RFID UBIQUITY AND PRIVACY LOSS CONCERNS AN ANALYSIS OF A PENNSYLVANIA UNIVERSITY

David M. Douglas, Robert Morris University, dmdst27@mail.rmu.edu
Karen L. Paullet, Robert Morris University, paullet@rmu.edu

ABSTRACT

Radio Frequency Identification technology is an ever-present automatic identification and data collection system. This technology has transformed how business and government operate their identification and data collection systems. Concerns about potential loss of privacy have increased as an aspect of a person's interaction with RFID technology and device. A study of 317 undergraduate and graduate students at a mid-Atlantic university found that there was a significant association between gender and familiarity with RFID technology. Student respondents agreed that they would limit their use of RFID devices if a user profile could be built on them without their knowledge of consent.

Keywords: radio frequency identification (RFID), automatic identification and data collection (AIDC) system, digital data, and privacy

INTRODUCTION

Radio Frequency Identification (RFID) is no longer viewed as a novel automatic identification and data collection (AIDC) system or just a tool used for end-to-end supply chain management. Nor is RFID just a convenient warehouse tool used exclusively to identify and track items from a supplier to the retailer. It has gone beyond its technological acceptance as a replacement for the UPC barcode. RFID technology has become more flexible, powerful, compact, and cheaper than just a few years ago [2]. RFID technology is capable of identifying a tagged object, the person associated with the object, and the location of the object throughout space and time.

Supporters of RFID technology see it as a replacement for the familiar UPC barcode that would eliminate lines at store checkouts. In theory, shoppers would walk through the supermarket door with their purchases and all the products in their carts would be billed to their credit card [5]. "Like the Internet, which gradually spread through the fabric of the global economy, RFID seems destined to become ubiquitous and nearly invisible" [2].

Privacy advocates have concerns about RFID technology, its surveillance capabilities, and their rights to digital privacy. Existing information and communication technologies such as RFID allow both commercial and government sponsored surveillance systems to construct digital files on people and objects as they move through time and space. RFID systems have the ability to covertly collect this data in real time on a person's identity, location, and activities and electronically store and share that information with those with the ability or authorization to access it.

PURPOSE OF STUDY

The purpose of this research was to identify and compare gender and generational trends within university student groups that represented aspects of privacy loss concerns associated with the passive and active use of RFID technology and devices in 2009. Another important aspect of the research was to determine what was more important to the user, convenience or privacy when they interacted with various phases of an RFID technology or devices in 2009.

The problem leading to this study was the lack of identification and analysis of privacy loss concerns among segments of a university student population who could have concerns regarding their loss of digital privacy when they interacted with various phases of an RFID technology or devices. This study explores the following research questions:

RQ1. Are privacy loss concerns hindering user acceptance of RFID technology for daily activities such as work, travel, and retail purchases?

RQ2. What is more important to the user of RFID devices, convenience or privacy?

RFID DEFINED

RFID technology uses radio waves and the physics of electromagnetic (EM) wave theory to allow RFID systems to function. One of these early applications was the crystal radio sets of the 1930s. The ability of crystal radio sets to harvest energy from a radio signal was an important achievement and was one of the key foundations to the development of passive RFID technology. Improvements in radio and radar technology during World War II lead to the use of the far-field system used by RFID devices [3].

The Association for Automatic Identification and Mobility (AIM Global) provides the following definition for RFID.

> Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves. It is grouped under the broad category of automatic identification technologies [13].

RFID technology is seen as a cross-section technology. The applications are seen as having potential in aspects of daily and business life when they are related to object identification. Other uses include document identification, theft prevention, routing control, supply chain management, environmental monitoring, automated payment systems, and smart homes and offices. Although businesses have extolled the value and merits of RFID technology, there are some concerns and risks involved with its use and deployment. Privacy and civil liberty advocates are concerned with the ability of RFID technology to track people, objects, vehicles, and currency [8].

PRIVACY DEFINED

Conceptually, privacy is difficult to define because the concept of privacy has a rich and varied judicial, academic, and personal denotation. Moreover, the meaning of privacy has varied between cultures, history, and time. Therefore, the researchers will operationally define privacy for this study. Privacy is the right of an individual to control how the digital data collected and stored via RFID technology is used regarding their public activities, private behavior, and location in time and space.

The first systematic storage of personal data became possible because of the computers ability to store data digitally on magnetic tapes. Digital files also known as digital dossiers began in 1946 with the appearance of mainframe computers. As improvements were made in the computers ability to process and store data, so did the computers ability to search, collect, transfer, and analyze data. As governmental agencies began to computerize their records, the Social Security number (SSN) became the key link between particular bits of data and the individual [9].

Spiekermann & Ziekow [11] identified five immediate and key threats of RFID to privacy based on the fundamental research and on user studies conducted by AutoID Labs and Humboldt University in Berlin. Included on the list were the unauthorized assessment of one's belongings, tracking people via the object in their possession, retrieving social networks, technology paternalism, and making people responsible for the object in their possession [10].

According to Best, Kruger, & Ladewig [1] since 1990 there have been three major developments capable of changing public opinion concerning personal privacy. The number one development was the emergence of the Internet as a new and rapidly adopted communication technology. The second development was the launch of the "war on terrorism." Finally, the last development was the expansion of a wide range of technologies whose sole purpose was to conduct discrete surveillance.

METHODOLOGY

This study examined privacy loss concerns between gender and generational groups associated with the use of radio frequency identification (RFID) devices among students at a mid-Atlantic university. Additionally, the study explored the importance of student attitude of convenience versus privacy when they interacted with RFID devices. A quantitative research approach was applicable for determining if there were particular characteristics to concerns of privacy loss among generational and gender groups at a mid-Atlantic university. With a quantitative approach, associated relationships to consumer acceptance of RFID technology and privacy loss concerns could be compared and analyzed. The researchers selected a non-probability convenience sampling approach in order to target this particular group. Non-probability sampling is widespread in the world of social science research. In this case, a

convenience sample of a university student population drove the selection process.

The 317 survey participants were comprised of students who resided on campus or commuted to classes. As of January 2009 the student population of the university was approximately 5,200. Included within the group were graduate and undergraduate students who were 18 years of age or older. Generational groups from various disciplines were surveyed. No distinctions was made between daytime, evening, or Saturday students.

The survey instrument was comprised of three sections. Part one of the survey focused on specific demographics of the student population. The researchers adapted demographic inquires from Hossain & Prybutok [4] and Mjolsnes & Teigen [7] then designed the questions to ascertain certain variables that may exist within the university community. Part two of the survey instrument focused on user concerns with privacy loss and adoption intention was modified from the research studies of Lu, Yu, & Liu [6]. Part three of the survey instrument involved the aspect of privacy loss concerns if or when the respondents interacted with a particular RFID device. Additionally, participants were asked what was more important to them when they interacted with an RFID device, convenience or privacy. The survey questions for part three were adapted and designed from questionnaires administered by Mjolsnes & Teigen [7] and Hossain & Prybutok [4].

SAMPLE

The convenience sample consisted of 317 undergraduate and graduate students at a mid-Atlantic university from a population of approximately 5,200 students. A 5% margin of error with a 95% confidence level was used for this study. The survey instrument contained basic demographic questions, addressed student consumer acceptance of RFID devices, and asked participants what was more important to them when they interacted with a RFID device, privacy or convenience.

In order to foster a representational sample to reflect the target population, the researchers contacted faculty from all six academic schools via e-mail during the spring semester in January 2009. Faculty members who agreed to participate in the survey were from the School of Adult & Continuing Education, the School of Communications & Information Systems, the School of Business, and the School of Education & Social Science.

E-mails were sent via the university Intranet to faculty members that explained the purpose of the survey and asked for permission to administer the survey during one of their spring semester classes. Once permission was granted, an appointment was made via e-mail to conduct the survey at the convenience of the faculty member during their scheduled class time. The researchers administered the survey to the 317 students between January and February 2009. Included with the survey packet was a brief description of RFID and contact information if they were interested in the findings of the study. Students were informed that their involvement was voluntary and if they choose not to participate, it would not affect their current or future relationship with the university.

RESULTS

Concerns about RFID surveillance and the right to privacy, in particular digital privacy, have become a salient issue in recent years. Ubiquitous RFID devices can determine the identity, location, and activity of users who interact with the devices. Existing information and communication technology now allow both private and government sponsored surveillance systems to construct digital dossiers on people throughout time and space, often without their knowledge or consent.

Male respondents totaled 198 or 62.5% of the study population. Female respondents totaled 119 or 37.5% of the study group. A frequency analysis was used to determine the diversity among the generational group represented in the survey. Those born before 1945 (Matures) represented the smallest minority segment of the study group with just 1 respondent or (0.3%) of the population. Those born between the years 1945-1964 (Baby Boomers) were represented by 6 respondents or (1.9%) of the study group. Generation Xers, or those born between the years 1966-1979, supplied 29 of the responses or (9.1%) of the survey population. The largest portion of the respondents were Generation Yers, or those born between the years 1980-1990, supplied 276 of the responses or (87.1%) of the survey group. Those born after 1990 represented the second smallest group with 5 respondents or (1.6%) of the study population.

The first research objective was to determine if privacy loss concerns were hindering user acceptance of RFID technology. Unfamiliarity and apprehension

can lead to generational and gender bias and prevent people from adopting a new technology until its benefits are realized. As members of a university community, the survey population had most likely, knowingly or unknowingly, interacted with an RFID technology or device in the past. The survey participants indicated their reaction to their concerns regarding loss of their privacy by circling one of the five-point Likert scale responses (see Table 1). The selection choices were strongly disagree, disagree, neutral, agree, and strongly agree. The selection of the particular RFID devices were designed to determine if any survey respondents had concerns about loss of privacy when they interacted with any of the RFID enabled objects appearing on the list.

Table 1: User Reaction to Privacy Loss with an RFID Enabled Object

RFID Device	Gender	Reaction to Privacy Loss When Interacting With RFID Devices					Total
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	
Work ID	Male	22	26	75	47	26	196
	Female	7	22	39	33	16	117
Building Access Device	Male	24	32	65	54	21	196
	Female	8	17	35	41	18	119
Drivers License	Male	16	23	46	58	55	198
	Female	10	14	21	36	37	118
Credit Card	Male	16	20	45	46	70	197
	Female	6	10	20	29	53	118
RFID Tagged Merchandise	Male	26	30	71	43	26	196
	Female	15	21	49	24	10	119
Passports	Male	16	19	50	43	69	197
	Female	9	11	25	29	45	119

However, the findings indicated that many were not familiar with RFID technology prior to completing the survey. Of the 317 respondents, 141 or 44.5% indicated they were not familiar with RFID technology prior to the survey. Of the 141 respondents who were not familiar with RFID, 77 or 55% were males and 64 or 45% were females. The reasoning behind this outcome could be that RFID technology is becoming as ubiquitous as the UPC barcode it is intended to replace.

Of the 176 respondents (see Table 2) who were familiar with RFID, 121 or 69% were males and 55 or 31% were females. The research indicted that there was a significant association between gender and familiarity with RFID technology. The gender variations in familiarity with RFID technology could be attributed to how genders view and use emerging communication and information systems.

Table 2: Gender and RFID Familiarity

Gender	Familiarity with RFID technology prior to survey		Total
	YES	NO	
Male	121	77	198
Female	55	64	119
Total	176	141	317
χ^2 (1, n = 317) = 6.1, p = .014, phi = .15			

A chi-square test for independence indicated a significant association between gender and familiarity with RFID technology prior to the researchers overview of the fundamental of RFID technology, $\chi 2$ (1, n = 317) = 6.1, p = .014, phi = .15. An additional chi-square test for independence was conducted in order to explore the relationship between generational groups and any prior familiarity the respondents had with RFID systems**.** The chi-square test collapsed the generational groupings into two variables (see Table 3), those who were born before 1980, and those who were born on or after 1980. A chi-square test for independence indicated a significant (.05) association between generational group and familiarity with RFID technology prior to the researchers overview of the fundamental of RFID technology, χ^2 (1, n = 317) = 3.9,p = .05, phi = .12.

Table 3: RFID Familiarity

Generational Group	Familiarity with RFID technology prior to survey		Total
	YES	NO	
Born before 1980	26	10	36
Born on or after 1980	150	131	281
Total	**176**	**141**	**317**
χ^2 (1, n = 317) = 3.9, p = .05, phi = .12			

A chi-square test for independence was conducted in order to explore the relationship between gender and the awareness the respondents had regarding the knowledge that RFID devices could collect personal information on them without their knowledge or consent. The chi-square test collapsed the generational groupings into two variables (see Table 4), those born before 1980 and those born in 1980 and after indicated there was not a significant association between generational groups and awareness that RFID devices could collect personal

information on respondents without their knowledge or consent, χ^2 (1, n = 316) = 2.5, p = .11, phi = .099.

Table 4: RFID Awareness

Generational Group	Awareness that RFID devices could collect personal information		Total
	YES	NO	
Born before 1980	21	15	36
Born on or after 1980	120	161	280
Total	**141**	**175**	**316**
χ^2 (1, n = 316) = 2.5, p = .11, phi = .099			

Research question 2 asked survey participants what was more important to them when they interacted with an RFID device (Table 5). The two choices were convenience or privacy. Survey questions were asked to obtain specific aspects of privacy loss concerns associated with the convenience of using RFID enabled objects. One question specifically asked the respondents what was more important to them, convenience or privacy. The research question also explored the impact of gender and generation based on levels of respondent reaction to privacy loss concerns that RFID devices could collect information on them without their permission

Table 5: Gender and Generation Privacy Loss Concerns

Reaction to Privacy Loss Concerns	Gender and Generation	Generation	Gender
	Statistically Significant		
Information w/o Permission	F(2, 310) = .68, p = .51	F(2, 310) = 1.64, p = .20	F(1, 310) = .75, p = .39
	No	No	No
Biometric Data	F(2, 310) = .53, p = .59.	F(2, 310) = .80, p = .45	F(1, 310) = .01, p = 1.0
	No	No	No
RFID Tag Read Capabilities	F(2, 310) = .33, p = .72	F(2, 310) = 1.23, p = .30.	F(1, 310) = .40, p = .53
	No	No	No
RFID Chip Implant	F(2, 309) = 1.23, p = .30	F(2, 309) = 3.23, p = .038	F(1, 309) = .05, p = .83
	No	Yes	No
Convenience or Privacy	F(2, 309) = 1.64, p = .20	F(2, 309) = 2.10, p = .13	F(1, 309) = .001, p = .98
	No	No	No

First, respondents were asked if they would consent to an RFID device to collect, share, and store their biometric data, as measured by a Likert 5-point scale. Subjects were divided into three age groups according to their generational units (Group 1: born before 1966; Group 2: born between 1966-1979; Group 3: born 1980 and after). The interaction between gender and generational groups was not statistically significant, F(2, 310) = .53, p = .59. There was not a statistically significant main effect for generational groups, F(2, 310) = .80, p = .45. There was not a statistically significant effect for gender, F(1, 310) = .01, p = 1.0.

Second, participants were asked if they would block an RFID read tag capabilities on purchased items when given the choice, as measured by a Likert 5-point scale. Subjects were divided into three age groups according to their generational units (Group 1: born before 1966; Group 2: born between 1966-1979; Group 3: born 1980 and after). The interaction between gender and generational groups were not statistically significant, F(2, 310) = .33, p = .72. There was not a statistically significant main effect for generational groups, F(2, 310) = 1.23, p = .30. There was not a statistically significant effect for gender, F(1, 310) = .40, p = .53.

Third, student participants were asked if they would consent to an RFID chip implant if they did not have to carry ID, money, or credit cards in their person, as measured by a Likert 5-point scale. Subjects were divided into three age groups according to their generational units (Group 1: born before 1966; Group 2: born between 1966-1979; Group 3: born 1980 and after). The interaction between gender and generational groups was not statistically significant, F(2, 309) = 1.23, p = .30. There was a statistically significant main effect for generational groups, F(2, 309) = 3.23, p = .038; however, the effect size was small (partial eta squared = .02). There was not a statistically significant effect for gender, F(1, 309) = .05, p = .83.

Finally, respondents were asked if convenience was more important than privacy when the survey participant used an RFID device, as measured by a Likert 5-point scale. Subjects were divided into three age groups according to their generational units (Group 1: born before 1966; Group 2: born between 1966-1979; Group 3: born 1980 and after). The interaction between gender and generational groups were not statistically significant, F(2, 309) = 1.04, p = .36. There was not a statistically significant main effect for generational groups, F(2, 309) = 2.10, p = .13. There was not a statistically significant effect for gender, F(1, 309) = .001, p = .98.

The researchers also sought to reveal possible privacy loss concerns and trends that were applicable to gender and generational groups. Of the 176 respondents who were familiar with RFID, 121 or 69% were males and 55 or 31% were females. The research indicted that there was a significant association between gender and familiarity with RFID technology. A chi-square test for independence indicated a significant association between gender and familiarity with RFID technology prior to the researchers overview of the fundamentals of RFID technology, $\chi 2(1, n = 317) = 6.1$, $p = .014$, phi = .15. The gender variations in familiarity with RFID technology could be attributed to how genders view and use emerging communication and information systems.

In the analysis between two of the generational groups, those born before 1980 and those who were born on or after 1980, a significant association was found between generational groups and familiarity with RFID technology. Of the 317 respondents, 141 or 44.5% indicated they were not familiar with RFID technology prior to the survey. Of the 141 respondents who were not familiar with RFID, 10 were born before 1980 and 131 were born on or after 1980. The researchers believe that the lack of familiarity with RFID technology of those born on or after 1980 was due to the growing ubiquity and transparency of the RFID enabled devices and generational indifferences toward privacy in the modern world.

Of the 176 respondents who acknowledged an awareness of RFID, 26 were born before 1980 and 150 were born on or after 1980. The research indicated that there was a significant association between generational groups and familiarity with RFID technology. A chi-square test for independence indicated a significant association between generational groups and familiarity with RFID technology prior to the researchers overview of the fundamentals of RFID technology, $\chi 2(1, n = 317) = 3.9$, $p = .05$, phi = phi = .12. This could signify that unfamiliarity and or an apprehension to technology can lead to generational and gender bias in preventing people from adopting RFID until its benefits are realized. It is possible that the disparity between the generational groups in their comprehension of the technology was that it was still an emerging technology in 2009.

Unfamiliarity and apprehension can lead to generational and gender bias and prevent people from adopting a new technology until its benefits are realized. As members of a university community, the survey population had most likely, knowingly or unknowingly, interacted with an RFID technology or device in the past.

DISCUSSION

Radio Frequency Identification (RFID) is an information and communication system that uses microchips to electronically collect, store, and share data from a distance. Common applications that used RFID technology included automatic toll collection systems, access control devices, passports, merchandise inventory control, and implanted pet ID tags. These common yet subtle RFID devices available to business and government have far-reaching means of invading privacy.

Hossain & Prybutok [4] reported three findings in their investigation on the dynamics that influence consumer acceptance of RFID technology. The outcome of the study suggested that convenience, culture, and security were significant factors in predicting a person's intention to use an RFID technology. First, it was suggested that the higher perceived level of convenience received from RFID technology, the higher the level of acceptance by consumers. Second, consumer levels of RFID technology were influenced by societal beliefs and value systems. Consumer norms and behaviors were also found to influence acceptance levels. Finally, consumers were less willing to use RFID technology when personal information was at risk. As mentioned previously the three factors that could predict a person's intention to use RFID technology were convenience, culture, and security. A major finding of the study, revealed that privacy, as a factor in adoption of RFID technology was insignificant.

The researchers believe that the foremost reason for this generational indifference to privacy and convenience is the amalgamation of communication technology and modern naïveté. People just no longer care what type of information they share or with whom it is shared. With the exponential growth of social networking sites on the Internet and the type of information that is shared on them, privacy is no longer sought after or desired. It is shunned.

What it means to be modern in 2010 is sharing nearly every conceivable aspect of your life with both friends and strangers over the numerous social networking sites available on the Internet. The glory days of confidently and anonymity will soon enter its final stages. Privacy most likely will become a quaint memory of past generations.

Digital dossiers set the person apart from the masses and confirm a person's individual passions and proclivities. These in turn could be used by the state to predict a person's future behavior (good or evil) and by businesses to determine individual spending habits [12]. Automatic identification and data collection (AIDC) systems are changing the world and altering how the concept of privacy is being interpreted by businesses, governments, and people.

FUTURE RESEARCH

It would be useful to revisit the same research population and conduct a follow-up survey with more detailed questions on their familiarity and awareness of RFID technology and devices. Additional studies of privacy loss concerns could be conducted separately on each of the RFID items appearing on the survey instrument.

Each of the items could play a pivotal roll in how people scrutinize their privacy in 2010 and in the future. It would also be useful to investigate if concerns of loss of privacy varied based on ethnicity or political attitudes. Finally, investigating other university communities of similar demographics could offer unique research opportunities to compare their differences and similarities as user acceptance expands and RFID technology evolves.

CONCLUSION

People give little thought to the information they post on the subject of themselves or others. They willingly share information on their proclivities and eccentricities with little concern as to who will read them. People seem to forget that once information is posted on the Internet, it is there for lack of a better term, eternity. Moreover, there appears to be little control that individuals have over what and how much information is gathered on them. Not surprising, even less is known about which government agencies and private businesses are collecting, storing, sharing, and analyzing people's digital dossiers.

Society has yet to experience the full impact and enormous influence RFID will play in the social order of communities, governments, and industries both today and in the future. Although fear, trust, and risk are an important characteristic of RFID acceptance, privacy loss fears should be a foremost concern for all people who live in a free and democratic society. Despite the known and yet unseen consequences (both positive and negative) that RFID systems may well create in the modern world, it is likely that RFID technology is here to stay. One unanswered question remains. Where will the RFID of the future take us?

REFERENCES

1. Best, S., J., Krueger, B., S., & Ladewig, J. (2006, Fall). The polls-trends: Privacy in the information age. *Public Opinion Quarterly*. 70(3), 375-401. Retrieved from ABI/INFORM Global database.

2. Field, A. (2008, October 2). RFID's new profile: As the hype has faded, the technology'simpact on supply chains is growing. *The Journal of Commerce*. Retrieved February 28, 2009 from http:// ww.joc.com/articles/ news.asp? section=SPEC2&sid=46578

3. Hawrylak, P., J., Mickle, M., H., & Cain, J., T. (2008). RFID Tags. In L. Yan, L. T. Yang, & H. Ning (Eds.), In The Internet of things: From RFID to the next-generation pervasive networked systems (pp. 1-32). Boca Raton, FL: Auerbach Publications.

4. Hossain, M. M., and Prybutok, V. R. (2007). Consumer acceptance of RFID technology:An exploratory study. *IEEE Transactions on Engineering Management*, 55(2), 316. Retrieved August 30, 2008 from ProQuest database. (Document ID: 1472047901).

5. Langheinrich, M. (2006). RFID and privacy. Retrieved April 30, 2009 from http://www.vs.inf.ethz.ch/publ/papers/langhein2006rfidprivacy.pdf

6. Lu, J., Yu, C., and Liu C. (2005). Facilitating conditions, wireless trust and adoption intention. *The Journal of Computer Information Systems*, 46(1), 17-24. Retrieved March 9, 2008 from Proquest database. (Document ID: 914802151).

7. Mjolsnes, S., F. & Teigen, M. (2007). A survey on trust and privacy negotiability in the Norwegian mobile telecom market. *Electronic Notes in Theoretical Computer Science*. (179), 135-142.

8. Sklavos, N. & Agarwal, V. (2008). RFID security: Threats and solutions. In L. Yan, Y. Zang, L. T. Yang, & H. Ning (Eds.), The Internet of things:

From RFID to the next-generation pervasive networked systems. New York: Auerbach Publications.

9. Solove, D., J. (2004). The digital person: technology and privacy in the information age. New York: New York University Press.

10. Spiekermann, S. (2005). Perceived controls: Scales for privacy in ubiquitous computing. (2005, July). Paper presented at the 10th International Conference on User Modeling. Available at SSRN: http://ssrn.com/abstract=761109

11. Spiekermann, S. & Ziekow, H. (2005, May). RFID: A 7- point plan to ensure privacy. Paper presented at the 13th European Conference on Information Systems in Regensburg. Available at SSRN: http://ssrn.com/abstract=761047

12. Vaidhyanathan, S. (2008, February 15). Naked in the nonopticon: Surveillance and marketing combine to strip away our privacy. *The Chronicle Review*. B7-B10.

13. Weinberg, J. (2006). RFID, privacy, and regulation. In S. Garfinkel & B. Rosenberg (Eds.). RFID: Applications, security, and privacy (pp. 83-97). Upper Saddle River, NJ: Addison-Wesley