Consumer Acceptance of RFID Technology: An Exploratory Study

Muhammad Muazzem Hossain, and Victor R. Prybutok, *Member, IEEE*

***Abstract*— Radio Frequency Identification (RFID) technology is used in numerous applications and offers a plethora of interesting potential new applications. However, this potential raises issues that require addressing to achieve its widespread acceptance by consumers. This paper investigates the factors that affect consumer acceptance of RFID technology. The purpose of this effort is to develop and test a theoretical model that contextualizes the Technology Acceptance Model (TAM) within the context of RFID technology. The research model proposes that convenience, culture, privacy, regulation, and security are the principal factors influencing the consumers' acceptance of RFID. However, the results show that convenience, culture, and security are significant predictors. This study is the first in the RFID literature to use the technology acceptance model for explaining consumer acceptance of RFID technology. The findings suggest that (1) higher perceived convenience of RFID technology leads to greater acceptance of this technology, (2) societal beliefs, value systems, norms, and/or behaviors influence the extent of consumer acceptance of RFID technology, and (3) higher perceived importance of and less willingness to sacrifice personal information security lead to lower intention to use RFID technology. Contextualization of TAM to RFID technology makes this study relevant to practitioners because the results can provide insight to organizations using or exploring the use of RFID technology.**

***Index Terms*— Consumer Acceptance, Contextualization, RFID Technology, Technology Acceptance Model.**

I. Introduction

RFID technology is gaining attention both from academicians and from practitioners. RFID has the potential to serve as a fundamental technology for ubiquitous services where both objects and people can be identified automatically via attached RFID tags [35]. However, with the promise of RFID technology come issues that need to be addressed for its widespread acceptance by consumers. For example, the use of RFID technology by retailers and government agencies raises questions about potential violation of personal information privacy [35], and potential security threats to personal information [40]. Motivated by such issues, this study proposes and validates a theoretical model of consumer acceptance of RFID technology. The proposed model is developed based on the extant literature and provides a theoretical framework of the critical factors that determine the consumer's acceptance of RFID technology. A contribution of this work involves reviewing the technology acceptance model and contextualizing it to the RFID technology. This contextualization is done with the intent of extending the technology acceptance model to the acceptance of a specific technology - RFID technology. This study is the first in the RFID literature to utilize and contextualize the technology acceptance model for explaining consumer acceptance of RFID technology.

A special issue of Communications of the ACM in 2005 (Vol. 48, No. 9) was devoted to RFID with a view to better understand RFID technology. RFID stands for Radio Frequency Identification and is a technology that uses electromagnetic transmission (i.e., radio waves) to store and retrieve data from an identification chip. This chip is called an RFID tag or transponder and is read by an RFID reader or transceiver without human interaction. An RFID system is comprised of five key components – RFID tag or transponder, reader/writer, encoder, middleware, and application software [20]. An RFID tag consists of a microchip and an antenna. The RFID reader/writer requests the identifying information contained in the microchip by sending an RF signal to the tag that then uses its antenna to transmit that information to the reader/writer via wireless data communication. The reader then translates the received information into a digital form and sends it to the application software with the help of middleware. The encoder, often the RFID reader/writer itself, encodes the data for storage in the tag once or many times, dependent upon whether the RFID tag is read-only tag or a read-write tag [20].

RFID was first invented in 1948 and has subsequently undergone several developmental stages [4]. In the 1950s, the explorations of RFID technology were confined to laboratory experiments while the development of theory and field trials with RFID took place in 1960s. The next decade saw an explosion in the development and testing of RFID technology. The commercial applications of RFID started in 1980s but in 1990s RFID became more widely deployed [4]. RFID technology is increasingly utilized to identify and track items and people via an automated passive process that uses the tags

Manuscript received September 1, 2006; revised June 27, 2007. Review of this manuscript was arranged by Department Editor A. Chakrabarti.

M. M. Hossain is with the Information Technology and Decision Sciences Department, College of Business Administration, University of North Texas, Denton, TX 76201 USA (e-mail: HossainM@unt.edu).

V. R. Prybutok is with the Information Technology and Decision Sciences Department, College of Business Administration, University of North Texas, Denton, TX 76201 USA (e-mail: prybutok@unt.edu).

[35].

RFID technology is already used in several consumer applications. Commuters around the world use RFID tags to automatically pay for public transport and tolls without waiting in line for a teller [36]. Some examples of such RFID tags include the T-Money in South Korea, EZ-Link Card in Singapore, Touch n Go Card in Malaysia, Octopus Card in Hong Kong, Oyster Card in London, Easy Card in Taiwan, EZ Tag in North Texas and Houston, FasTrak in California, Pikepass in Oklahoma, and SunPass in Florida. Microwave RFID tags are used by many car owners to access control of their vehicles [47]. For example, consumers of the Toyota Prius, Toyota Avalon, and Lexus brands can use their Smart Key, an RFID-enabled tag, to open doors and start their cars remotely. The RFID technology offers a plethora of interesting potential applications, such as the use of RFID in "microwave ovens that can read the tags on packages and cook food without explicit instructions, refrigerators that can recognize expired foods, and closets that can tally their contents" [25, p. 103].

However, review of the IS literature shows a lack of research about the consumer acceptance issues relevant to RFID technology. There are some fragmented studies in the IS literature that explore the factors affecting consumer acceptance of RFID technology. The extant literature suggests that companies providing RFID-based solutions must address the issues of privacy and security threats resulting from the use of RFID-based systems [35] [36], and capitalize on the convenience that RFID-based applications provide to the consumer [14]. RFID technology poses a set of unique challenges in terms of privacy, security, and monetary benefits [36], that are relevant to consumer acceptance of this technology becoming a part of daily activities.

Consumer acceptance of RFID technology is a complex issue, but the main focus of the consumer is likely to be the usefulness of the technology [24]. Various theories have evolved over the past half century to explain the adoption of a technology such as RFID by consumers. The Theory of Reasoned Action (TRA) developed by Fishbein and Ajzen [15] posits that behavior is a result of behavioral intention. Therefore, the consumers' intention to use RFID technology influences their acceptance of this technology. Thus, the consumer's intention to use RFID technology and the consumer's acceptance of RFID technology are used synonymously.

II. Theoretical Background

A review of the relevant literature suggests that the Technology Acceptance Model (TAM) [10] [11] and the Theory of Planned Behavior (TPB) [5] are the two widely used theoretical frameworks that are relevant to why users accept or reject information technology [30]. Numerous studies have validated the effectiveness of TAM in predicting the user's intention to use IT (e.g., [51] [2] [28]). IS researchers have extensively investigated TAM and extended it with constructs such as impulsiveness and social norms [51], perceived user resources [31], compatibility [7], perceived credibility [45], perceived financial cost [29], perceived financial resource [46], computer self-efficacy [3], and importance of service in online shopping environment [49]. Some studies employed TAM to explain individual differences in accepting information technology [32] and in understanding the cultural differences of technology acceptance [43] [33]. Because of the broad basis of applications established by TAM, TAM provides a foundation for this study. However, the RFID technology embodies some technological and usage-context factors such as privacy and security issues [35] [14] that potentially alter the traditional TAM model for use in explaining the user acceptance of this technology. The specific influences of such technological and usage-context factors are not entirely reflected by the principal constructs of TAM [11]. Thus, the constructs of TAM require modification to fit the context of RFID technology and TAM requires modification and extension to account for additional constructs that are suggested in the RFID literature. The model proposed in this study contextualizes the TAM to RFID technology by substituting the perceived convenience of using RFID technology for perceived usefulness and perceived ease of use of the technology because perceived convenience embodies both concepts. The contextualized model is then extended by adding four constructs – perceived privacy, perceived security, perceived regulations' influence, and perceived culture's influence. Perceived privacy and perceived security each consist of two dimensions resulting in four variables, namely – importance of privacy, unwillingness to sacrifice privacy, importance of security, and unwillingness to sacrifice security.

The Technology Acceptance Model

The TAM was originally proposed by Davis [10] and later was extended by Davis et al. [11]. The modified TAM incorporated into the original TAM a mediating variable (behavioral intention to use technology) that precedes the dependent variable (usage of the technology). TAM posits that perceived usefulness and perceived ease of use determine the user's intention to use information technology. Perceived usefulness is defined as the extent that an individual believes their job performance is enhanced by using a particular technology. Perceived ease of use is defined as the extent to which an individual believes that using a particular system is free of effort. TAM also postulates that perceived ease of use is a predictor of perceived usefulness.

Researchers have utilized and validated TAM for use with numerous types of technology [51]. Some studies suggest that TAM successfully predicts an individual's acceptance of various corporate information technologies (e.g., [8] [1] [39] [12]). According to Straub et al. [42], TAM may hold across technologies, people, settings, and times. Recently, TAM has its footprints in e-commerce [51] [50], and mobile service [46]. This study expands TAM to the study of consumer acceptance of the RFID technology.

III. Research Model and Hypotheses

This study proposes and validates the research model presented in Figure 1 based on the IS acceptance literature, especially Davis [10] and Davis et al. [11]. The research model is based on TAM, but substitutes perceived usefulness and perceived ease of use with perceived convenience of using RFID technology to contextualize TAM to RFID technology. The contextualized TAM is then extended by adding perceived cultural influence, perceived privacy, perceived regulations' influence, and perceived security to the model. Table I summarizes the research constructs.

TABLE I
Summary of Constructs

Constructs	Definition	Source
Perceived Convenience	The extent to which a consumer believes that using an RFID device would be comfortable, free of effort, and provide fitness of performing a task or fulfilling a requirement as of time and place.	Contextualized from TAM by Davis [10].
Perceived Culture's Influence	The extent to which a consumer believes that his or her society's beliefs, value systems, norms, or behaviors would influence the use of RFID technology.	Developed in this research by building upon Straub et al. [42] and McCoy et al. [33].
Perceived Privacy	The degree to which a consumer believes that he/she has the right to control the collection and use of his/her personal information, even after he/she has disclosed it to others.	Developed in this research by building upon Earp et al. [13] and Ohkubo et al. [35].
Perceived Security	The degree to which a consumer feels protected against security threats resulting from the use of RFID technology.	Developed in this study by building upon Smith [40].
Perceived Regulations' Influence	The extent to which a consumer believes that the use of law in RFID technology would generate desired outcomes.	Developed in this research by building upon Jones et al. [23].
Intention to Use	The likelihood to use in the future.	Modified from TAM by Davis [10].

A. Perceived Convenience (Perceived Usefulness and Perceived Ease of Use)

The dictionary definition of convenience includes usefulness, benefit, comfort, ease, and fitness. The perceived convenience of using RFID technology is defined as the extent to which a consumer believes that using an RFID device is comfortable, free of effort, and is fit for performing a task or fulfilling a requirement in a given time and place. Examining the above definition reveals two critical aspects of convenience – ease of use (includes comfortability and free of effort) and usefulness (includes fitness of performing tasks). These two aspects of perceived convenience are analogous to perceived ease of use and perceived usefulness, respectively, in the Technology Acceptance Model. Therefore, we posit that TAM is contextualized to RFID technology acceptance model by substituting perceived convenience for perceived ease of use and perceived usefulness.

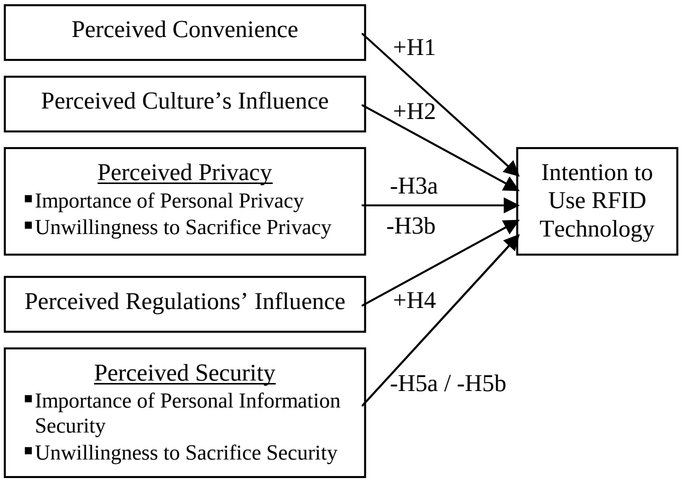
Perceived Convenience
+H1
Perceived Culture's Influence
+H2
Perceived Privacy
▪Importance of Personal Privacy
▪Unwillingness to Sacrifice Privacy
-H3a
-H3b
Intention to Use RFID Technology
Perceived Regulations' Influence
+H4
Perceived Security
▪Importance of Personal Information Security
▪Unwillingness to Sacrifice Security
-H5a / -H5b

Fig. 1: Research Model for Consumer Acceptance of RFID (CARFID) Technology

People tend to use a technology if they perceive that the technology is easy to use and will help them perform their job better [10]. Similarly, Eckfeldt [14] suggests that companies providing RFID-based solutions should leverage the potential convenience that RFID-based applications provide the consumer. For instance, the EZ-Pass toll collection system and ExxonMobil Corporation's Speedpass system remain highly successful RFID applications in terms of consumer acceptance because these systems provide consumers with greater convenience. According to Zhang and Prybutok [48], service convenience increases the consumers' satisfaction level and affects consumer intention. Therefore, RFID-based systems are more likely to achieve better adoption rates if they make the consumers' life more convenient [14]. Following this argument, the following alternative hypothesis can be proposed:

H_{a1}: The perceived convenience of using RFID technology has a significant positive influence on consumer intention to use this technology.

B. Perceived Culture's Influence

While culture is not easy to define, many researchers have attempted to do so. For instance, Hofstede [21] defined culture as "the collective programming of the mind which distinguishes the members of one human group from another" (p. 5). According to Kluckhohn [27], culture is the "ways of thinking, feeling and reacting, acquired and transmitted by symbols, constituting the distinctive achievements of human groups, including their embodiments in artifacts; the essential core of culture consists of traditional (i.e., historically derived and selected) ideas and especially their attached values" (p. 86). Integrating the above definitions, culture is defined as the beliefs, value systems, norms, or behaviors of a given organization, or society. Perceived culture's influence on RFID technology is, therefore, the degree to which an individual believes that his or her society's beliefs, value systems, norms, or behaviors would influence the use of RFID technology. Studies focused on culture's influence on the acceptance of technology provide mixed results. Straub et al. [42] suggest that a link between cultural factors and technology acceptance are not empirically established with certainty. However, McCoy et al. [33] extended the work of Straub et al. [42] by collecting culture data and validating TAM in Uruguay and the USA. They suggest that the technology acceptance model is appropriate to explain variations of intention to use a technology across cultures. In other words, the influence that a culture has on technology has a bearing on the intention to use the technology by the members of that culture. Thus, the following alternative hypothesis is proposed:

H_a2: The influence of culture on perceptions about RFID technology has a significant bearing on the intention to use RFID technology by the members of that culture.

C. Perceived Privacy

Privacy definitions vary according to both the context and the environment [37]. In the broadest sense, privacy is defined as the right to be left alone [23]. However, Privacy International [37] argues that there are four types of privacy - information privacy, bodily privacy, privacy of communications, and territorial privacy. The most relevant to the RFID technology acceptance debate is information privacy [23]. Information privacy is defined as the right of individuals to control the collection and use of their personal information, even after they have disclosed it to others. For instance, if an individual provides his/her personal information to a company while obtaining a product or a service, then he/she has the right to object to any further use of his/her information other than is necessary for delivery of the particular product or the service. Perceived privacy in the context of RFID technology and as used in this study is defined as the extent that a consumer has the right to control the collection and use of his/her personal information via RFID technology. RFID-based application systems pose various threats to personal information privacy. For example, in retailing, if personal identification data are linked to a unique product code and stored on an RFID tag, then retailers can build profiles of their customers and customer buying behaviors. This can help retailers infer not only their customers' buying behaviors but also characteristics of their customers' health, lifestyle, and travel [23]. The collection of personal information by organizations intensifies the consumers' concerns about personal privacy because the information collected is potentially available to third parties [13]. Ohkubo et al. [35] identified two privacy issues that complicate the adoption of RFID technology: leakage of the consumer's personal information and tracking of the consumer's physical location. However, Ohkubo et al. [35] also argue that perceptions of these privacy issues differ, depending upon personal tolerance. A consumer with lower personal tolerance for the above issues places higher importance on personal privacy and is less willing to sacrifice privacy than the one with a higher personal tolerance for such privacy issues. In other words, the perceived privacy of using RFID technology depends on how consumers perceive the importance of personal privacy and on the extent to which consumers are willing to sacrifice their personal privacy. A consumer with higher privacy concerns and less willingness to sacrifice personal privacy has a decreased likelihood of using RFID-based application systems than the consumer with lower concerns and some willingness to sacrifice personal privacy. Thus, the following alternative hypotheses can be postulated:

H_a3a: The higher the perceived importance of personal privacy, the lower the intention to use RFID technology.

H_a3b: The less willing the consumer is to sacrifice personal privacy, the lower their intention to use RFID technology.

D. Perceived Regulations' Influence

Regulation is generally defined as the use of law in generating desired outcomes. For example, regulating RFID technology implies that a law is enacted to ensure that the use of RFID technology complies with the requirements and standards outlined by the law. In this study, regulation is defined to include laws, privacy policies, and fair information practices. Prior studies suggest that regulations play a critical role in addressing potential privacy and security threats to personal data [35] [23] [38]. For instance, Squicciarini et al. [41] claim that privacy policies should identify the recipients for the user data, the intended use of the data, and how long the data will be retained. In the context of RFID technology, RFID developers, vendors and government regulatory agencies must recognize the privacy and security threats, and take appropriate countermeasures to increase the willingness of consumers to cooperate with the economic and social infrastructure of RFID technology [35]. In this vein, many consumer and privacy policy groups are calling for the development of privacy policy guidelines to protect consumers from privacy and security threats that potentially occur from the use of RFID technology [23]. Jones et al. [23] also argue that public policy guidelines regulating RFID technology are capable of increasing consumer trust and confidence in RFID. Furthermore, this increased consumer trust and confidence in RFID is more likely to improve the consumer acceptance rates of RFID technology. This implies that regulations have a significant positive influence on the future use of RFID technology. The alternative hypothesis that follows is:

H_a4: The consumers' perception of regulatory protections associated with RFID technology is positively associated with their intention to use RFID technology.

E. Perceived Security

Security refers to the protection against security threat, which is defined as a "circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse" [26]. This definition asserts that security threats can take place through network and data transactions attacks as well as through unauthorized access [6]. The use of RFID tags presents potential security threats because a third party can gather or steal personal information knowingly or unknowingly [40]. Security is a major issue pertaining to the acceptance of RFID-based applications. However, Smith [40] argues that RFID-based application systems should create improved customer satisfaction and loyalty. Such improved customer satisfaction gained from RFID-based technology increases the likelihood of future use of the technology. Therefore, the key to increased consumer acceptance of RFID technology is to assess the benefits of the technology from consumer’s point of view. Consumers accept security risks if they believe that the benefits accrued are worth the risk. In effect, consumers estimate the benefits and risk exposure before they willingly use a system [14]. This leads to the proposition that consumer acceptance of RFID technology is influenced by how consumers view the importance of security and how willing they are to sacrifice security against the benefits derived from the use of the technology. The following alternative hypotheses are based on the above proposition:

H_a5a: The higher the perceived importance of personal information security, the lower the intention to use RFID technology.

H_a5b: The less willing consumers are to sacrifice their personal information security, the lower their intention to use RFID technology.

IV. Research Methodology

One independent construct (perceived convenience) and the dependent construct (intention to use RFID) were contextualized from the technology acceptance model [10] to consumer acceptance of RFID technology model. The term contextualization was first used by linguists involved in translating biblical meanings into contemporary cultural contexts [19]. Formally adopted by scholars in the Theological Education Fund (TEF) in early 1950s, contextualization refers to correctly reading and relating the meaning of sections of the Bible to a specific context [18]. In this study contextualization involves modifying the constructs or ideas of a model to fit the context of the application. For instance, perceived convenience embodies perceived usefulness and perceived ease of use, which are two major constructs of the technology acceptance model. The technology acceptance model (TAM) [10] perspective is “to provide an explanation of the determinants of computer acceptance that is generally capable of explaining user behavior across a broad range of end-user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified” (p. 985). Consistent with this definition, TAM, provides the foundation for a generic technology acceptance construct. However, to relate TAM to a specific technology such as RFID technology we need to correctly understand the contextual issues of the TAM constructs as applicable to that specific technology. In the context of RFID technology, perceived usefulness and perceived ease of use delineate the concept of perceived convenience. We, therefore, contextualized these constructs from the technology acceptance model to perceived convenience in our consumer acceptance of RFID technology model. None of the other constructs were previously measured in the context of RFID usage. Thus proprietary scales for six independent constructs were developed based on prior literature and reviewed by experts in the field. The reviewers include university professors who have been teaching various courses on information technology for more than a decade and are actively involved in research in the field of RFID technology. Each reviewer was given a copy of the initial instrument comprised of 82 items measuring eight constructs and asked to comment. A pilot test with 15 experts who are pursuing doctoral degrees in information technology, logistics, and marketing also was conducted. The objective of review and pilot test was to ensure that none of the items were ambiguous and that the items adequately captured the domain of interest [9]. Seven items were eliminated based on the expert opinion. The final instrument (see Appendix I) consisted of a total of 75 items measuring seven independent variables and one dependent variable. Expert opinion indicated that the scales had adequate content validity. A few demographic variables were also included in the instrument. Responses to all items were measured using a 7 point Likert scale anchored between (1) strongly disagree and (7) strongly agree.

An online survey method was used to collect the data for the study. The survey was developed in ‘websurveyor’ and the link was emailed to the prospective respondents. The sample consisted of undergraduate and graduate students enrolled in various business courses in a major southwestern university in the United States, the University of North Texas. The University of North Texas is situated 35 miles north of Dallas, Texas, and is a leading public university in the region with a student population of almost 35,000. About 35% of its students commute from Dallas via the NTTA Tollway and President George Bush Turnpike [44]. Commuters using either of these two major roads often use NTTA TollTag, an RFID tag, to pay their toll. Therefore, a significant portion of the students at the University of North Texas are familiar with RFID toll technology. Thus the sample was appropriate for this study.

The survey was sent to 307 students and administered over a period of 24 days. Though it was a convenience sampling, these students were chosen to participate in the survey because they attended classes that provide an introduction to RFID technology about one month prior to the administration of the survey. Two hundred and fifty six usable responses were obtained at the end of the survey period. This represents a 83.4% response rate. The responses were divided into an early-response group and late-response group to check for any early-versus-late response bias. Independent samples t-tests were used to test for such bias in the data. Conducting t-tests using SPSS showed the absence of early-versus-late response bias.

V. Analyses and Results

The data was initially factor analyzed to identify the relevant factors. The results of the factor analysis for independent measures are shown in Table II and those for dependent measure in Table III. Table II shows that the factor analysis resulted in seven factors that measure the independent variables. The items loaded into factors as expected based on theory except for two items – CULOPU and REGSUP2. CULOPU, a measurement item of culture's influence on RFID technology, also loaded with the items of convenience with a cross-load of 0.314. REGSUP2, a measurement item of regulations' influence on RFID, simultaneously loaded with the items of security measurement with a cross-load of 0.324. Since the study is exploratory in nature, a cross-loading of less 0.5 is acceptable [17]. A separate factor analysis was conducted for the dependent measure. Table III shows that the factor analysis resulted in one factor for the dependent variable.

Insert Table II and Table III about here.

The reliability of the factors was checked using Cronbach's alpha. A Cronbach's alpha of 0.65 or higher [34] was used as an acceptable value for internal consistency of the measures. The Cronbach's alpha of the dependent variable (Intention to use RFID) is 0.868. The Cronbach's alphas for independent variables range from 0.699 to 0.958. These values support the contention that all the factors had adequate reliability, though the 0.699 value is marginal. The reliabilities of the factors are shown in Tables 2 and 3. The item-total correlations were examined to ensure that the factors have acceptable convergent validity. Factors are deemed to have adequate convergent validity if all item-total correlations equal or exceed the recommended criterion of 0.40 [22]. Table IV shows that all item-total correlations are more than the recommended criterion of 0.40, and supports the contention that the scales have adequate levels of convergent validity. The across factor correlations were then compared to the reliabilities of the scales to check whether the scales displayed adequate discriminant validity [16]. A construct has an adequate level of discriminant validity if the reliability of the construct is higher than the correlations between that construct and any other construct [16]. Table V shows that the scales also have adequate levels of discriminant validity.

Insert Table IV and Table V about here.

In order to test the proposed hypotheses, two methods of analysis were employed - multiple regression analysis and discriminant analysis.

A. Regression Analysis

Regression Analysis is a statistical tool concerned with evaluating the relationship between a dependent variable and one or more independent variables. The proposed research model (Figure 1) in this study has one dependent variable and seven independent variables. Summated scores of the respective factors were used to obtain the scores for both independent and dependent measures. For regression analysis, *Intention* was used as dependent variable, and *Convenience*, *Culture*, *PrivacyIMP*, *PrivacyWTS*, *Regulation*, *SecurityIMP* and *SecurityWTS* as independent variables.

The runs test, Levene's test and Kolmogorov-Smirnov tests were conducted to test for randomness, constancy of variance, and normality, respectively. These tests show that there is no evidence of violation of the assumptions underlying multiple regression analysis. Also, there is no evidence of multicollinearity because the VIFs and condition indices are within acceptable levels (VIFs < 4.00 and condition indices < 30.00).

The results of multiple regression analysis (Table VI) show that Convenience, Culture, SecurityIMP and SecurityWTS are significant predictors of intention to use RFID technology. These findings support four hypotheses (H1, H2, H5a and H5b). The results also show insufficient evidence for support of three hypotheses (H3a, H3b and H4), suggesting that PrivacyIMP, PrivacyWTS and Regulation play insignificant roles in predicting the intention to use RFID technology in the presence of the other variables.

Insert Table VI about here.

B. Discriminant Analysis

This study proposes that the perceived convenience of using RFID, perceived culture's influence on RFID, perceived importance of personal privacy, perceived unwillingness to sacrifice personal privacy, perceived regulations' influence on RFID, perceived importance of personal information security, and perceived unwillingness to sacrifice personal information security affect the intention to use RFID technology. A discriminant model was developed to show the underlying differences between the consumers who have higher intention to use RFID and those who have lower intention to use RFID. As an initial step, a cluster analysis was conducted. K-Means clustering revealed that the data can be clustered into two groups – the "high intention to use RFID" group and the "low intention to use RFID" group. A discriminant analysis was then conducted with these clusters as the dependent variables and the summated scores of Convenience, Culture, PrivacyIMP, PrivacyWTS, Regulation, SecurityIMP and SecurityWTS as the independent variables. The results of the Discriminant analysis are shown in Table VII.

Insert Table VII about here.

Consistent with the results of multiple regression analysis, the results of Discriminant analysis (Table VII) show that only Convenience, Culture, SecurityIMP and SecurityWTS play significant roles in discriminating the high intention to use RFID group from the low intention to use RFID group. But the p-value of Box's M statistic posits that there was evidence of a violation of the assumption of equal population variance structures. There are two types of assumptions underlying Discriminant analysis – the assumptions pertaining to the formation of the Discriminant function (normality, linearity, and multicollinearity) and the assumptions pertaining to the estimation of the discriminant function (equal variance and co-variances) [17]. Hair et al. [17] argue that the sensitivity of the test to normality, linearity and multicollinearity makes the significance of covariance differences less than 0.05 an acceptable level. Therefore, the evidence of the violation of the assumption of equal population variance structures does not distort the findings of the discriminant analysis that are in congruence with the findings of the regression analysis.

VI. Discussion and Implication

The objective of this study was to explore the factors that affect consumer acceptance of RFID technology. The findings suggest that convenience, culture and security are significant in predicting the intention to use RFID technology. However, surprisingly, and contrary to the prior literature, the issue of privacy as a factor to explain the future adoption of RFID technology was found insignificant. One plausible explanation for such a finding may lie in the nature of how the RFID technology is used. From consumers' point of view, the implementation of RFID technology (such as the implementation of an automatic toll collection system) is such that consumers often do not realize that their personal privacy is threatened. Therefore, as consumer awareness about RFID usage increases, consumers may better recognize the potential privacy threats that RFID technology presents [35]. Another explanation is that consumers are aware of the potential privacy threats that RFID technology presents but pay little attention to such issues. The underpinning of this argument is that consumers are rational decision-makers and believe that the benefits of using RFID technology (i.e., the convenience of using RFID technology) are greater than the potential privacy threat. Yet a third explanation of such contrary findings may lie in the pervasive and ubiquitous nature of technology. The ever-increasing growth of technology such as the internet influences perceptions about privacy issues. The more pervasive the positive influence of technology on people, the less the issue of personal privacy arises. Lastly, respondents could have provided significantly different responses depending on how they perceived the notion of privacy as it pertained to personal information. This is possible because personal information might have different meanings to different respondents. For instance, personal information might imply name and address to some respondents but social security number or health records to others.

As hypothesized, perceived convenience, perceived culture's influence, and perceived security were found to have significant influence on the consumer's willingness to accept the RFID technology. Perceived convenience has a positive impact on the consumer intention to use RFID technology. This implies that the higher the perceived convenience of RFID technology, the greater the consumer intention to use the technology. The influence of culture on perceptions about RFID technology is also a significant determinant of the consumer acceptance of this technology. That is, the extent of consumer acceptance of RFID technology is influenced by societal beliefs, value systems, norms, or behaviors. Another significant determinant of the consumer acceptance of RFID technology is the perception of personal information security. We found that the higher the perceived importance of personal information security and the lower the willingness to sacrifice personal information security, the lower the intention to use RFID technology.

Contrary to the proposed hypothesis, this study also found regulations were not relevant to predicting the intention to use RFID. There are two main reasons for such a contradictory finding. First, there are no well-defined, universal regulations as to the control, implementation and use of RFID technology. Second, the absence of such universal, comprehensible regulations leads to consumers' misunderstanding of what regulations can and will do to produce a desired outcome.

Contextualization of TAM to Consumer Acceptance of RFID Technology Model makes a unique contribution to the RFID literature, in particular, and to the IS literature, in general. Although numerous studies have utilized, validated and extended TAM to explain the acceptance of various technologies, this study is the first attempt in the IS literature to contextualize TAM within the RFID environment. The concept of contextualization of a model to fit the needs and requirements of specific phenomenon has manifold merits. First, contextualization benefits academicians by enabling them to personalize constructs for use in a study and as a result promotes both a diversity and uniqueness of academic research. Second, contextualization can help researchers to better understand research phenomena and to develop research models using native constructs rather than borrowing constructs from different contexts. Third, contextualization also provides a unique contribution to studies involving phenomena with peculiar characteristics. Such peculiarity is best explained by native concepts. The use of immigrant concepts may simply complicate the explanation of a phenomenon. Last, but not least, contextualization of TAM to RFID technology enhances the relevance of this study to organizations using or attempting to use RFID technology. Practitioners (e.g., organizations) value academic research more if the focus of such research is more pragmatic. Contextualization helps academicians conduct research by utilizing the contextual terminologies that both academicians and practitioners understand. Thus, it helps to bridge the gap between academicians and practitioners.

VII. Limitations and Future Direction

One of the major limitations of this study involves the sample. Despite the fact that students are consumers of RFID technology, the results from a student sample impose some limitations on the generalizability of these findings. Future research should test and validate the model by collecting data from a different composition of subjects.

Another issue relevant to this research is that several of the constructs used in this study are in the developmental stage. Although RFID technology was invented in 1940s, academic research in this field has only recently gained momentum. Since scientific studies on the acceptance of this technology are scarce, there isn’t a well-developed, meaningful scale to measure the constructs used in RFID related studies. Therefore, furthering the scale development of constructs relevant to the adoption of RFID technology stated in this study provides researchers with an excellent avenue for future research.

The research model presented in this study is based on an extensive review of prior literature on the acceptance of RFID technology. However, this study does not claim that a comprehensive, exhaustive list of factors has been identified. Future studies can extend the model by incorporating constructs that can supplement the model.

Finally, the purpose of this study was to explore the factors that have influenced the acceptance of RFID technology by consumers. However, the area of the adoption of RFID technology by organizations also offers tremendous research potential.

Appendix I

Survey Instrument

This survey aims at exploring the factors affecting consumer acceptance of RFID technology. RFID stands for *Radio Frequency Identification*. RFID technology uses radio waves to store data in and retrieve data from RFID tags using a RFID reader. Examples of RFID tags include automated toll tags, clickers used in classrooms to collect and record student responses, electronic tags attached to animals to track their identification, etc.

Please take about 10 minutes of your time to fill out this survey. There is no identifying information on this survey and your answers are completely anonymous. Please answer honestly because your frankness will help us understand important issues related to RFID technology. While this information is important to us, you are under no obligation to complete the survey. Also, if you are under the age of 18, please do not fill out this survey.

PART I: Please read the questions/statements and choose the option that best expresses your view using the following scale:
1 = Strongly Disagree
2 = Disagree
3 = Somewhat Disagree
4 = Neither Agree Nor Disagree
5 = Somewhat Agree
6 = Agree
7 = Strongly Agree

1) It is <u>IMPORTANT</u> to me to control the amount of access that each of the following has to my personal information.

My employer	1 2 3 4 5 6 7
My doctor	1 2 3 4 5 6 7
Government Agencies	1 2 3 4 5 6 7
My insurance companies	1 2 3 4 5 6 7
Companies from which you buy products or services	1 2 3 4 5 6 7
My Instructor	1 2 3 4 5 6 7

2) I am <u>WILLING</u> to share my personal information with the following.

My employer	1 2 3 4 5 6 7
My doctor	1 2 3 4 5 6 7
Government Agencies	1 2 3 4 5 6 7
My insurance companies	1 2 3 4 5 6 7
Companies from which you buy products or services	1 2 3 4 5 6 7
My Instructor	1 2 3 4 5 6 7

3) Evaluate the following statements.

Individuals should have the right to control the collection, use and dissemination of their personal information.	1 2 3 4 5 6 7
Individuals should have the right to control the collection, use and dissemination of their personal information.	1 2 3 4 5 6 7
I will not wear a clothing that has RFID tags attached because anyone with an RFID reader can read the data and build a profile of my consumer behavior	1 2 3 4 5 6 7

4) The following are <u>IMPORTANT</u> to me when I use a network system.

Computer and Network System Security	1 2 3 4 5 6 7
Client/Server Security	1 2 3 4 5 6 7
Secure Applications	1 2 3 4 5 6 7

Protection from Malicious Software	1 2 3 4 5 6 7
User Identification and Authentication	1 2 3 4 5 6 7
Backup and Recovery	1 2 3 4 5 6 7
Security Features (e.g., SET, SSL, locks, etc.)	1 2 3 4 5 6 7

5) I am WILLING to sacrifice the following in my decision to use a network system.

Computer and Network System Security	1 2 3 4 5 6 7
Client/Server Security	1 2 3 4 5 6 7
Secure Applications	1 2 3 4 5 6 7
Protection from Malicious Software	1 2 3 4 5 6 7
User Identification and Authentication	1 2 3 4 5 6 7
Backup and Recovery	1 2 3 4 5 6 7
Security Features (e.g., SET, SSL, locks, etc.)	1 2 3 4 5 6 7

6) Evaluate the following statements.

I will use RFID devices if I know that my personal information will be captured and stored securely.	1 2 3 4 5 6 7
I will not use RFID tags because they are not secure.	1 2 3 4 5 6 7

7) I SUPPORT the following, as they pertain to RFID.

Fair Information Practices	1 2 3 4 5 6 7
Regulations that protect Human Rights	1 2 3 4 5 6 7
Regulations by government to protect citizens	1 2 3 4 5 6 7
Regulations that protect Privacy Interpretations	1 2 3 4 5 6 7

8) Evaluate the following statements.

The US government should create an agency to protect US citizens from privacy invasions that may result from the use of RFID.	1 2 3 4 5 6 7
I support laws that will confer individuals with the right to know what information is gathered about them using RFID technology.	1 2 3 4 5 6 7
I believe that collecting sensitive information via RFID tags should be regulated.	1 2 3 4 5 6 7
Individuals should have the right to control the collection, use and dissemination of their personal information.	1 2 3 4 5 6 7

9) Evaluate the following statements.

I will not use any technology that conflicts with my social beliefs and norms.	1 2 3 4 5 6 7
Friends' opinions impact whether or not I will use RFID technology.	1 2 3 4 5 6 7
I will use RFID devices if the use of such devices helps me gain peer group acceptance.	1 2 3 4 5 6 7
I can make a more informed decision about the use of RFID devices if I know more about RFID technology.	1 2 3 4 5 6 7
I feel more comfortable using a technology that others are using.	1 2 3 4 5 6 7

10) I will use RFID technology in the following instances if the use of such technology SAVES me time.

Shopping for groceries	1 2 3 4 5 6 7
Paying bills	1 2 3 4 5 6 7
Paying tolls	1 2 3 4 5 6 7
Keeping financial records	1 2 3 4 5 6 7
Answering questions in class	1 2 3 4 5 6 7

11) I will use RFID technology in the following instances if the use of such technology is EASIER than that of the conventional methods.

Shopping for groceries	1 2 3 4 5 6 7
Paying bills	1 2 3 4 5 6 7
Paying tolls	1 2 3 4 5 6 7
Keeping financial records	1 2 3 4 5 6 7
Answering questions in class	1 2 3 4 5 6 7

12) I will be COMFORTABLE using RFID devices.

Always	1 2 3 4 5 6 7
Frequently	1 2 3 4 5 6 7
Sometimes	1 2 3 4 5 6 7
Never	1 2 3 4 5 6 7

13) I am WILLING to use RFID devices.

Always	1 2 3 4 5 6 7
Frequently	1 2 3 4 5 6 7
Sometimes	1 2 3 4 5 6 7
Never	1 2 3 4 5 6 7

PART II: Demographic Information

Please note, survey responses are completely anonymous.

14) What is your gender?
O Male
O Female

15) How old are you?
O 18-25
O 26-33
O 34-41
O 42-49
O 50 or older

16) What is your highest level of education completed?
O High School Graduate
O College Graduate
O Bachelor's Degree
O Master's Degree or above

Acknowledgment

M. M. Hossain thanks Dr. Rajasree Rajamma for her valuable suggestions. In addition, the authors acknowledge Prof. G. Farris, Prof. A. Chakrabarti, and the anonymous reviewers for their insightful comments on this paper.

REFERENCES

[1] D.A. Adams, R. R. Nelson, and P. A. Todd, "Perceived usefulness, ease of use, and usage of information technology: a replication," *MIS Quart.*, vol. 16, pp. 227-247, 1992.

[2] R. Agarwal, and E. Karahanna, "Time flies when you're having fun> Cognitive absorption and beliefs about information technology usage?" *MIS Quart.*, vol. 24, no. 4, pp. 665-693, 2000.

[3] R. Agarwal, V. Sambamurthy, and R. M. Stair, "Research report: the evolving relationship between general and specific computer self-efficacy – an empirical assessment," *Inf. Syst. Res.*, vol. 11, pp. 418-430, 2000.

[4] AIM, Inc. (2001). Shrouds of time: The history of RFID. [Online]. Available: http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.

[5] I. Ajzen, "The theory of planned behavior," *Org. Behavior and Human Dec. Processes*, vol. 50, pp. 179-211, 1991.

[6] F. Belanger, J. S. Hiller, and W. J. Smith, "Trustworthiness in Electronic Commerce: The Role of Privacy, Security and Site Attributes," *J. Strategic Inf. Syst.*, vol. 11, pp. 245-270, 2002.

[7] L.D. Chen, M. L. Gillenson, and D. L. Sherrell, "Enticing online consumers: an extended technology acceptance perspective," *Inf. and Manage.*, vol. 39, pp. 705-719, 2002.

[8] W.C. Chin, and P. A. Todd, "On the use, usefulness and ease of structural equation modeling in MIS research: a note of caution," *MIS Quart.*, vol. 19, pp. 237-246, 1995.

[9] G.A. Churchill, "A Paradigm for Developing Better Measures of Marketing Constructs," *J. of Marketing Res.*, vol. 16, pp. 64-73, 1979 (Feb).

[10] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quart.*, vol. 13, pp. 318-339, 1989.

[11] F.D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models," *Manage. Sci.*, vol. 35, pp. 982-1003, 1989.

[12] W.J. Doll, A. Hendrickson, and X. Deng, "Using Davis's perceived usefulness and ease of use instruments for decision making: a confirmatory and multi-group invariance analysis," *Dec. Sci.*, vol. 29, pp. 839-869, 1998.

[13] J.B. Earp, A. I. Anton, L. Aiman-Smith, and W. H. Stufflebeam, "Examining internet privacy policies within the context of user privacy values," *IEEE Trans. Eng. Manage.*, vol. 52, no. 2, pp. 227-237, 2005.

[14] B. Eckfeldt, "What does RFID do for the consumer?" *Comm. ACM*, 48(9), pp. 77-79, 2005.

[15] M. Fishbein, and I. Ajzen, "*Belief, attitude, intention and behavior: An introduction to theory and behavior*," Addison-Wesley, Reading, MA, 1975.

[16] J.F. Gaski, and J. R. Nevin, "The differential effects of exercised and unexercised power sources in a marketing channel," *J. Marketing Res.*, vol. 22, no. 2, pp. 130-142, 1985.

[17] J.F. Hair, R. E. Anderson, R. L. Tatham, and W. C. Black, *Multivariate Data Analysis*, Fifth edition, Prentice Hall, Upper Saddle River, NJ, 1998.

[18] D.J. Hesselgrave, "Contextualization that is authentic and relevant," *Intl. J. of Frontier Missions*, vol. 12, no. 3, pp. 115-120, 1995.

[19] D. J. Hesselgrave, and E. Rommen, *Contextualization: Meanings, Methods, and Models*, Grand Rapids: Baker Book House, 1989.

[20] HighJump Software, A 3M Company. (2004). The true cost of radio frequency identification. [Online]. Available: http://highjumpsoftware.com/promos/rfid-cost-report.asp.

[21] G.H. Hofstede, *Culture Consequences: International Differences in Work-related Values*, Sage Publications, London, 1980.

[22] R.K. Jayanti, and A. C. Burns, "The Antecedents of Preventive Health Care Behavior: An Empirical Study," *J. Acad. Marketing Sci.*, vol. 26, no. 1, pp. 6-15, 1998.

[23] P. Jones, C. Clarke-Hill, D. Hillier, P. Shears, and D. Comfort, "Radio frequency identification in retailing and privacy and public policy issues," *Manage. Res. News*, vol. 27, no. 8/9, pp. 46-56, 2004.

[24] R.L. Juban, and D.C. Wyld, "Would you like chips with that?: Consumer perspectives of RFID," *Manage. Res. News*, vol. 27, no. 11/12, pp. 29-44, 2004.

[25] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," *CCS*, Washington, DC, 2003.

[26] R. Kalakota, and A. B. Whunston, *Frontiers of electronic commerce*, Addition-Wesley, Reading, MA, 1996.

[27] C. Kluckhohn, "Values and value-orientation in the theory of action: An exploration in definition and classification," In T. Parsons & E. Shils (Eds.), *Toward a general theory of action*. Cambridge, MA: Harvard University Press, pp. 388-433, 1951.

[28] M.L. Korzaan, "Going with the flow: Predicting online purchase intentions," *J. Comp. Inf. Syst.*, vol. 43, no. 4, pp. 25-31, 2003.

[29] P. Laurn, and H. H. Lin, "Toward an understanding of the behavioral intention to use mobile banking," *Comp. in Human Behavior*, vol. 21, pp. 873-891, 2005.

[30] P. Legris, J. Ingham, and P. Gollerette, "Why do people use information technology? A critical review of the technology acceptance model," *Inf. And Manage.*, vol. 40, pp. 191-204, 2003.

[31] K. Mathieson, E. Peacock, and W. W. Chin, "Extending the technology acceptance model: the influence of perceived user resources," *DATA BASE for Adv. In Inf. Syst.*, vol. 32, pp. 86-112, 2001.

[32] D. McCloskey, "Evaluating electronic commerce acceptance with the technology acceptance model," *J. Comp. Inf. Syst.*, vol. 44, no. 2, pp. 49-57, 2003.

[33] S. McCoy, A. Everard, and B. M. Jones, "An examination of the technology acceptance model in Uruguay and the US: A focus on culture," *J. Global Inf. Tech. Manage.*, vol. 8, no. 2, pp. 27-45, 2005.

[34] J.C. Nunnally, *Psychometric theory*, Second edition, McGraw-Hill, New York, 1978.

[35] M. Ohkubo, K. Suzuki, and S. Kinoshita, "RFID privacy issues and technical challenges," *Comm. ACM*, vol. 48, no. 9, pp. 66-71, 2005.

[36] A.R. Peslak, "An ethical exploration of privacy and radio frequency identification," *J. Bus. Ethics*, vol. 59, pp. 327-345, 2005.

[37] Privacy International. (2003). Privacy and human rights 2003: Overview. [Online]. Available: http://www.privacyinternational.org/survey/phr2003/overview.htm.

[38] C.M. Roberts, "Radio frequency identification (RFID)," *Comp. and Security*, vol. 25, pp. 18-26, 2006.

[39] A.H. Segars, and V. Grover, "Re-examining perceived ease of use and usefulness: a confirmatory factor analysis," *MIS Quart.*, vol. 17, pp. 517-525, 1993.

[40] A. Smith, "Exploring radio frequency identification technology and its impact on business systems," *Inf. Manage. And Comp. Security*, vol. 13, no. 1, 16-28, 2005.

[41] A.C. Squicciarini, E. Bertino, E. Ferrari, and I. Ray, "Achieving privacy in trust negotiations with an ontology-based approach," *IEEE Trans. On Dependable and Secure Comp.*, vol. 3, no. 1, pp. 13-30, 2006.

[42] D.W. Straub, M. Keil, and W. Brenner, "Testing the technology acceptance model across cultures: A three country study," *Inf. And Manage.*, vol. 33, pp. 1-11, 1997.

[43] S. Taylor, and P. Todd, "Assessing IT usage: the role of prior experience," *MIS Quart.*, vol. 19, no. 4, pp. 561-570, 1995.

[44] University of North Texas Fall 2003 Parking/Transportation Survey. (2003). Available: http://www.unt.edu/ir_acc/Surveys/Fall_2003_Transportation_Survey/Fall%202003%20Parking-Transportation%20Report.pdf.

[45] Y.S. Wang, "The adoption of electronic tax filing systems: an empirical study," *Govt. Inf. Quart.*, vol. 20, pp. 333-352, 2003.

[46] Y.S. Wang, Y. M. Wang, H. H. Lin, and T. I. Tang, "Determinants of user acceptance of internet banking: an empirical study," *Intl. J. Service Industry Manage.*, vol. 14, pp. 501-519, 2003.

[47] R. Want, "RFID: A key to automating everything," *Sci. American*, vol. 290, no. 1, pp. 56, 2004.

[48] X. Zhang, and V. R. Prybutok, "A consumer perspective of e-service quality," *IEEE Trans. Eng. Manage.*, vol. 52, no. 4, pp. 461-477, 2005.

[49] X. Zhang, and V. R. Prybutok, "An empirical study of online shopping: A service perspective," *Intl. J. Services Tech. and Manage.*, vol. 5, no. 1, pp. 1-13, 2004.

[50] X. Zhang, and V. R. Prybutok, "Application of TAM: the moderating effect of gender on online shopping," *Intl. J. Inf. Tech. Manage.*, vol. 12, no. 2, pp. 99-118, 2003.

[51] X. Zhang, V. R. Prybutok, and C. E. Koh, "The role of impulsiveness in a TAM-based online purchasing behavior model," *Inf. Resources Manage. J.*, vol. 19, no. 2, pp. 54-68, 2006.

Muhammad M. Hossain received his Bachelor of Business Administration (BBA) degree in 1996 from the International Islamic University, Malaysia, and an MS in Information Technologies in 2004 from the University of North Texas, Denton, Texas, USA. Currently, he is pursuing his Ph.D. in Management Science in the College of Business Administration at the University of North Texas. He is a member of the International Honor Society Beta Gamma Sigma and active in the Decision Sciences Institute. He has presented several papers at conferences that include the Annual Meeting of Decision Sciences Institute and the Baldrige Award Recipients (BAR) Consortium.

Victor R. Prybutok is a Regents Professor of Decision Sciences in the Information Technology and Decision Sciences Department and Director of the Center for Quality and Productivity in the College of Business Administration at the University of North Texas. He received, from Drexel University, his B.S. with High Honors in 1974, an M.S. in Bio-Mathematics in 1976, a M.S. in Environmental Health in 1980, and a Ph.D. in Environmental Analysis and Applied Statistics in 1984. He is a senior member of the American Society for Quality (ASQ) and active in the American Statistical Association, Decision Sciences Institute, Institute of Electrical and Electronic Engineers, and Operations Research Society of America. Dr. Prybutok is an ASQ certified quality engineer, certified quality auditor, certified quality manager, and served as a Texas Quality Award Examiner in 1993. Journals where his over 80 published articles have appeared include The American Statistician, Communications of the ACM, Communications in Statistics, Data Base, Decision Sciences, European Journal of Operational Research, IEEE Transactions on Engineering Management, MIS Quarterly, OMEGA: The International Journal of Management Science, and Operations Research. In addition, he is in Who's Who in American Education and Who's Who in America, and Who's Who in the South and Southwest.

TABLE II
ROTATED COMPONENT MATRIX: INDEPENDENT VARIABLES

Items	Components						
	1	2	3	4	5	6	7
1. Convenience: Perceived Convenience of Using RFID							
CONEAS3: I will use RFID technology in paying tolls if the use of such technology is easier than that of the conventional methods	**0.853**	0.036	-0.021	0.036	0.037	0.074	0.003
CONSAV1: I will use RFID technology in shopping for groceries if the use of such technology saves me time	**0.824**	0.020	-0.102	0.005	-0.032	-0.027	0.111
CONSAV3: I will use RFID technology in paying tolls if the use of such technology saves me time	**0.821**	0.070	-0.033	-0.078	0.033	0.046	0.014
CONEAS5: I will use RFID technology in answering questions in class if the use of such technology is easier than that of the conventional methods	**0.814**	-0.028	-0.014	0.091	-0.084	0.083	-0.045
CONEAS2: I will use RFID technology in paying bills if the use of such technology is easier than that of the conventional methods	**0.811**	0.018	-0.112	0.057	-0.079	0.029	0.194
CONEAS1: I will use RFID technology in shopping for groceries if the use of such technology is easier than that of the conventional methods	**0.811**	0.045	-0.068	0.004	-0.038	-0.020	0.114
CONSAV2: I will use RFID technology in paying bills if the use of such technology saves me time	**0.794**	0.093	-0.145	0.028	-0.096	-0.004	0.216
CONSAV5: I will use RFID technology in answering questions in class if the use of such technology saves me time	**0.772**	0.048	0.053	0.059	-0.151	0.108	-0.019
CONEAS4: I will use RFID technology in keeping financial records if the use of such technology is easier than that of the conventional methods	**0.676**	-0.084	-0.237	-0.011	-0.116	0.117	0.243
2. SecurityIMP: Perceived Importance of Personal Information Security							
SCTIMP3: Secure Applications are important to me when I use a network system	0.047	**0.900**	0.252	0.130	-0.012	0.091	-0.014
SCTIMP2: Client/Server Security is important to me when I use a network system	0.020	**0.880**	0.223	0.123	0.011	0.140	-0.010
SCTIMP1: Computer and Network System Security are important to me when I use a network system	0.016	**0.868**	0.222	0.131	-0.009	0.118	0.012
SCTIMP5: User Identification and Authentication are important to me when I use a network system	0.036	**0.864**	0.198	0.112	-0.054	0.151	-0.063
SCTIMP4: Protection from Malicious Software is important to me when I use a network system	0.088	**0.842**	0.216	0.138	-0.043	0.165	-0.057
SCTIMP7: Security Features (e.g., SET, SSL, locks, etc.) are important to me when I use a network system	0.071	**0.815**	0.254	0.090	-0.012	0.131	-0.037
SCTIMP6: Backup and Recovery are important to me when I use a network system	-0.004	**0.737**	0.215	0.126	-0.069	0.170	0.004
3. SecurityWTS: Perceived Unwillingness to Sacrifice Security							
rcSCTWIL3: (Reverse Coded) I am willing to sacrifice secure applications in my decision to use a network system	-0.073	0.206	**0.912**	0.035	0.041	0.027	-0.089
rcSCTWIL1: (Reverse Coded) I am willing to sacrifice computer and network system security in my decision to use a network system	-0.081	0.187	**0.904**	0.007	0.067	0.031	-0.049
rcSCTWIL2: (Reverse Coded) I am willing to sacrifice client/server security in my decision to use a network system	-0.079	0.186	**0.896**	-0.017	0.064	0.048	-0.088
rcSCTWIL4: (Reverse Coded) I am willing to sacrifice protection from malicious software in my decision to use a network system	-0.015	0.224	**0.863**	-0.003	-0.003	0.082	-0.094
rcSCTWIL5: (Reverse Coded) I am willing to sacrifice user identification and authentication in my decision to use a network system	-0.118	0.249	**0.843**	0.013	0.016	0.035	-0.019
rcSCTWIL7: (Reverse Coded) I am willing to sacrifice security features (e.g., SET, SSL, locks, etc.) in my decision to use a network system	-0.080	0.281	**0.836**	0.010	0.010	0.028	-0.068
rcSCTWIL6: (Reverse Coded) I am willing to sacrifice backup and recovery in my decision to use a network system	-0.141	0.159	**0.776**	-0.030	0.018	-0.020	0.019
4. PrivacyIMP: Perceived Importance of Personal Privacy							
PVCIMP4: It is important to me to control the amount of access that my insurance companies have to my personal information	0.040	0.086	**0.004**	0.862	0.103	0.062	-0.005
PVCIMP3: It is important to me to control the amount of access that government agencies have to my personal information	0.126	0.101	**0.019**	0.836	0.087	0.026	0.023
PVCIMP6: It is important to me to control the amount of access that my instructor has to my personal information	-0.051	0.159	**-0.027**	0.835	-0.008	0.059	0.002
PVCIMP1: It is important to me to control the amount of access that my employer has to my personal information	0.045	0.115	**-0.033**	0.825	0.081	0.024	-0.034
PVCIMP5: It is important to me to control the amount of access that companies from which I buy products or services have to my personal	-0.012	0.180	**0.041**	0.788	-0.005	0.121	-0.036

information							
5. PrivacyWTS: Perceived Unwillingness to Sacrifice Privacy							
rcPVCWIL4: (Reverse Coded) I am willing to share my personal information with my insurance companies	-0.110	-0.081	**0.047**	0.084	0.823	0.080	-0.025
rcPVCWIL3: (Reverse Coded) I am willing to share my personal information with government agencies	-0.006	-0.048	**0.009**	0.104	0.790	-0.058	0.041
rcPVCWIL1: (Reverse Coded) I am willing to share my personal information with my employer	-0.128	-0.111	**-0.002**	-0.017	0.769	-0.179	0.069
rcPVCWIL6: (Reverse Coded) I am willing to share my personal information with my instructor	-0.117	0.094	**0.097**	0.058	0.686	0.081	0.059
6. Regulation: Perceived Regulations' Influence on RFID							
REGSUP3: I support regulations by government to protect citizens, as they pertain to RFID	0.033	0.299	**0.051**	0.081	-0.029	0.858	-0.021
REGSUP2: I support regulations that protect human rights, as they pertain to RFID	0.115	0.324	**0.086**	0.112	0.061	0.830	-0.051
REGSUP1: I support Fair Information Practices, as they pertain to RFID	0.178	0.201	**0.035**	0.112	-0.083	0.747	0.075
7. Culture: Perceived Culture's Influence on RFID							
CULIFO: Friends' opinions impact whether or not I will use RFID technology	0.154	-0.043	**-0.109**	-0.013	0.076	-0.027	0.822
CULOPU: I feel more comfortable using a technology that others are using	0.314	0.138	**0.016**	-0.027	-0.018	0.126	0.725
CULPGA: I will use RFID devices if the use of such devices helps me gain peer group acceptance	0.163	-0.270	**-0.226**	-0.016	0.132	-0.096	0.669
Cronbach's Alpha	**0.935**	**0.958**	**0.958**	**0.899**	**0.785**	**0.848**	**0.699**
Factor Mean	**4.548**	**6.080**	**5.420**	**5.273**	**4.233**	**5.309**	**3.561**
Factor Standard Deviation	**1.564**	**1.171**	**1.508**	**1.491**	**1.362**	**1.269**	**1.331**

Scale Anchor: 1 = Strongly Disagree; 7 = Strongly Agree

TABLE III
ROTATED COMPONENT MATRIX: DEPENDENT VARIABLE

Items	Component
	1
ITUCOM2: I will frequently be comfortable using RFID devices	**0.902**
ITUWIL2: I am frequently willing to use RFID devices	**0.883**
ITUCOM1: I will always be comfortable using RFID devices	**0.868**
ITUWIL1: I am always willing to use RFID devices	**0.866**
ITUCOM3: I will sometimes be comfortable using RFID devices	**0.503**
Cronbach's Alpha	**0.868**
Factor Mean	**3.526**
Factor Standard Deviation	**1.376**

TABLE IV
SCALE RELIABILITY AND CONVERGENT VALIDITY

Scale Items	Corrected Item-Total Correlation	Cronbach's Alpha
Independent Measures		
1. Convenience: Perceived Convenience of Using RFID		**0.935**
CONEAS1: I will use RFID technology in shopping for groceries if the use of such technology is easier than that of the conventional methods	0.759	
CONEAS2: I will use RFID technology in paying bills if the use of such technology is easier than that of the conventional methods	0.806	
CONEAS3: I will use RFID technology in paying tolls if the use of such technology is easier than that of the conventional methods	0.791	
CONEAS4: I will use RFID technology in keeping financial records if the use of such technology is easier than that of the conventional methods	0.673	

CONEAS5: I will use RFID technology in answering questions in class if the use of such technology is easier than that of the conventional methods	0.752	
CONSAV1: I will use RFID technology in shopping for groceries if the use of such technology saves me time	0.777	
CONSAV2: I will use RFID technology in paying bills if the use of such technology saves me time	0.790	
CONSAV3: I will use RFID technology in paying tolls if the use of such technology saves me time	0.746	
CONSAV5: I will use RFID technology in answering questions in class if the use of such technology saves me time	0.707	
2. Culture: Perceived Culture's Influence on RFID		**0.699**
CULIFO: Friends’ opinions impact whether or not I will use RFID technology	0.597	
CULOPU: I feel more comfortable using a technology that others are using	0.475	
CULPGA: I will use RFID devices if the use of such devices helps me gain peer group acceptance	0.479	
3. PrivacyIMP: Perceived Importance of Personal Privacy		**0.899**
PVCIMP1: It is important to me to control the amount of access that my employer has to my personal information	0.739	
PVCIMP3: It is important to me to control the amount of access that government agencies have to my personal information	0.749	
PVCIMP4: It is important to me to control the amount of access that my insurance companies have to my personal information	0.785	
PVCIMP5: It is important to me to control the amount of access that companies from which I buy products or services have to my personal information	0.712	
PVCIMP6: It is important to me to control the amount of access that my instructor has to my personal information	0.763	
4. PrivacyWTS: Perceived Unwillingness to Sacrifice Privacy		**0.785**
rcPVCWIL1: (Reverse Coded) I am willing to share my personal information with my employer	0.598	
rcPVCWIL3: (Reverse Coded) I am willing to share my personal information with government agencies	0.606	
rcPVCWIL4: (Reverse Coded) I am willing to share my personal information with my insurance companies	0.669	
rcPVCWIL6: (Reverse Coded) I am willing to share my personal information with my instructor	0.504	
5. Regulation: Perceived Regulations' Influence on RFID		**0.848**
REGSUP1: I support Fair Information Practices, as they pertain to RFID	0.601	
REGSUP2: I support regulations that protect human rights, as they pertain to RFID	0.776	
REGSUP3: I support regulations by government to protect citizens, as they pertain to RFID	0.782	
6. SecurityIMP: Perceived Importance of Personal Information Security		**0.958**
SCTIMP1: Computer and Network System Security are important to me when I use a network system	0.875	
SCTIMP2: Client/Server Security is important to me when I use a network system	0.893	
SCTIMP3: Secure Applications are important to me when I use a network system	0.924	
SCTIMP4: Protection from Malicious Software is important to me when I use a network system	0.862	
SCTIMP5: User Identification and Authentication are important to me when I use a network system	0.869	
SCTIMP6: Backup and Recovery are important to me when I use a network system	0.74	
SCTIMP7: Security Features (e.g., SET, SSL, locks, etc.) are important to me when I use a network system	0.831	
7. SecurityWTS: Perceived Unwillingness to Sacrifice Security		**0.958**
rcSCTWIL1: (Reverse Coded) I am willing to sacrifice computer and network system security in my decision to use a network system	0.895	
rcSCTWIL2: (Reverse Coded) I am willing to sacrifice client/server security in my decision to use a network system	0.888	
rcSCTWIL3: (Reverse Coded) I am willing to sacrifice secure applications in my decision to use a network system	0.916	
rcSCTWIL4: (Reverse Coded) I am willing to sacrifice protection from malicious software in my decision to use a network system	0.854	
rcSCTWIL5: (Reverse Coded) I am willing to sacrifice user identification and authentication in my decision to use a network system	0.845	
rcSCTWIL6: (Reverse Coded) I am willing to sacrifice backup and recovery in my decision to use a network system	0.738	
rcSCTWIL7: (Reverse Coded) I am willing to sacrifice security features (e.g., SET, SSL, locks, etc.) in my decision to use a network system	0.844	
Dependent Measure		
1. Intention: Intention to Use RFID		**0.868**
ITUCOM1: I will always be comfortable using RFID devices	0.754	
ITUCOM2: I will frequently be comfortable using RFID devices	0.834	
ITUCOM3: I will sometimes be comfortable using RFID devices	0.369	
ITUWIL1: I am always willing to use RFID devices	0.742	
ITUWIL2: I am frequently willing to use RFID devices	0.79	

TABLE V
DISCRIMINANT VALIDITY OF CONSTRUCTS

	Convenience	SecurityIMP	SecurityWTS	PrivacyIMP	PrivacyWTS	Regulation	Culture
Convenience	**0.935 ***						
SecurityIMP	0.364	**0.958**					
SecurityWTS	0.062	-0.033	**0.958**				
PrivacyIMP	-0.181	0.084	0.116	**0.899**			
PrivacyWTS	0.182	-0.003	0.230	-0.069	**0.785**		
Regulation	0.058	-0.124	0.286	-0.064	0.476	**0.848**	
Culture	-0.181	-0.234	0.042	0.073	0.160	0.470	**0.699**

* The diagonal values are alpha scores.

TABLE VI
REGRESSION ANALYSIS PREDICTING INTENTION TO USE RFID

Predictors	**Unstd. Beta Coeff**	**Std Beta Coeff**	**t-Stat**	**p-Value**	**VIF**	**Hypothesis**	**Hypothesized Effect**	**Supported?**
Convenience	0.355	0.403	7.329	0.000	1.290	H_a1	+	Yes
Culture	0.299	0.289	5.357	0.000	1.239	H_a2	+	Yes
PrivacyIMP	-0.017	-0.019	-0.357	0.721	1.149	H_a3a	-	No
PrivacyWTS	-0.014	-0.013	-0.264	0.792	1.106	H_a3b	-	No
Regulation	0.042	0.039	0.689	0.492	1.350	H_a4	+	No
SecurityIMP	-0.160	-0.136	-2.129	0.034	1.750	H_a5a	-	Yes
SecurityWTS	-0.107	-0.117	-2.033	0.043	1.417	H_a5b	-	Yes
R	0.646							
R^2	0.418							
Adjusted R^2	0.401							

TABLE VII
DISCRIMINANT ANALYSIS: INTENTION TO USE RFID AND DETERMINANTS

	High Intention to Use RFID		Low Intention to Use RFID		Equality of Group Means		Canonical Discriminant Function Coeff
	Mean	SD	Mean	SD	F	p-value	
Convenience	5.082	1.272	4.084	1.648	28.807	0.000	0.339
Culture	4.008	1.150	3.173	1.359	27.738	0.000	0.351
PrivacyIMP	5.176	1.340	5.356	1.611	0.925	0.337	-0.065
PrivacyWTS	4.122	1.325	4.330	1.392	1.494	0.223	-0.073
Regulation	5.325	1.149	5.294	1.368	0.037	0.848	0.110
SecurityIMP	5.862	1.154	6.270	1.156	7.951	0.005	-0.219
SecurityWTS	4.947	1.604	5.831	1.291	23.835	0.000	-0.277
Discriminant Analysis Results	Box's M *	= 81.000		F	= 2.808	p-value	= 0.000
	Wilks' Lambda	= 0.801		p-value	= 0.000	Hit Ratio	= 67.2%

* Tests null hypothesis of equal population covariance matrices.