CIN: Computers, Informatics, Nursing • Vol. 30, No. 10, 531–537 • Copyright © 2012 Wolters Kluwer Health | Lippincott Williams & Wilkins

CONTINUING EDUCATION

Predicting Nurses' Acceptance of Radiofrequency Identification Technology

ADAM NORTEN, PhD

The technology of radiofrequency identification allows for the scanning of radiofrequency identification–tagged objects and individuals without line-of-sight requirements. Healthcare organizations use radiofrequency identification to ensure the health and safety of patients and medical personnel and to uncover inefficiencies. Although the successful implementation of a system incorporating radiofrequency identification technologies requires acceptance and use of the technology, some nurses using radiofrequency identification in hospitals feel like "Big Brother" is watching them. This predictive study used a theoretical model assessing the effect of five independent variables: privacy concerns, attitudes, subjective norms, controllability, and self-efficacy, on a dependent variable, nurses' behavioral intention to use radiofrequency identification. A Web-based questionnaire containing previously validated questions was answered by 106 US RNs. Multiple linear regression showed that all constructs together accounted for 60% of the variance in nurses' intention to use radiofrequency identification. Of the predictors in the model, attitudes provided the largest unique contribution when the other predictors in the model were held constant; subjective norms also provided a unique contribution. Privacy concerns, controllability, and self-efficacy did not provide a significant contribution to nurses' behavioral intention to use radiofrequency identification.

KEY WORDS

Nurses • Radiofrequency identification • Radiofrequency identification device • RFID

Hospitals and medical centers benefit from the tracking capabilities that radiofrequency identification (RFID) technologies offer, using RFID tags to follow the locations of supplies and individuals.[1] For example, to uncover inefficiencies in hospital operations, Massachusetts General Hospital in Boston uses RFID to track the locations of physicians and patients at three of its clinics, transmitting their ID number every 10 seconds, pinpointing them to within 3 ft.[2] Stanford University Medical Center and New York Presbyterian Hospital use RFID technology to monitor patient location.[1] Doctors and nurses at Englewood Hospital in Englewood, NJ, hold their RFID badges up to an RFID interrogator to access the hospital's clinical information system.[3] Singapore health officials had RFID sensors installed in hospital ceilings during an outbreak of severe acute respiratory syndrome to monitor individuals entering and leaving Singapore General Hospital.[1] Shady Palms, an assisted-living facility center in Tampa, FL, uses RFID tags inserted into the clothing of residents with dementia to track their movements.[4]

Radiofrequency identification is an unobtrusive technology that facilitates electronic transmission of potentially sensitive data without line-of-site requirements and without the sender's active participation or knowledge.[5,6]

Author Affiliation: East-West University, Chicago, IL.

The author received no financial support from any individuals or entities pertaining to this article.

The author has disclosed that he has no significant relationships with, or financial interest in, any commercial companies pertaining to this article.

Corresponding author: Adam Norten, PhD, (norten@comcast.net).

DOI: 10.1097/NXN.0b013e31825e1eef

Radiofrequency identification systems feature two components: an RFID tag and a reader or interrogator.[1] An RFID tag or transponder consists of an antenna and integrated chip or silicon chip that holds information concerning the item to which it is attached,[1] in the form of a numeric Electronic Product Code[1] or alphanumeric identifiers generated in accordance with the American National Standards Institute/Health Industry Bar Code 4.0 standard.[7]

The RFID interrogator creates a radiofrequency field[8] that automatically receives the signal and responds using

radio waves.[1,8] Active RFID tags contain batteries to facilitate data transmission. Batteries remain off until switched on by radio waves from the RFID interrogator.[1] Passive RFID tags are affixed to food products including fresh meat[9]; retail items such as clothing,[10] watches, purses, shoes, and jewelry[6]; in restaurants to track plates of sushi; in law firms to monitor the location of files; and by corporations to monitor where servers, storage drives, laptops, and other equipment in data centers are located.[11] Government and nongovernment entities also use RFID tags to track weapons, keys, and tools.[12] Individuals can purchase products, such as tamper-resistant ankle bands that can easily be placed on infants[13] to monitor babies who are vulnerable to sudden infant death syndrome,[14] or to start cars.[15]

Fisher and Monahan[16] uncovered an unintended consequence of hospitals' use of RFID. Hospital staff members, particularly nurses, expressed negative views of hospitals using RFID, concerned that they were being overly scrutinized and felt like "Big Brother" was watching them. In a 2006 pilot project, hospital staff members, including doctors and nurses who were required to wear the tags, expressed their dislike of constant monitoring.[17]

A nurses' union has taken the position that identification badges embedded with RFID tags constitute an invasion of the nurses' right to privacy.[18] Several strong nurses' unions have eschewed implementation of RFID systems.[16] "Even if the stated intention is "workflow management," the implications for nurses are those of labor intensification, job insecurity, undesired scrutiny, and privacy loss."[19(p122)] Some works suggested negative consequences may ensue from RFID required use, including "sabotage or employee separation from the organization."[20(p291)] Ohkubo et al[6] warned that, without proper safeguards, the RFID tag may contain potentially sensitive data that can be retrieved surreptitiously.

Studies of the factors that influence the attitudes of certain groups of individuals to accept or reject RFID did not include nurses.[21,22] In this investigation, the researcher examined attitudes toward RFID use among US RNs. To ensure that RFID technologies are used to their fullest capabilities, their impact on nurses needs to be understood.[16] Greater efficiency and security through the use of RFID technologies will not be achieved if nurses do not want to use the technology.

CONCEPTUAL FRAMEWORK/ RESEARCH GAP

Two main theories aim to explain whether an individual will accept or reject technology: the technology acceptance model (TAM)[23] and the theory of planned behavior (TPB).[24] The TAM and TPB are based on the theory of reasoned action (TRA),[25] rooted in social psychology.[26] The TRA posits that an individual's intent to engage in a behavior is the major determinant of whether the individual engages in that behavior.[27] Behavior is influenced by attitude and by subjective norms.[27]

The TPB focuses on how individuals' external environments influence their intentions, whereas TAM focuses on how individuals' perceptions influence their intentions.[28] Whereas TRA considers behavior only as influenced by attitude and subjective norms, TPB adds perceived behavioral control as a third construct affecting behavior.[27] According to Cammock et al,[27] attitude reflects "an individual's favorable or unfavorable evaluation of a particular behavior."[27(p401)] Subjective norms refer to an individual's perceptions of others' desires that he/she perform a particular behavior, whereas perceived behavioral control focuses on an individual's perception of the ease or difficulty of performing a given behavior.[27] Ajzen[29] in 2002 proposed that the TPB introduced by Ajzen[24] in 1991 be modified by separating the construct of perceived behavioral control into two separate constructs: self-efficacy and controllability. Cammock et al[27] called this new model the ETPB and concluded that the ETPB proved a superior model over the TRA and conventional TPB in that it "accounted for 60% of the variance in behavioral intentions."[27(p411)]

PROPOSED CONCEPTUAL MODEL

The researcher proposed a model, based on the extant literature and ETPB of Cammock et al[27] adding the construct of "privacy."[21,22,27,30] This theoretical framework assessed nurses' intention to use RFID technology, including privacy concerns, attitudes toward RFID technology (attitudes), social pressure (subjective norms), perception of control over their RFID technology usage (controllability), and belief in their ability to use RFID technology (self-efficacy).[21,22,27,30] In a qualitative study using interviews and participant observation, Fisher and Monahan[16] studied privacy concerns of hospital staff members, particularly nurses, in regard to their being tracked by their employers through the use of RFID technologies. The results indicated that nurses expressed concern about being overly scrutinized and felt that they were being watched.

To conduct this study investigating the impact of privacy concerns on nurses' behavioral intention to use RFID, the researcher built a concept map (Figure 1) based on research conducted by Hossain and Prybutok,[21] Muller-Seitz et al,[22] and Xu and Gupta.[30] Hossain and Prybutok[21] found that privacy did not affect consumer intention to use RFID technology. In their study, Xu and Gupta[30] also determined that privacy issues did not affect consumer intention to use a positioning technology, found in a mobile telephone, which provided location tracking similar

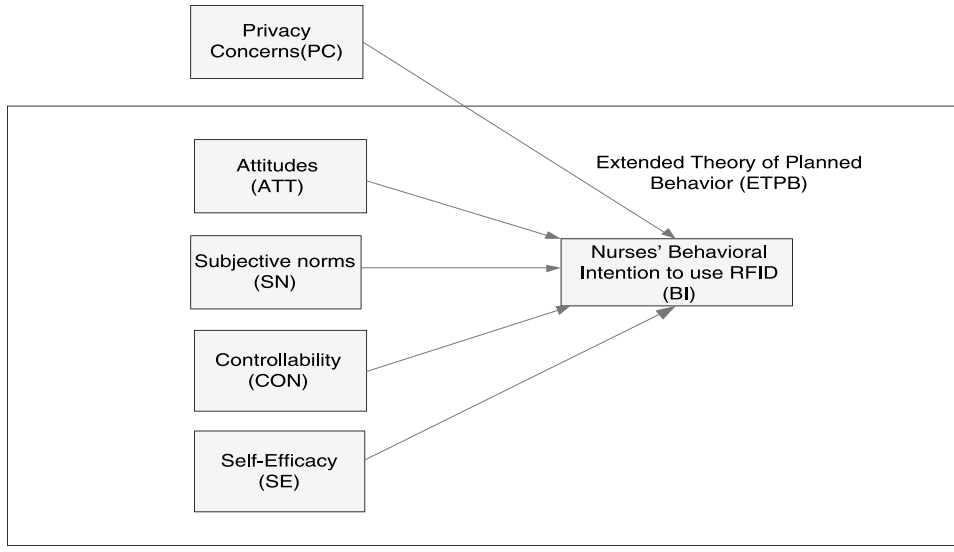

FIGURE 1. Proposed concept map of ETPB,[27] with the additional construct of privacy concerns.[21,22,30]

to RFID. These results are in contrast to those of Muller-Seitz et al[22] and studies by Gunther and Spiekermann,[31] Jensen et al,[32] Rothensee and Spiekermann,[33] and Spiekermann[34] that identified privacy as a key factor affecting RFID acceptance.

RESEARCH QUESTION

What is the relative strength of the contribution of the five independent variables (ie, privacy concerns, attitudes, subjective norms, controllability, and self-efficacy) in predicting nurses' behavioral intention to use RFID?

METHODS

Institutional Review Board Approval

Inasmuch as this study involved human subjects, the researcher obtained approval of the questionnaire from Nova Southeastern University's institutional review board.

Measurement

Using a quantitative research design and survey methodology, US nurses responded to questions designed to elicit their views on the impact of each of the model's five constructs (ie, privacy concerns, attitudes, subjective norms, controllability, and self-efficacy) and their impacts on nurses' intention to use RFID technology. Responses were analyzed statistically.

The researcher used previously validated items and distinctly defined variables to measure the effect of privacy concerns, attitudes, subjective norms, controllability, and self-efficacy on behavioral intention. The instrument was distributed through the Web, enabling the researcher to communicate rapidly with sizeable groups while facilitating an environment of openness and participation at a reasonable cost.[35] Web-based questionnaires support collection of data and eliminate errors in data entry.[36,37] The questionnaire, a 32-item instrument with items answered by a five-point Likert scale,[38] was constructed using validated survey questions from Xu and Gupta,[30] Taylor and Todd,[39] and Cammock et al.[27] Using existing variables, rather than creating new constructs, was suggested by Leidner and Jarvenpaa.[40]

In this investigation, the internal consistency and reliability of each of the subscales were measured using Cronbach's α. Questionnaire items were evaluated for directionality, and those with a reversed directionality were reverse scored to guarantee that items were scored in the same direction.[41] This study used external validity,[42,43] content validity,[44] and construct validity[45] to ensure valid results.

Sample

The target population for this study was male and female US RNs 18 years and older. Because the researcher was unable to find hospitals willing to participate in a study that sought to gather information that may have reflected negatively on them, sampling nurses who are using RFID was not an option. Instead, the survey was conducted online. Information concerning the work or professional affiliations of the nurses surveyed was not sought.

To ensure that the sample was representative of the target population, the study used Zoomerang's TrueSample feature. Using Zoomerang (SurveyMonkey, Palo Alto, CA), a researcher can distribute an online survey to individuals meeting certain demographic and behavioral criteria and monitor their responses in real time. The TrueSample feature removes fake, duplicate, and unengaged respondents from the research sample, thus preventing them from compromising the integrity the survey results. The criteria chosen for the study included age (18 years or older), country (United States), and profession (RNs). The sample of US RNs was directed to a Web-based instrument on which they answered questions designed to elicit their views on the five constructs in the model (ie, privacy concerns, attitudes, subjective norms, controllability, and self-efficacy) and the constructs' impact on their behavioral intention to use RFID technology.

A medium effect size (0.15–0.34)[46] was used to calculate the sample size. The program G*Power 3.1.0 was used to determine the sample size of 92 participants (G*Power version 3.1.0, Universität Kiel, Kiel, Germany).

Data Collection/Data Analysis

The survey was made available to each participating nurse using a Web-based survey provider. Participation was voluntary and anonymous. A total of 106 nurses completed the survey, and 103 survey responses comprised the data set.

Before data analysis was performed, preanalysis data screening confirmed that conclusions were founded on valid data[47] and assisted in identifying any problems or anomalies in the data collected.[36] To eliminate participant error in inputting responses, data were sent directly from the Web-based questionnaire to a spreadsheet and inputted into statistical formats using PASW 18.0 software (SPSS: An IBM Company, Chicago, IL).

This study investigated the five independent variables—privacy concerns, attitudes, subjective norms, controllability, and self-efficacy—and their impact on the dependent or criterion variable, nurses' behavioral intention to use RFID technology. To this end, standard multiple linear regression was used, with all the independent (predictor) variables inserted into the model simultaneously. Variables were assessed by how much they added to the value of the prediction of dependent (criterion) variable.[48] An F test determined whether the group of independent variables, taken together, predicted the dependent variable.[48] R^2, also known as the coefficient of determination, was used to calculate how much variance can be attributed to the group of independent variables.[48] β Coefficients were used to calculate the amount each independent variable predicted, and a *t* test calculated the significance of the predictors.[48]

RESULTS

Descriptive Analysis

To examine the research question, multiple linear regression was used to develop a predictive model to measure the contribution of privacy concerns, attitudes, subjective norms, controllability, and self-efficacy to behavioral intention to use RFID.[49] The multiple linear regression equation for this study was defined as[49]

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + e.$$

The multiple linear regression model used in this investigation was

$$\mathrm{BI} = \beta_0 + \beta_{\mathrm{PC}} * PC + \beta_{\mathrm{ATT}} * ATT + \beta_{\mathrm{SN}} * SN + \beta_{\mathrm{Con}} * CON + \beta_{\mathrm{SE}} * SE + e,$$

where behavioral intention is the dependent variable behavioral intention, PC is privacy concerns, ATT is attitudes, SN is subjective norms, CON is controllability, and SE is self-efficacy.

The multiple linear regression model was statistically significant, $F_{5,97} = 29.15$, $P < .001$, $R^2 = 0.60$, indicating that the model of five variables effectively predicted behavioral intention to use RFID (Table 1). The combination of predictors accounted for 60% of the variance in nurses' behavioral intention to use RFID. Of the five predictors in the model, attitudes provided the largest unique contribution when the other predictors in the model were held constant, $t = -7.95$, suggesting that, as the nurses' attitudes increased by one unit of agreement, their behavioral intention to use RFID decreased by 0.69 units.

Subjective norms also provided a unique contribution, $t = 2.58$, suggesting that, as subjective norms increased by one unit of agreement, behavioral intention to use RFID increased by 0.18 units of agreement (Table 1). The other predictors in the model (privacy concerns, controllability, and self-efficacy) were not statistically significant and did not provide significant unique contributions toward nurses' behavioral intention to use RFID. The

Table 1

Multiple Linear Regression With Survey Subscales Predicting Behavioral Intention to Use RFID

Variable	*B*	SE	β	*t*	*P*
Privacy concerns	0.03	0.09	0.03	0.36	.720
Attitudes	−0.67	0.09	−0.69	−7.95	.001
Subjective norms	0.19	0.07	0.18	2.58	.011
Controllability	−0.04	0.07	−0.04	−0.64	.525
Self-efficacy	0.13	0.08	0.11	1.61	.111

$F_{5,97} = 29.15$, $P < .001$, $R^2 = 0.60$.

null hypothesis that privacy concerns, subjective norms, controllability, and self-efficacy do not predict nurses' behavioral intention to use RFID was thus rejected.

DISCUSSION/IMPLICATIONS

Using multiple linear regression analysis, the study sought to determine the relative strength of the contribution of the five independent variables (ie, privacy concerns, attitudes, subjective norms, controllability, and self-efficacy) in predicting nurses' behavioral intention to use RFID. Attitudes provided the largest unique contribution when the other five predictors in the model were held constant. Subjective norms also provided a unique contribution. The other predictors in the model, including the privacy concerns construct, which had not previously been applied in the context of RFID usage in the field of nursing, did not provide unique contributions to nurses' behavior intention to use RFID. All the constructs together accounted for 60% of the variance in nurses' intention to use RFID.

A theoretical model using the variables of privacy concerns, attitudes, subjective norms, controllability, and self-efficacy to predict nurses' behavioral intention to use RFID was developed. The main contributions are (1) the development and empirical validation of a theoretical model that predicts 60% of the variance in nurses' behavioral intention to use RFID technologies and (2) the determination of the factors that most affect nurses' behavioral intention to use RFID technologies. The researcher's conclusions should aid in understanding issues that must be addressed when nurses are required to use RFID technologies.

There are two implications resulting from this investigation. First, the study's findings showed a strong connection between nurses' attitudes and their behavioral intention to use RFID. As in Taylor and Todd,[39] attitude "reflects feelings of favorableness or unfavorableness toward performing a behavior."[39(p149)] Significantly, the nurses surveyed were presented with a scenario in which they were required to use RFID, but still expressed strong opinions about their intention to use RFID. Thus, each nurse's attitude toward RFID will play a role in determining his/her actual use of RFID and ultimately the success or failure of the RFID system as a whole. Hospitals and medical centers with RFID-based tracking systems that depend on their nurses carrying, wearing, or using RFID-tagged badges, equipment, or supplies overlook the attitudes of their nurses toward RFID at their own risk. To reap the benefits that RFID has to offer, the hospitals and medical centers should seek to understand and address any issues, concerns, or reservations their nurses have regarding the technology. The hospitals and medical centers can thereby improve work satisfaction among their nurses, facilitate greater engagement among their nurses with the technology, and promote the success of their RFID installations.

In addition, multiple linear regression showed that subjective norms (social pressure to perform or not perform a certain behavior) affected nurses' intention to use RFID in a mandatory-use environment. Although the results were less significant than those concerning attitudes, they suggest that, to ensure that their nurses use RFID technologies as intended, healthcare facilities should consider uncovering and addressing issues concerning subjective norms.

Second, the research model developed for this investigation, which predicted 60% of the variance in nurses' behavioral intention to use RFID, can help information-systems practitioners and researchers. In particular, the research model can aid researchers in better understanding some of the factors affecting nurses' acceptance of RFID technologies, thus providing the basis for further research addressing these issues.

LIMITATIONS AND RECOMMENDATIONS

Study results lend themselves to many areas of future research. Investigating the views of healthcare professionals other than US RNs, such as doctors, pharmacists, and medical technicians, would offer insight into how different medical professionals respond to being required to use RFID technologies.

Asking survey respondents to verify whether they are familiar with, use, or have used RFID technologies at their places of employment could be part of future research. The current study asked nurses about hypothetical rather than actual use of RFID technologies. Surveying nurses and other healthcare professionals who use RFID technologies could yield different results from those found in this study. Including other healthcare organizations that use RFID technologies, such as assisted-living and advanced care facilities, could likewise make the results more generalizable.

Finally, investigating the literature for other factors affecting RFID acceptance, such as perceived security,[21] security concerns,[22] security trust,[50] or employee knowledge of RFID,[50] could be incorporated into future studies. To keep the present study manageable, it was not an inclusive analysis of every factor influencing RFID technology acceptance.

CONCLUSION

This study aimed to develop a model (Figure 1) based on the analysis of the effect of privacy concerns, attitudes, subjective norms, controllability, and self-efficacy on nurses' behavioral intention to use RFID. The study queried what factors affect nurses' behavioral intention

to use RFID. The researcher developed a 32-item Web-based survey, based on existing validated scales, which used Likert-scaled items to determine the factors that affect nurses' behavioral intention to use RFID. Of those 32 items, 12 addressed privacy concerns, eight queried attitudes, two questioned subjective norms, three addressed controllability in the instrument, four interrogated self-efficacy, and three inquired about behavioral intention.

The research model predicted that privacy concerns, attitudes, subjective norms, controllability, and self-efficacy would have a significant effect on nurses' behavioral intention to use RFID. Multiple linear regression showed that the constructs together accounted for 60% of the variance in nurses' intention to use RFID. Of the five predictors in the model, attitudes provided the largest unique contribution when the other predictors in the model were held constant. Subjective norms also provided a unique contribution.

REFERENCES

1. Littman MK. Implementing RFID technology in hospital environments. In: Wickramasinghe N, Geisler E, eds. *Encyclopedia of Healthcare Information Systems*. Vol. 2. Hershey, PA: Medical Information Science Reference; 2008:705–710.
2. Swedberg C. Massachusetts General uses RFID to better understand its clinics. *RFID J*. Published November 15, 2007. http://www.rfidjournal.com/article/print/5324. Accessed October 5, 2011.
3. Bacheldor B. N.J. medical center uses LF tags to protect patient records. *RFID J*. Published November 14, 2007. http://www.rfidjournal.com/article/articleprint/3747. Accessed October 5, 2011.
4. O'Connor MC. RFID gives dementia patients their freedom. *RFID J*. February 10, 2009. http://www.rfidjournal.com/article/print/4610. Accessed October 5, 2011.
5. Consumers Against Supermarket Privacy Invasion and Numbering, Privacy Rights Clearinghouse, American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center, Junkbusters, Privacy Activism. *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations*. San Diego, CA: PRC; 2003. http://www.privacyrights.org/ar/RFIDposition.htm. Accessed October 5, 2011.
6. Ohkubo M, Suzuki K, Kinoshita S. RFID privacy issues and technical challenges. *Commun ACM*. 2005;48(9):66–71.
7. O'Connor MC. Health industry group issues RFID standard, but excludes UHF for consumable items. *RFID J*. Published August 14, 2009. http://www.rfidjournal.com/article/print/5131. Accessed October 5, 2011.
8. Uddin MJ, Ibrahimy MI, Reaz MBI, Nordin AN. Design and application of radio frequency identification systems. *Eur J Sci Res*. 2009;33(3):438–453.
9. Jones S. Advances in RFID tracking for meatpackers. *BarCode News*. Published August 2, 2011. http://barcode.com/20110802631/advances-in-rfid-tracking-for-meatpackers.html. Accessed October 11, 2011.
10. O'Connor MC. Bloomingdale's tests item-level RFID. *RFID J*. Published August 26, 2009. http://www.rfidjournal.com/article/print/5160. Accessed October 5, 2011.
11. Totty M. New ways to use RFID. *Wall Street J*. Published June 2, 2009. http://online.wsj.com/article/SB10001424052970203771904574175882366028604.html#printMode. Accessed October 5, 2011.
12. Oak Ridge National Laboratory. *Low-Frequency Radio Identification* [brochure]. Published January 25, 2009. http://www.ornl.gov/sci/ees/mssed/pdf/ADS_LFRID_Fact_Sheet_January_2009_R1.pdf. Accessed October 11, 2011.
13. Swedberg C. Tamper-resistant RFID infant-tracking system improves security. *RFID J*. Published August 27, 2008. http://www.rfidjournal.com/article/print/4285. Accessed October 5, 2011.
14. Swedberg C. Researchers use RFID to fight SIDS. *RFID J*. Published April 17, 2007. http://www.rfidjournal.com/article/print/3252. Accessed October 5, 2011.
15. Newitz A. The RFID hacking underground. *Wired*. Published May 2007. http://www.wired.com/wired/archive/14.05/rfid.html. Accessed October 5, 2011.
16. Fisher JA, Monahan T. Tracking the social dimensions of RFID systems in hospitals. *Int J Med Inform*. 2008;77:176–183.
17. Miller JJ, Ferrin DM, Flynn T, Ashby M, White KP Jr, Mauer MG. Using RFID technologies to capture simulation data in a hospital emergency department. In: *Proc 2006 Winter Simulation Conf*. Monterey, CA: Winter Simulation Conference; 2006:1365–1371.
18. Chanen JS. The boss is watching. *Am Bar Assoc J*. 2008;94:49–53. http://www.abajournal.com/magazine/article/the_boss_is_watching/. Accessed October 5, 2011.
19. Monahan T. *Surveillance in the Time of Insecurity*. Piscataway, NJ: Rutgers University Press; 2010.
20. Brown S, Massey A, Montoya-Weiss M, Burkman J. Do I really have to? User acceptance of mandated technology. *Eur J Inform Syst*. 2002;11:283–295.
21. Hossain MM, Prybutok VR. Consumer acceptance of RFID technology: an exploratory study. *IEEE Trans Eng Manage*. 2008;55:316–328.
22. Muller-Seitz G, Dautzenberg K, Creusen U, Stromereder C. Customer acceptance of RFID technology: evidence from the German electronic retail sector. *J Retail Consumer Serv*. 2009;16:31–39.
23. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q*. 1989;133:319–339.
24. Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Proc*. 1991;50:179–211.
25. Fishbein M, Ajzen I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley; 1975.
26. Koskela T, Julkunen J, Keranen V, Kostamo N, Ylianttila M. User experiences on a community-based music voting service. In: *2009 IEEE Congress on Services*. Los Angeles, CA: IEEE Computer Society; 2009:747–753.
27. Cammock T, Carragher N, Prentice G. Undergraduate intentions to apply to the Northern Ireland civil service: the application of a theory of planned behavior model. *Eur J Soc Psychol*. 2009;39:401–414.
28. Liu D-S, Chen W. An empirical research on the determinants of user m-commerce acceptance. In: Lee R, ed. In: *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*. Berlin, Germany: Springer; 2009;209:93–104.
29. Ajzen I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *J Appl Soc Psychol*. 2002;32:665–683.
30. Xu H, Gupta S. The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electr Markets*. 2009;19:137–149.
31. Gunther O, Spiekermann S. RFID and the perception of control: the consumer view. *Commun ACM*. 2005;48(9):73–76.
32. Jensen AS, Cazier JA, Dave DS. Mitigating consumer perceptions of privacy and security risks with the use of residual RFID technologies through governmental trust. *J Inform Syst Security*. 2008;4(1):41–66.
33. Rothensee M, Spiekermann S. Between extreme rejection and cautious acceptance: consumers' reactions to RFID-based IS in retail. *Soc Sci Comput Rev*. 2007;26(1):75–86.
34. Spiekermann S. RFID and privacy: what consumers really want and fear. *Pers Ubiquit Comput*. 2009;13:423–434.
35. Rhodes SD, Bowie AD, Hergenrather CK. Collecting behavioral data using the World Wide Web: considerations for researchers. *J. Epidemiol Commun Health*. 2003;57:68–73.
36. Levy Y. *Assessing the Value of E-Learning Systems*. Hershey, PA: Information Science; 2006.

37. Porter S, Whitcomb EM. The impact of contact type on Web survey response rate. *Public Opin Q*. 2003;67:579–588.
38. Norten A. *User Acceptance of RFID Technology in a Mandatory-Use Environment* [dissertation]. Fort Lauderdale–David, FL: Nova Southeastern; 2011.
39. Taylor S, Todd P. Understanding information technology usage: a test of competing models. *Inform Syst Res*. 1995;6(23):144–176.
40. Leidner DE, Jarvenpaa SL. The use of information technology to enhance management school education: a theoretical view. *MIS Q*. 1995;19(3):265–291.
41. Howell DC. *Statistical Methods for Psychology*. Belmont CA: Wadsworth Cengage Learning; 2010.
42. King WR, He J. External validity in IS survey research. *Commun Assoc Inform Syst*. 2005;16:880–894.
43. Leedy PD, Ormrod JE. *Practical Research: Planning and Design*. Upper Saddle River, NJ: Prentice Hall; 2005.
44. Boudreau M, Gefen D, Straub DW. Validation in information systems research: a state-of-the-art assessment. *MIS Q*. 2001;25(1):1–16.
45. Straub DW. Validating instruments in MIS research. *MIS Q*. 1989;13(2):147–170.
46. Cohen J. A power primer. *Psychol Bull*. 1992;112(1):155–159.
47. Mertler CA, Vannatta RA. *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*. Los Angeles, CA: Pyrczak; 2001.
48. Tabachnick BG, Fidell LS. *Using Multivariate Statistics*. Boston, MA: Allyn & Bacon; 2006.
49. Hair JF, Black WC, Babin BJ, Anderson RE. *Multivariate Data Analysis*. Upper Saddle River, NJ: Prentice Hall; 2010.
50. Lee MS. An empirical study about RFID acceptance—focus on the employees in Korea. *Int J Bus Econ Finance Manage Sci*. 2009;1:78–87.