the respondents claimed to be an expert with RFID technologies.

Scale Validation and Reliability

We constructed our final, paper-based survey instrument using questions from several validated existing surveys. We modified questions where necessary to coincide with the nature of Residual RFID technology and refined them through two separate pilot studies. (See appendix A for a copy of the survey instrument.) Nearly all items in the survey are 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 is stated. We stored all data collected during the study in a secure database for later statistical analysis.

With all factors loading, the constructs cleanly load on five separate factors, as shown in table 2. We selected the strongest three of the five questions in each construct to represent each factor. As shown in table 2, all Cronbach Alpha values are .8 or higher, factor loadings are routinely near .8 as well. This analysis demonstrates that there are five clear factors, all of which load cleanly on the latent constructs we are attempting to measure[1]. Results were analyzed using Lisrel version 8.2 for structural equation modeling.

Table 2. Rotated Factor Matrix									

Factor / Alpha	Items	Description	Mean	Std. Dev.	Factor Loadings*				
					1	2	3	4	5
PU	PU1	Using RFID technology will improve the quality of my shopping experience.	4.24	1.10	.003	-.116	.279	.254	**.825**
α = .83	PU2	RFID technology will improve the efficiency of my shopping experience.	4.29	1.11	.027	.005	.169	.282	**.866**
	PU3	The widespread adoption of this technology will ultimately lead to lower prices.	3.88	1.20	-.127	.029	.311	.088	**.689**
PEOU	PEOU1	Residual RFID will make returning purchases easier.	4.85	.96	.107	.045	.027	**.860**	.150
α = .81	PEOU2	Tracking stolen products will be made easier through Residual RFID.	5.00	.96	.154	.033	.138	**.865**	.103
	PEOU3	Residual RFID will make filing insurance claims easier.	4.58	.99	.001	.001	.095	**.727**	.310
RL	RL1	How likely is it that someone will use Residual RFID to steal your personal information?	4.92	1.15	.309	**.865**	-.129	.116	.006
α = .94	RL2	How likely is it that your personal information will be stolen as a result of Residual RFID?	4.73	1.12	.257	**.903**	-.158	.000	.000
	RL3	How likely is it that your privacy will be violated as a result of Residual RFID?	4.86	1.15	.236	**.888**	-.221	.001	.003
RH	RH1	How much harm could be done to you if someone broke into RFID databases containing your private personal information?	5.53	1.13	**.913**	.227	-.106	.048	.003
α = .92	RH2	How much harm could be done to you if an organization that employs RFID abused your information?	5.53	1.13	**.886**	.287	.007	.049	.009
	RH3	How much harm could be done if consumers' personal information is stolen because of RFID?	5.67	1.20	**.859**	.238	-.103	.135	.004
BI	BI1	I would prefer to purchase products from retailers that use RFID.	3.87	1.19	.007	-.212	**.737**	.213	.299
α = .85	BI2	I would actively seek out products that use RFID.	3.48	1.21	-.160	-.124	**.854**	.006	.246
	BI3	If given the choice between a RFID product	3.66	1.19	-.123	-.195	**.843**	.101	.214

[1] Conducted using unconstrained maximum likelihood extraction and varimax rotation.

		and a non-RFID product, I would choose the product that uses RFID.								

IV. RESULTS

Enabled Residual Tags

The results of this research study support TAM on all three constructs: 1) perceived ease of use has a reasonable impact on perceived usefulness, 2) perceived ease of use has a reasonable impact on behavioral intentions and 3) perceived usefulness has a reasonable impact on behavioral intentions. In addition, and most noteworthy, our modified TAM constructs are supported as well. Privacy risk likelihood has a significant and negative impact on behavioral intentions, close in significance to the impact of perceived usefulness and perceived ease of use, validating the importance of this construct. Likewise, privacy risk harm also has a significant negative impact on behavioral intention. This validates our five hypotheses, as shown in table 3 below.

Table 3. Hypotheses Summary for Enabled Tags			
Hypothesis	Description	Effect – Enabled Tags	Supported
H1	PEOU will have a positive impact on PU.	0.57	Yes
H2	PU will have a positive impact on BI.	0.59	Yes
H3	PEOU will have a positive impact on BI.	0.38	Yes
H4	RL will have a negative impact on BI.	-0.46	Yes
H5	RH will have a negative impact on BI.	-0.15	Yes

Table 4 and figure 7 present the path coefficients and the strength of the path for each hypothesis. The data support all paths at the .05 significance level, supporting our hypothesis. Likewise, the overall fit of the model, described in table 4, supports the complete model. Most fit indices are in the .90 or higher range as recommend by Kelloway [1998] with the RMSEA below .10, also recommended by Kelloway [1998]. The overall model therefore has a good fit.

Table 4. Fit Statistics for Enabled Tag Model		
Fit Measure	Abbreviation	Fit Statistics – Active Tags
Chi-square	χ^2	310.78
Degrees of freedom	Df	85.00
Discrepancy/df	χ^2/df	0.65
Goodness of fit index	GFI	0.89
Normed fit index	NFI	0.91
Relative fit index	RFI	0.89
Incremental fit index	IFI	0.93
Comparative fit index	CFI	0.93
Root mean square error of approximation	RMSEA	0.087
Root mean square residual	RMR	0.20

Adjusted Goodness of fit index	AGFI	0.85
Squared multiple correlations for PU	SMC/R^2	0.52
Squared multiple correlations for BI	SMC/R^2	0.28

RMSEA = .087
NFI   = .91
PNFI   = .74
RFI   = .89

** = Significant to 0.01
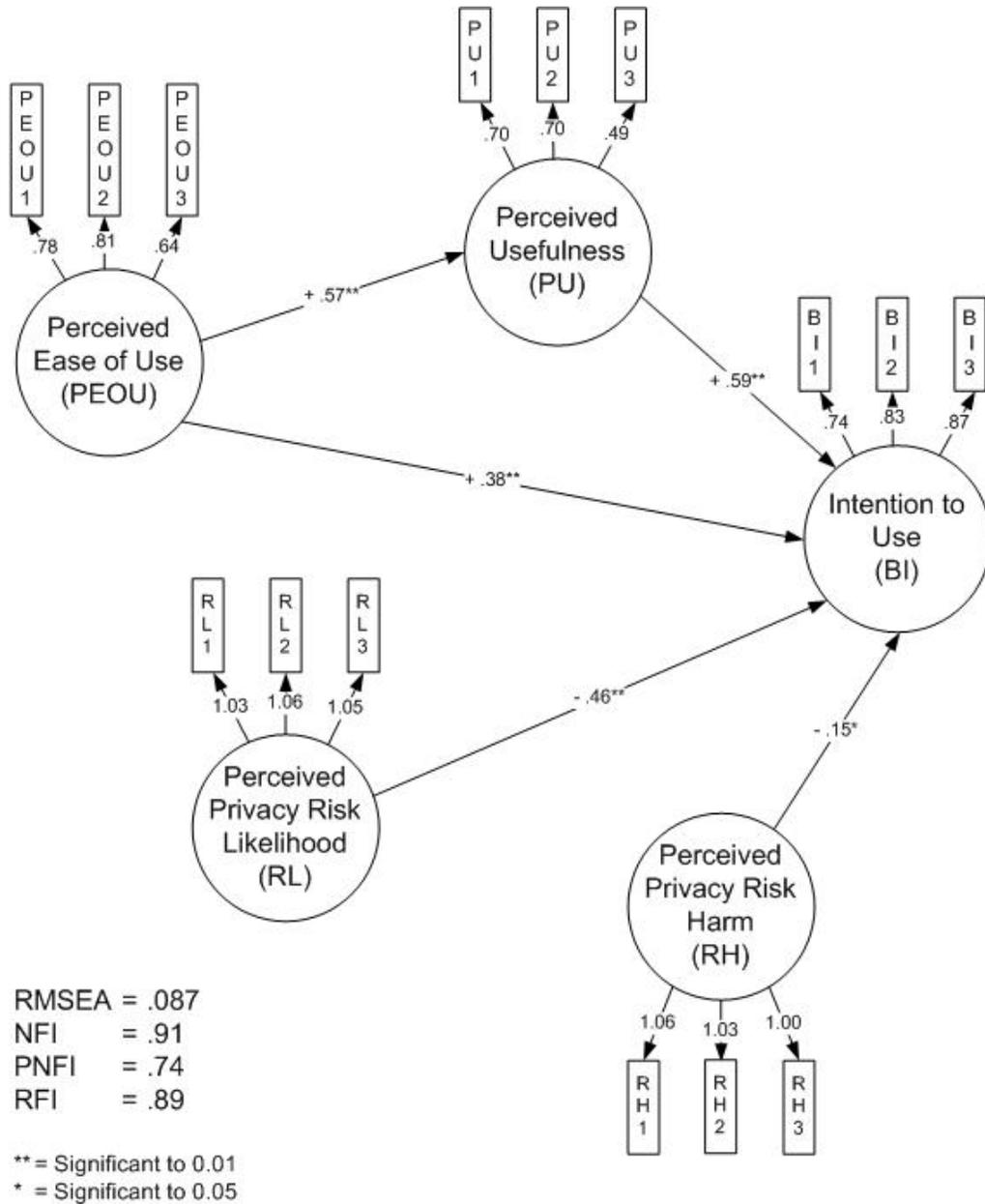* = Significant to 0.05

Figure 7: Privacy Risk Model

Disabled RFID Tag Results

Rather than measure only the negative impact of privacy risk on consumers' behavioral intentions, we wanted to learn whether there was anything companies could do, from a consumer perspective, to mitigate privacy risk likelihood and harm. In addition to our questions designed to ascertain consumer behavior, we asked our subjects the following questions to determine whether their behavior would change under the circumstances presented:

1) I would be more inclined to purchase products that use RFID if I could disable the RFID tag after my purchase. (BI1 in this model)

2) I would be more inclined to purchase products that use RFID if the retailer would automatically disable the RFID tag after my purchase. (BI2 in this model)

We then ran the model using these two elements, using the same scale validation, and determined that when the consumer has the ability to disable the tags, as indicated by the two scenarios presented above, privacy risk likelihood and privacy risk harm become non-significant in the model, as shown in figure 8, while TAM remains strong and significant.
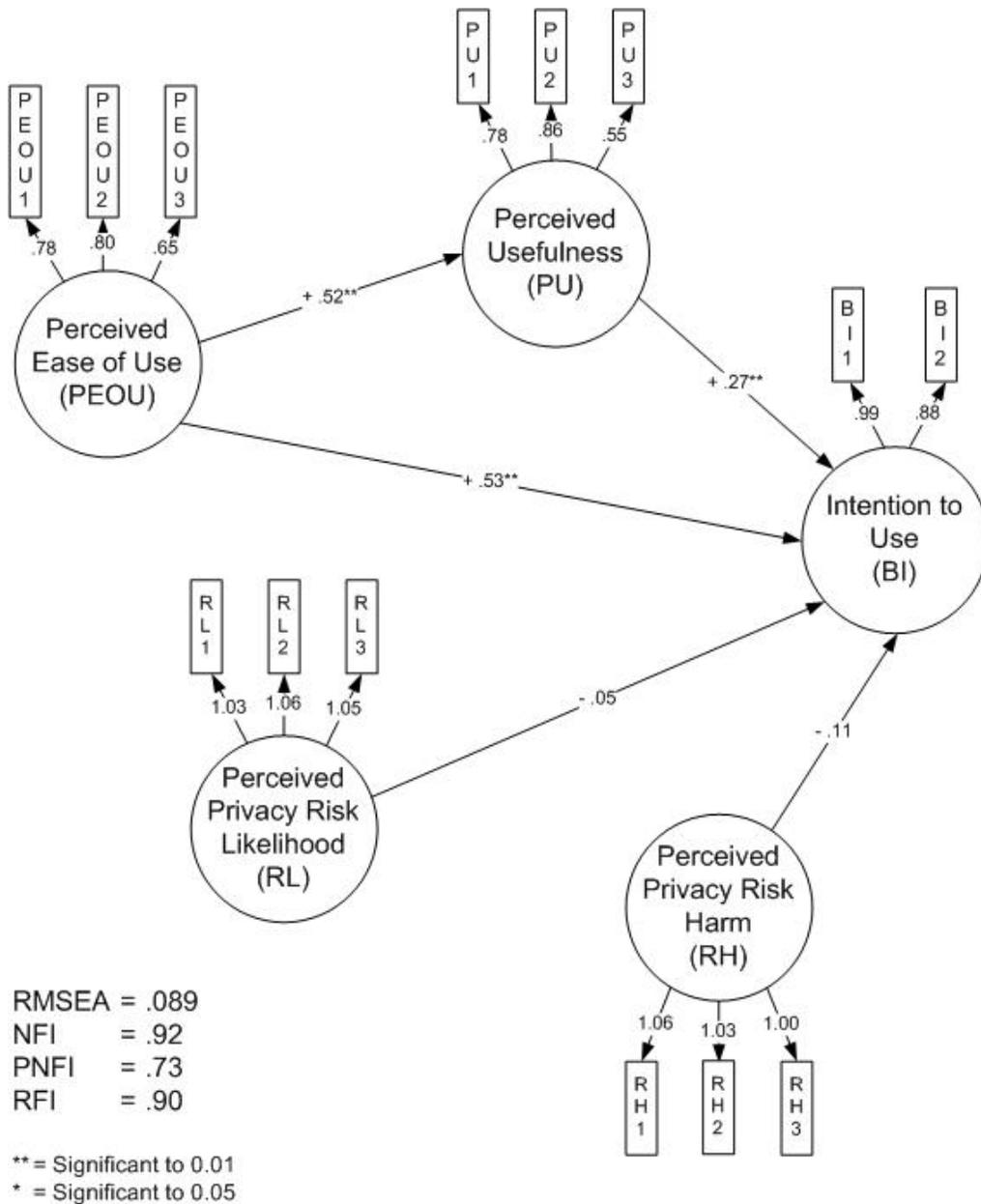

RMSEA = .089
NFI   = .92
PNFI   = .73
RFI   = .90

** = Significant to 0.01
* = Significant to 0.05

Figure 8: Privacy Risk Model, Disabled RFID Tags

The inclusion of this second scenario, as shown in figure 8, is important as it renders our fourth and fifth hypotheses unsupported (see table 5 below). Deactivated tags result in no verifiable perceived privacy risk likelihood and therefore no verifiable perceived privacy risk harm. Organizations should carefully consider these findings before adopting a SCM that includes Residual RFID technology.

Table 5. Hypotheses Summary for Disabled Tag Model					
Hypothesis	Description	Effect – Active Tags	Supported	Effect – Disabled Tags	Supported
H1	PEOU will have a positive impact on PU.	0.57	Yes	0.52	Yes
H2	PU will have a positive impact on BI.	0.59	Yes	0.27	Yes
H3	PEOU will have a positive impact on BI.	0.38	Yes	0.53	Yes
H4	RL will have a negative impact on BI.	-0.46	Yes	-0.05	No
H5	RH will have a negative impact on BI.	-0.15	Yes	-0.11	No

Table 6 displays the fit statistics for this model and shows a good overall fit.

Table 6. Fit Statistics for Disabled Tag Model		
Fit Measure	Abbreviation	Fit Statistics – Disabled Tags
Chi-square	χ^2	251.850
Degrees of freedom	Df	72.000
Discrepancy/df	χ^2/df	0.570
Goodness of fit index	GFI	0.900
Normed fit index	NFI	0.920
Relative fit index	RFI	0.900
Incremental fit index	IFI	0.940
Comparative fit index	CFI	0.940
Root mean square error of approximation	RMSEA	0.089
Root mean square residual	RMR	0.21
Adjusted Goodness of fit index	AGFI	0.85
Squared multiple correlations for PU	SMC/R2	0.34
Squared multiple correlations for BI	SMC/R2	0.23

It should be noted, however, that disabling the tag automatically removes any benefits companies and consumers might receive from Residual RFID tags and may raise either tag or item costs. While disabling the tags may remove the problem, it does so by making them non-residual and at a cost of the benefits of residual tags.

V. DISCUSSION

Consumers' perceptions of privacy risk associated with RFID technology, as well as their perceptions of its usefulness and ease of use, directly influence their intention to adopt and accept this technology. The technology

acceptance model (TAM) as fully supported in the complete model with enabled tags, with every hypothesis having significant support. Notably, perceived ease of use (PEOU) has a positive and direct impact on perceived usefulness (PU) and intention to use (BI); PU has a positive impact on BI while perceived privacy risk likelihood (RL) and perceived privacy risk harm (RH) have direct and negative impacts on BI. All of these constructs are important in understanding the behavioral intentions of consumers. Predictably, when we disable the tags (take away the technology) in model 2, RH and RL become insignificant, but PEOU and PU remain strong predictors of BI. This shows that privacy risk harm and privacy risk likelihood are especially important when dealing with Residual RFID, as opposed to disabled tags. However, since the residual tags have the most to offer business, consumers and society, it would be well if we could find a way to address these privacy risks.

This paper makes an important point by expanding TAM to a new domain, that of residual RFID tags, that looks at passive technology adoptions with both positive and negative utility. The fit indices, factor analysis and findings are very strong, showing a strong and resilient model for this technology. TAM is our most studied theoretical framework in information systems [Premkumar & Bhattacherjee, 2008] and is an important part of building upon a cumulative tradition in our discipline.

Even though TAM is our most studied construct, it still requires significant investigation to fully understand and use it in our changing business and technological environments. For example, Lai and Li [2005] assert that even though TAM is a mature model and has been validated in different contexts, it still must be empirically investigated for its invariance across different respondent subgroups in order to make sure that different sample profiles would not have a negative effect on the findings. Unfortunately, this has not happened in most TAM research.

This suggests that while we are developing a cumulative tradition, especially as it relates to TAM, that tradition still requires much investigation to finish this process. Additionally, it is arguably even more important in a field such as information systems, that seems to be changing much faster than other disciplines, to build and maintain this cumulative tradition as people and technologies evolve. What was true yesterday may be more nuanced today as new generations of people emerge with different interactions with technology and technology has more to offer than in the past. Thus, looking at TAM in a new context can still make an important contribution to our IS literature, especially as it foreshadows a wave of new technology being rolled out that will have a significant impact on consumers, that of residual RFID.

Residual RFID is an important part of cultivating and securing the information supply chain that takes place after the technology reaches the consumer. With mass adoption of Residual RFID technologies imminent, we can no longer leave the consumer out of the supply chain. These technologies, used in the supply chain and left over, can now have a significant impact on consumers' acceptance and purchase of products with embedded Residual RFID technologies. Specifically, consumers' perceptions of privacy risk likelihood and privacy risk harm have a significant negative impact on consumers' willingness to adopt products that use these technologies. Therefore, companies must extend the mental conception of their supply chains to the consumer, and consider how the consumer will accept and interact with a product before implementing full-scale mass deployment of these technologies. Otherwise, consumer backlash may become a significant issue.

This research shows that positive and negative utility are both important to consumers when considering the adoption and acceptance of residual RFID tags, and that both risk likelihood and risk harm are strong and important deterrents to consumer acceptance of this technology. While many businesses focus on the positive impact of the technology and how it will benefit them, they would be wise to remember that ultimately the consumer must accept this technology, and right now, many have unaddressed concerns that may prohibit such acceptance. Perceptions of risk likelihood are an especially strong deterrent to this consumer acceptance and businesses must address such deterrents if they want consumers to embrace this technology.

While it is useful and important for businesses to focus on positive utility factors such as perceived ease of use and perceived usefulness, it is also essential that they not forget about negative utility factors, such as privacy risk likelihood and privacy risk harm, that have the potential to lead consumers to a possible rejection of products containing RFID technologies. Notably, when we give consumers the choice to disable Residual RFID tags, either on their own or automatically at the time of purchase, the problem of negative utility becomes insignificant. This, however, may be an undesirable course of action, as through the disabling of the tags, businesses and consumers not only lose the negative reaction, but they also sacrifice the benefits that this technology can bring to businesses as well as to consumers. Disabling the tags essentially takes away their residual nature.

Due to the nature of RFID technology, and especially the residual aspects of it that allow it to remain active indefinitely, it is likely beyond the ability of businesses alone to adequately address these concerns while still reaping the positive aspects of the technology. The easiest way for businesses to reduce the fear is by disabling the tags, which makes the concerns about risk harm and risk likelihood insignificant. However, this very act is essentially

making the concern go away by not using the technology. By not using the technology, businesses are giving up all of the positive benefits that could accrue to society now and in the future by having residual tags to help with the after market supply chain activities. This does reduce the concerns, but this would be like throwing the baby out with the bath water.

One such benefit that would be lost with disabling the tags is that of having a greener after market supply chain. By not disabling the tags, businesses, governments and consumer groups could use this technology to trace the life history of a product through its use and disposal, making it easier and more efficient to recycle goods. As concern for the environment grows, this could be a potentially untapped benefit for consumer recycling of goods and reverse logistics. Business groups might be able to tout this and other potential benefits to government officials as a way to address the real problems of reducing the risk harm and risk likelihood perceptions of consumers in a manner that still preserves the benefits.

Breaking risk out into risk likelihood and risk harm, as we do in this study, is very important in helping us understand this process. Doing so gives us the ability to look at these constructs independently so that organizations may address each construct independently. For example, organizations may look at the relative impact strength of risk likelihood versus risk harm and spend considerable time, effort, and money reinforcing and improving security measures to reduce the perception of a breach occurring. Organizations and governments might also use this strategy to focus on reducing the amount of harm that may occur by enacting ID theft laws that limit consumer liability and may increase consumers' intentions to accept RFID technology.

Because of the innovative nature of this research, presented here in advance of a significant shift in information supply chains, it is challenging for consumers to realistically comprehend the full-scale implications of moving toward a world where Residual RFID tags are everywhere, present in every consumer product. Consequently, while this research is important in understanding how consumers react when presented with likely scenarios, reactions may change as consumer understanding matures in this area.

Future Research

Future research should expand upon this model by exploring how to mitigate privacy risk likelihood and privacy risk harm perceptions through organizational and educational practices as well as governmental intervention. In addition, it might be useful for future researchers to integrate trust into the model to determine whether trust can be a mitigating factor for privacy risk. Additionally, it would be interesting to study the shifts in consumers' views over time

across generation. This will be especially interesting when consumers become more aware of the RFID technology and the impact on their world. The current study makes an important contribution by setting a baseline of their views today that would be useful for future comparisons as the world changes.

In this increasingly flat world it will be useful to re-examine this research in an international context and in various settings, such as health care, consumer purchases, high and low end products, etc. Consumers may react differently to Residual RFID use in health care as opposed to retail. Therefore, we recommend study within different contexts. It may also be worth studying the impact of government use of RFID, such as the current plan to embed RFID tags in U.S. passports.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor, or who are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.

2. The contents of Web pages may change over time. Where version information is provided in the references, different versions may not contain the information or the conclusions referenced.

3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.

4. The authors of this article, not AIS, are responsible for the accuracy of the URL and version information.

Abramson, Larry (2004) "Radio Frequency IDs." *National Public Radio (NPR)*, Morning Edition, March 26, 2004. http://www.npr.org/templates/story/story.php?storyId=1792847.

Ajzen, I. and M. Fishbein (1980) *Understanding Attitudes and Predicting Social Behavior,* Englewood Cliffs, NJ: Prentice-Hall.

Attaran, M. (2006) "RFID Pays Off", *Industrial Engineer* (38)9: p. 46.

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

Conca, C., B. D. Medlin and D. Dave (2005) "Technology-based Security Threats: Taxonomy of Sources Targets and a Process Model of Alleviation", *International Journal Information Technology Management*, (4)2, pp. 166-177.

Davis, F. D., R. P. Bagozzi and P. R. Warshaw (1989) "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", *Management Science*, 35, pp. 982-1002.

Drennan, J., G. S. Mort and J. Previte (2006) "Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users", *Journal of Organizational and End User Computing*, (18)1, pp. 1-22.

Eckfeldt, B. (2005) "What does RFID do for the Consumer?" *Communications of the ACM*. (48)9, pp. 77-79.

Emigh, J. (2004) "Is RFID the Key to Supply-Chain Security?" *eWeek.com*, October 6, 2004, http://www.eweek.com/c/a/Supply-Chain-Management-and-Logistics/Is-RFID-the-Key-to-SupplyChain-Security/.

Featherman, M. S. and P. A. Pavlou (2003) "Predicting E-services Adoption: A Perceived Risk Facets Perspective". *International Journal of Human-Computer Studies*, 59, pp. 451-474.

Gao, X., Z. Xiang, H. Wang, J. Shen, J. Huang and S. Song (2004) "An Approach to Security and Privacy of RFID System for Supply Chain," *Proceedings of the Conference on IEEE International*, September 2004, pp. 164-168.

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

Gaudin, S. (2008) "Washington State Passes RFID Antispying Law", *Computerworld Inc.*, March 27, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9072438&source=rss_news6.

Heijden, H., T. Verhagen and M. Creemers (2003) "Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives", *European Journal of Information Systems*, 12, pp. 41-48.

Hoffman, D. L., T. P. Novak and M. Peralta (2004) "Building Consumer Trust Online", *Communications of the ACM*, (42)4, pp. 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", January 25, 2006, retrieved March 14, 2008 from http://www-03.ibm.com/press/us/en/pressrelease/19154.wss.

Juban, R. L. and D. C. Wyld (2004) "Would You Like Chips with That?: Consumer Perspectives of RFID", *Management Research News*, (27)11, pp. 29-44.

Juels, A. and R. Pappu (2003) "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," in Wright, R. (ed.) *Financial Cryptography*, Springer-Verlag.

Juels, A., R. Rivers and M. Szydlo (2003) "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proceedings of the 10th Annual Conference on Computer and Communications Security*, pp. 103-111.

Karjoth, G. and P. A. Moskowitz (2005) "Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced," *WPES*, November 2005, Alexandria, VA., pp. 27-30.

Keen, P. G. W. (1980) "MIS Research: Reference Disciplines and a Cumulative Tradition", *International Conference on Information Systems*, Philadelphia, Pennsylvania.

Kelloway, E. K. (1998) *Using LISREL for Structural Equation Modeling: A Researcher's Guide*, Thousand Oaks, CA: Sage Publications.

Lai, V. S. and H. Li (2005) "Technology Acceptance Model For Internet Banking: An Invariance Analysis", *Information & Management,* 42, pp. 373-386.

Kim, S. and C. S. Leem (2005) "Security of the Internet-based Instant Messenger: Risk and Safeguards", *Internet Research*, (15)1, pp. 68-98.

Labuschagne, L. and J. H. P. Eloff (2000) "Electronic Commerce: the information-security challenge", *Information Management & Computer Security,* (8)3, 54-159.

Lee, Y., K. A. Kozar and K. R. T. Larsen (2003) "The Technology Acceptance Model: Past, Present, and Future". *Communications of AIS*, (50)12, pp. 752-780.

Malhotra, N. K., S. S. Kim and J. Agarwal (2004) "Internet users' Information Privacy concerns (IUIPC): The Construct, the Scale and a Casual Model*", Information Systems Research*, (15)4, 336-355.

Markelevich, A. and R. Bell (2006) "RFID: The Challenges It Will Bring," *Strategic Finance*, August 2006, pp. 46-49.

McCullah, D. (2003) "RFID Tags: Big Brother in Small Package," *CNet*, January 13, 2003, http://www.news.com/2010-1069-980325.html.

Milne, G. R. and M. J. Culnan (2004) "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't read) Online Privacy Notices", *Journal of Interactive Marketing*, (18)3, pp. 15-29.

Premkumar, G. and A. Bhattacherjee (2008) "Explaining Information Technology Usage: A Test of Competing Models", *Omega,* 36, pg 64-75.

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

Sarma, S. E., S. A. Weis and D. W. Engels (2002) "Radio-Frequency Identification Systems", in Kaliski, Jr., B. S., C. K. Koc, and C. Paar (eds.), *Cryptographic Hardware and Embedded Systems*, Springer-Verlag, pp. 454-469.

Spiekermann, S. and H. Ziekow (2005) "RFID: A 7-Point Plan to Ensure Privacy", *13th European Conference on Information Systems*, Regensburg, Germany.

Straub, D. W. and R. J. Welke (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, (22)4, pp. 441-469.

Wyld, D. C. (2006) "RFID 101: The Next Big Thing for Management", *Management Research News*, (29)4, p.154.

Zhang, C. and S. Li (2006) "Secure Information Sharing in Internet-Based Supply Chain Management Systems," *The Journal of Computer Information Systems*, (46) 4, pp. 18-24.

APPENDIX A: SURVEY INTRODUCTION AND QUESTIONS

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 fulfill 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.

The first six questions of the survey are demographics questions, and as such, are not represented here. Questions 7 – 35 (except question 12, which is open-ended) are measured on a 7-point Likert scale, from Very Strongly Disagree (Value = 1) to Very Strongly Agree (Value = 7).

7. Residual RFID will make returning purchases easier.

8. Residual RFID will make returning purchases more efficient.

9. Residual RFID will make it easier for authorities to track stolen products.

10. Residual RFID will make filing insurance claims easier and more accurate.

11. Residual RFID will enable retailers to better serve me by helping them better understand my purchase preferences.

12. Please list other ways you can think of in which RFID might affect consumers. (Open ended)

13. Residual RFID will ultimately be used for my best interests.

14. Organizations that develop RFID technology will be careful to ensure that my privacy is protected.

15. Companies that employ RFID in their products will do what is best for me.

16. Companies that employ RFID in their products will do what is best for society.

17. The government will make every effort to protect my privacy from RFID abuse.

18. Organizations that use RFID will fulfill their promises.

19. Organizations that use RFID are honest.

20. Organizations behind RFID deployment have integrity.

21. Organizations that use RFID will tell the truth about its risks.

22. The government will tell the truth about the risks I may encounter with RFID.

23. Overall, I trust the organizations behind RFID technology.

24. Overall, I trust the organizations that use RFID.

25. Overall, organizations that use RFID technology are worthy of receiving consumer trust.

26. I trust the government not to abuse RFID technology.

27. I trust the government to protect me from RFID abuse.

28. I would prefer to purchase products from retailers that use RFID.

29. The use of RFID is unlikely to change my purchasing preferences.

30. I would actively seek out products that use RFID.

31. If given the choice between a RFID product and a non-RFID product, I would choose the product that uses RFID.

32. I would be more inclined to purchase products that use RFID if I could disable the RFID tag after my purchase.

33. I would be more inclined to purchase products that use RFID if the retailer would automatically disable the RFID tag after my purchase.

34. The greater ease with which products may be returned would encourage me to purchase products that use RFID.

35. I would be willing to pay extra to disable RFID tags in the products I purchase.

Questions 36 – 37 are measured on a 7-point Likert scale, from –10% (Value = 1) to +10% (Value = 7).

36. How much more or less would you expect to pay for products that use RFID?

37. How much more or less would you be willing to pay for products that use RFID?

Questions 38 – 42 are measured on a 7-point Likert scale, from Almost Impossible (Value = 1) to Almost Certain (Value = 7).

38. How likely is it that Residual RFID would enable others to use your private personal information in a way you would not approve of?

39. How likely is it that others would use Residual RFID to abuse some of your personal information?

40. How likely is it that someone will use Residual RFID to steal your personal information?

41. How likely is it that your private personal information will be stolen as a result of Residual RFID?

42. How likely is it that your privacy will be violated as a result of Residual RFID?

Questions 43 – 47 are measured on a 7-point Likert scale, from No Harm At All (Value = 1) to Severe Harm (Value = 7).

43. How much harm could be done to you if someone broke into RFID databases containing your private personal information?

44. How much harm could be done to you if an organization that employs RFID abused your information?

45. How much harm could be done if consumers' personal information is abused through RFID?

46. How much harm could be done if consumers' personal information is stolen because of RFID?

47. How much harm could be done to you if someone used Residual RFIDs to track your purchases and/or personal possessions?

ABOUT THE AUTHORS

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 *The Journal of Information Systems Security, Information Systems Security, Information and Management, Information Systems Frontiers, 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.*

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 RFID security applications, high-resolution display systems and textual analytics. He has published in the *International Journal of Business Environment* and the *Journal of Information System Security*.

Dinesh S. Dave is a professor and director of supply chain management 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.

Communications of the Association for Information Systems