December 2007

The Impact of Government Trust Perception on Privacy Risk Perceptions and Consumer Acceptance Of Residual RFID Technologies

Andrew Jensen

Joseph Cazier
Appalachian State University

Dinesh Dave
Appalachian State University

THE IMPACT OF GOVERNMENT TRUST PERCEPTION ON PRIVACY RISK PERCEPTIONS AND CONSUMER ACCEPTANCE OF RESIDUAL RFID TECHNOLOGIES

Andrew S. Jensen, Appalachian State University, aj68124@appstate.edu
Joseph A. Cazier, Appalachian State University, cazierja@appstate.edu
Dinesh S. Dave, Appalachian State University, daveds@appstate.edu

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 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 future, nearly 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 a small radio frequency identification (RFID) tag. 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.

We are on the verge of wide-scale adoption of RFID technologies 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.

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). All of these needed improvements may 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).

Implementation of RFID requires a significant investment, and the ROI is directly associated with the improvements it enables. The challenge for IT 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).

Passive vs. Active RFID tags

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.

Benefits of RFID for Consumers

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

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 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 security benefit for consumers 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 creates a precise time log and map of the consumer's travels, the perceived privacy risk that documentation poses is far less than the perceived convenience benefit the EZ-Pass system has generated.

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?

Residual RFID Benefits

The consumer benefits or RFID technology can be seen through many existing application. 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

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

Residual RFIDs can 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.

Improved Service

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." They also suggest that individuals may be tracked by others through the objects they carry (Spiekermann 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 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 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."

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 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

Cazier et al. (2007b) states 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.

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).

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. (2007b), 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. 2007b). 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 organizations 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 event of a privacy breach (Cazier et al. 2007b). 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).

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 2006b). This is critical in the RFID environment.

Cazier (2007a) expounds on the theory proposed by Mayer et al. (1995), regarding the three dimensions of trust, 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).

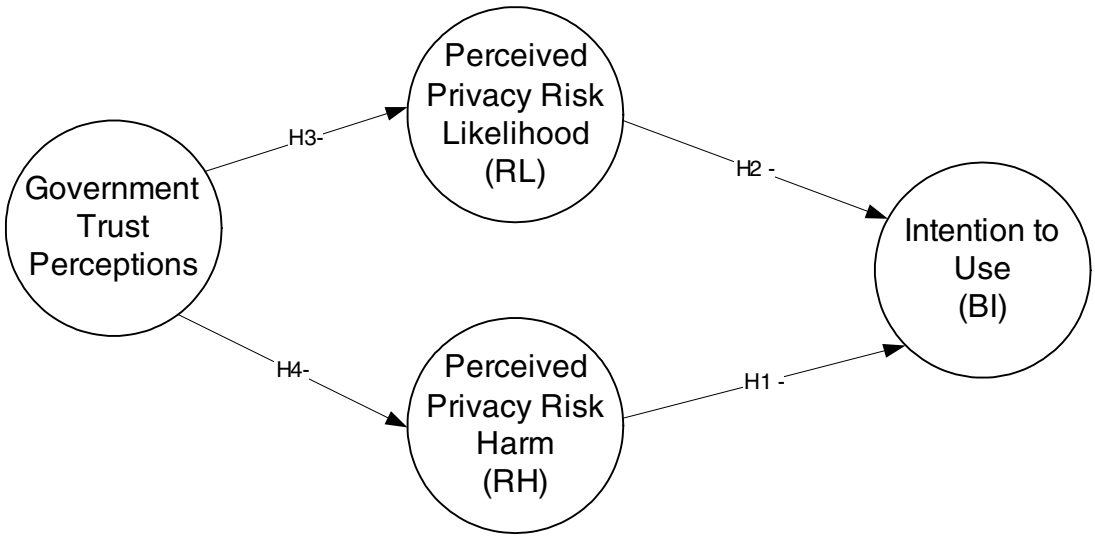

Figure 1. Government trust perceptions, risk likelihood, risk harm

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 2006a).

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 theft or 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 2006b). 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 discussed in sections 3.1 - 3.3, 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. The 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 summary, respondents 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 (Abramson 2004).

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. 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.

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.

Subjects

A sample was taken 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 to $50 thousand annually. Respondents' familiarity was 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.

PRELIMINARY RESULTS

Whether consumers trust their government to protect them from privacy violations may have significant impact on their intentions to use Residual RFID technologies. In our pilot studies we included five questions that were designed to measure the subjects' trust of the government and it's role in Residual RFID technology. All preliminary findings in this regard were significant and substantiated the model presented in section 3.3.

Complete results will be presented at AMCIS 2007.

DISCUSSION

The impact of Residual RFID, particularly on consumers, is an area of research that needs further attention. In this research-in-progress study, we have outlined several of the possible benefits and liabilities of Residual RFID from a consumer perspective. The survey instrument has been designed to measure and validate consumer perceptions on the

subject, and of the government's role, in particular. Through the survey, we attempt to ascertain how consumers will react to the pending implementation of Residual RFID technologies on a mass scale, and specifically how the consumers' perceptions of trust, particularly in their government, privacy risk likelihood and privacy risk harm impact their intentions to accept Residual RFID technology.

Consumers expect the government to be integrally involved in the legislation and regulation of technology, particularly where privacy and security are concerned. Our research, to be presented at AMCIS 2007, shows that by building trust with consumers, government has the ability to mitigate the risks associated with the adoption of Residual 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.

REFERENCES

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

Attaran, Mohsen. "RFID pays off ." *Industrial Engineer*. Norcross: Sep 2006. Vol. 38, Iss. 9; p. 46.

Cazier, J. A. (2007a) "Projecting Values Online: An E-Tailing Goldmine?", Forthcoming in *International Journal of Electronic Marketing and Retailing*.

Cazier, J. A. (2006a). *Value Congruence and Trust Online: Their Impact on Privacy and Price Premiums*, Youngstown, New York 14174-0350: Cambria Press.

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

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

Conca, C. Medlin, D. & 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.

Eckfeldt, Bruce, "What Does RFID do for the Consumer?" *Communications of the ACM*. September 2005/Vol. 48, No. 9; 77-79.

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

Hoffman, D.L., Novak, T.P., & Peralta, M. (2004). "Building consumer trust online" Association for Computing Machinery. *Communications of the ACM*. (42) 4, 80-86.

IBM, "IBM Survey: Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime: Changing Nature of Crime Leads to Significant Behavior-Changes", Retrieved from http://www 03.ibm.com/press/us/en/pressrelease/19154.wss on January 27, 2006.

Kim, S. and Leem, C. S. (2005). "Security of the internet-based instant messenger: Risk and safeguards", *Internet Research*, (15)1, 68-98.

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

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, Ziekow H (2005), "RFID: A 7-Point Plan to Ensure Privacy" In *Proceedings of the Thirteenth European Conference on Information Systems* (Bartmann D, Rajola F, Kallinikos J, Avison D, Winter R, Ein-Dor P, Becker J, Bodendorf F, Weinhardt C eds.), Regensburg, Germany.

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.

Wyld, David C. (2006). "RFID 101: the next big thing for management", *Management Research News*. Patrington: 2006.Vol.29, Iss. 4; pg. 154.