December 2006

The Role of Privacy Risk in IT Acceptance: An Empirical Study

Joseph Cazier
Appalachian State University

Vance Wilson
University of Wisconsin- Milwaukee

B. Dawn
Appalachian State University

The Role of Privacy Risk in IT Acceptance: An Empirical Study

Joseph A. Cazier
Appalachian State University
cazierja@appstate.edu

Vance Wilson
University of Wisconsin- Milwaukee
wilsonv@uwm.edu

B. Dawn Medlin
Appalachian State University
medlinbd@appstate.edu

ABSTRACT
Privacy risk is increasingly entering the public consciousness when it comes to use of information technology (IT). To gain insight into the role of risk in the technology adoption process, we studied the use of information systems for student registration and schedule management at two major U.S. universities. We extended the Technology Acceptance Model (TAM) with perceptual measures of privacy risk harm and privacy risk likelihood which apply to the extended model and predict students' intentions to use technology. Privacy risk factors are found to negatively influence intention and contribute substantially to model predictiveness. This finding underlines the growing importance of privacy risk in the use of IT.

KEYWORDS: TECHNOLOGY ACCEPTANCE MODEL (TAM), RISK, PRIVACY, SECURITY

INTRODUCTION

In The U.S., The Past Few Decades Have Seen The Proliferation Of It Into Virtually Every Aspect Of Business And Personal Life. As A Nation, We Regularly Use It To File Taxes, Conduct Banking And Financial Transactions, Order Pizzas, And Even Search For A Mate Or Buy A Car. The General Trend Has Been To Consider It In Terms Of The Benefits That Can Accrue To Individuals Or Organizations. However, Information Technology Is "Morally Neutral" In That It Can Be Employed For Either Positive Or Negative Uses (Conca, Medlin, & Dave, 2005, P. 167). For Example, E-Mail Can Be A Highly Useful Form Of Communication In Routine Work Situations Or For Sharing Information Among Friends Or Family. However, Email Can Also Be Used For The Dissemination Of Malicious Computer Code And Viruses.

Negative Aspects Of It, Such As Phishing, Spyware, Spamming, And Malicious Code, Are Forcing The Public To Reassess The Risks Of Use. In Response, Many Americans Have Stopped Doing Things Online That They Have Done In The Past—For Example, A Recent Ibm Study Finds 18% Of Participants Have Stopped Paying Bills Online (Ibm, 2006). We Propose It Is Becoming Increasingly Important To Consider Effects Of Individuals' Risk Perceptions In Understanding The Adoption And Use Of It. This Paper Presents An Exploratory Study Of The Role Of Users' *Perceived Privacy Risk* As Measured By Its Components *Risk Harm* And *Risk Likelihood* In Forming Behavioral Intentions Toward Continued Use Of It. In The Following Sections We Briefly Review The It Acceptance Literature And Then Define The Elements Of Risk Relating To Privacy Of Individuals And Organizations.

BACKGROUND

We frame this paper as an extension of the Technology Acceptance Model (TAM) (Davis, Bagozzi, & Warshaw 1989). TAM is a derivation of the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) that is customized for prediction of IT adoption and use. TRA and TAM represent a rational decision-making approach to the prediction of behaviors in which individual beliefs are mediated by attitude and behavioral intentions leading to subsequent use or non-use of technologies. For example, TAM posits that IT use will be predicted parsimoniously by perceived usefulness (PU) and perceived ease of use (PEOU) as mediated by behavioral intention (BI)[1]. Thus, all factors in TAM except IT use typically are measured as the

[1] Although attitude was included in the initial development of TAM, most subsequent studies do not include an attitude measure (Lee et al., 2003)

individual's perceptions of his or her beliefs and intentions. The ease of administering and measuring TAM through questionnaires and interviews has no doubt contributed to the popularity of this model among researchers.

In practice, TAM has proven to be both powerful and parsimonious. In a review of 101 TAM studies conducted across a wide range of IT types and usage contexts, Lee, Kozar, and Larsen (2003) report overwhelming support for the central relationships in TAM. Among the studies which assessed each specific relationship, 88% find PU influences BI, 71% find PEOU influences BI, 84% find PEOU influences PU, and 87% find BI influences IT use. In addition, Lee et al. describe 25 external factors that have been studied as contributors to TAM, ranging from measures of voluntariness of use to users' prior experiences with the technology. However, none of the external factors they describe addresses privacy risks of computer use[2].

Risk Factors

A number of researchers have studied monetary risks in online computing associated with e-commerce. Hoffman, Novak & Peralta (1999) find that when users perceived the online environment to be risky, they are less likely to purchase online. Labuschagne and Eloff write, "The major reason most people are still skeptical about electronic commerce is the perceived security risks associated with electronic transaction over the internet" (2000, pg 154).

In the present study we focus on privacy risk, or the risks involved in privacy of personal or organizational information. The specialized study of privacy risks in online computing is now becoming important because of the increasing presence of online activities that are intended to breach privacy of individuals and organizations, such as phishing and spyware. According to Drennan, Mort and Previte (2006), perception of risk is fundamental to the understanding of consumer concerns about privacy online and the relationship among the factors of privacy, risk and intentions. When people perceive risks they change their behaviors accordingly, often by performing a risk benefit calculation that assists them in deciding whether they should or should not disclose private information (Milne and Culnan, 2004).

One of the most evident types of privacy risk is that of identity theft, in which identification documents or identifying numbers are stolen. Victims of identity theft often spend years attempting to resolve the problems created by identity theft. Problems such as bounced checks, load denials, credit card application rejections and debt collection harassment can all be results of identity theft. For the 23-month period from its establishment in November 1999 through September 2001, the FTC Identity Theft Data Clearinghouse received 94,100 complaints from victim (http://www.consumer.gov/idtheft/). During that same time period, the FTC Clearinghouse data indicated that 2,633 victims reported monetary losses or out-of-pocket expenses as a result of identity theft. Of these 263 alleged losses above $10,000.00 and an additional 207 alleged losses above $5,000.

In more recent years identify theft has been accompanied by additional privacy threats such as phishing and spyware. The Phishing Trends Report, a repository for phishing attack information, reported that there were 15, 244 unique phishing incidents and 7197 unique phishing sites identified in December 2005 (http://www.antiphishing.org).

Numerous public reports continue to raise awareness of individual privacy risks. Some examples that have been reported include the following.

- Late in 2005, Ford Motor Company began notifying some 70,000 current and former white-collar workers that their sensitive personal and financial data had been stolen. The confidential information, which included employees' names, addresses and Social Security numbers, was contained on a stolen computer.
- Sam's Club, a division of Wal-Mart Stores Inc., continues to investigate a privacy breach that exposed credit card data belonging to a number of customers who bought gas at the wholesaler's stations in late September and early October 2005.
- One of the single most compelling data thefts of the year occurred at BJ's Wholesale Club, Inc. with the loss of thousands of customers' credit card information. The loss of this personal information led the Federal Trade Commission to bring charges against BJ's Wholesale Club, Inc.
- Organizations also are victimized by privacy breaches, with substantial resulting costs. Meyer (2002) finds the cost to combat such breaches is approximately $20,000 per hour during the first 72 hours of response.

Loss of privacy exposes both individuals and organizations to monetary costs, such as unauthorized bank account withdrawals, and nonmonetary costs, such as public exposure of personal affairs. If privacy risks of online computing come

[2] Computer anxiety measures certain aspects of risk, but these focus on apprehensions that the individual will be unsuccessful or inadequate in using the computer rather than concerns for privacy.

to be viewed as costly, then we anticipate this perception will obstruct continued use of online IT and will deny individuals and organizations many of the benefits that online IT currently delivers. This problem is compounded by evolving online technology, such as mobile commerce, which can be expected to introduce new privacy risks (Gosh and Swaminatha, 2001). The current increasing level of privacy risks and potential for new privacy risks in online computing suggest it is essential to begin research that explains and predicts how privacy risks will influence adoption and use of online IT.

Research Model and Hypotheses

Risk is calculated as the probability of an event occurring multiplied by the loss or amount of harm that could be done if that loss is realized (Straub and Welke, 1998). Our conceptualization of privacy risk follows the suggestion of Kim and Leem (2005) that risk involves two elements. These are the probability of an event occurring, which we denote as *perceived privacy risk likelihood,* and a loss amount, which we denote as *perceived privacy risk harm*[3]. Risk likelihood is the perception of probability that a privacy breach will occur. Risk harm is the perception of the level of damage that would occur in event of a privacy breach.

Our research model augments TAM with risk likelihood and risk harm (see Figure 1). Based on predominating findings in the TAM literature, we anticipate PEOU will have a positive effect on both PU and BI toward IT use, and we anticipate PU will have a positive effect on BI. We do not assess IT use in the present study.

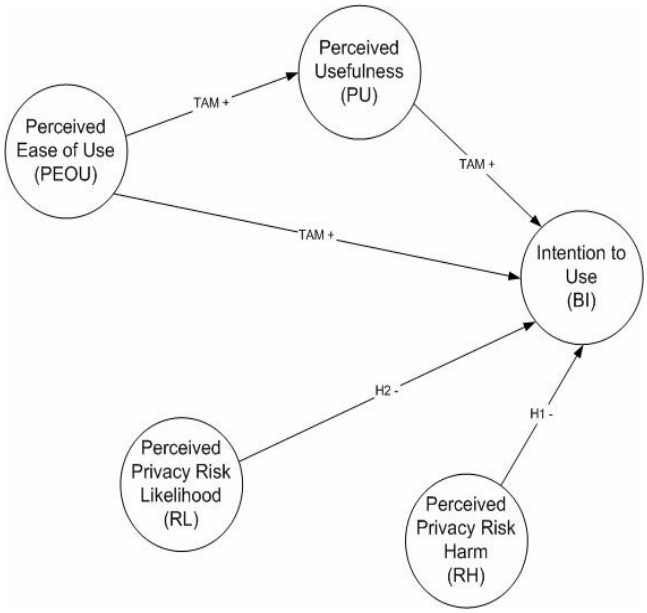

Figure 1: Privacy Risk Research Model

We propose that perception of privacy risk will influence decisions toward use of IT. We anticipate BI toward IT use will diminish where privacy risk is perceived to be high and increase where it is perceived to be low. In the present study, we operationalize privacy risk through its two elemental components, risk harm (RH) and risk likelihood. We hypothesize that both factors will negatively influence BI.

H1: Increasing risk harm will reduce BI toward IT use.

H2: Increasing risk likelihood will reduce BI toward IT use.

RESEARCH METHOD

The research methodology was conducted using an online survey instrument that assesses the perceptions and usage intentions of students toward their university's student registration and schedule management system. Students use the system for many interactions with their university, such as registering, adding and dropping classes, checking course grades, changing contact information, making advising appointments, and the monitoring of financial aid applications.

[3] For brevity we refer to these terms as risk likelihood (RL) and risk harm (RH) throughout the remainder of the paper.

Survey Instrument

The online survey stored responses in a database and was designed to prevent missing data by redisplaying any question for which a response was missing. Participants responded to scale items using a seven-point Likert scale with endpoints labeled "Strongly Disagree" / "Very Little" (Value =1) and "Strongly Agree" / "Very Little" (Value = 7) as dictated by the form in which the item was stated.

Measurement Items

Items measuring TAM constructs were drawn from Davis (1989). Items measuring risk harm and risk likelihood was developed as part of the present study using techniques prescribed by Gable and Wolf (1993). Five items were created to represent the essential content of each construct. For risk likelihood, the items assess the perception that a privacy breach is likely. For risk harm, the items assess the perception of the degree of damage that would result from a privacy breach. These items were then subjected to scale validation.

Scale Validation

We applied factor analysis methods to prune scale items, as recommended by Gable and Wolf (1993), and to confirm convergent and discriminate validity of the resulting scales. All items loaded cleanly on a single factor representing the intended construct (see Table 1). As a further confirmation of the reliability of the scales we also examined the Cronbach's Alpha and present the results in Column 1 of Table 1 It is recommended that the acceptable reliability for the Cronbach's Coefficient Alpha is .70 or greater (Peterson, 1994). All of the alpha values for our scales are greater than .80.

Factor / Alpha	Items	Description	Mean	Std. Dev.	Factor Loadings*				
					1	2	3	4	5
PU	PU1	Using this software improves the quality of my work.	4.78	1.43	**.880**	.206	-.005	.145	.012
α = .92	PU2	Using this software enhances effectiveness in my work.	4.85	1.42	**.852**	.203	.000	.229	-.045
	PU3	Using this software improves my work.	4.76	1.41	**.850**	.221	.027	.181	.034
PEOU	PEOU1	Learning to use this software was easy for me.	5.69	1.48	.161	**.864**	-.080	.075	-.031
α = .95	PEOU2	This software is easy to use.	5.77	1.41	.179	**.945**	-.053	.102	-.033
	PEOU3	My interaction with this software is clear	5.48	1.42	.283	**.747**	-.063	.188	.022
BI	BI1	I intend to continue using this software.	5.76	1.25	.154	.169	-.209	**.771**	-.105
α = .85	BI2	I intend to increase my use of this software	4.89	1.42	.273	.014	-.042	**.594**	.019
	BI3	I predict I would use this software.	5.54	1.31	.093	.164	-.141	**.818**	-.096
RL	RL1	How likely is it that the organization that manages this software would use your private personal information in a way that you would not approve of?	3.00	1.61	.001	-.085	**.813**	-.117	-.023
α = .81	RL2	How likely is it that this organization would abuse some of your personal information?	2.85	1.54	.002	-.082	**.930**	-.127	-.009
	RL3	How likely is it that someone will break into this software and steal your personal information?	3.21	1.56	.008	-.008	**.677**	-.089	-.108
RH	RH1	How much harm could be done to you if someone broke into this software? *reversed*	2.85	1.76	-.009	-.020	-.084	-.044	**.736**
α = .84	RH2	How much harm could be done to you if the organization that manages this software abused your information? *reversed*	2.77	1.63	.017	-.010	-.043	-.088	**.908**

Table 1: Rotated Factor Matrix

Conducted using unconstrained maximum likelihood extraction and Varimax rotation.

Subjects

Undergraduate business students at two major U.S. universities participated in the research. A total of 642 participants completed the entire questionnaire.

RESULTS

Descriptive Statistics

As seen in Table 1, mean response to items measuring PU, PEOU, and BI tend toward agreement, ranging in value from 4.76-5.77. Responses to risk likelihood and risk harm items have low means, ranging from 2.77-3.21, indicating that respondents generally believe the risk to be low. Their assessment may relate to the institutional nature of the IT or to the types of registration and schedule management tasks this IT is used for. However, the standard deviation of responses to privacy questions is higher than responses to other questions, indicating that there is a relatively high degree of uncertainty in the assessment of privacy risk by respondents.

SEM Analysis

In order to test the research model, we conducted structural equation modeling (SEM) analysis using AMOS 4.0 software (Arbuckle & Wothke, 1999). Fit of the model with the data was examined using prominent fit indices. Fit of the model us excellent on all measures (see Table 2). The values of GFI, NFI, RFI, IFI, and CFI are well above the .90 level recommended by Kelloway (1998). The value of RMSEA is well below the .10 level recommended by Kelloway (1998).

Fit Measure	Abbreviation	Fit Statistics
Chi-square	χ^2	198.7
Degrees of freedom	df	72
Discrepancy/df	χ^2/df	2.76
Goodness of fit index	GFI	0.957
Normed fit index	NFI	0.964
Relative fit index	RFI	0.955
Incremental fit index	IFI	0.977
Comparative fit index	CFI	0.977
Root mean square error of approximation	RMSEA	0.052

Table 2: Fit Statistics

Results of SEM analysis are shown in Figure 2. All paths in the model are significant, with direct and indirect relationships explaining 30 percent of the variance in BI. Covariance was tested between risk harm and risk likelihood, however, this relationship was not found to be significant was not included in the final model (path coeff. = .09, p = .051).

Model Interpretation

Hypothesis 1 states that increasing risk harm will reduce BI toward IT use. The hypothesis was supported (path coeff. = -.18, $p < .0001$). The influence of risk harm on BI is in the same numeric range as the effect of PEOU. Hypothesis 2 states that increasing risk likelihood will reduce BI toward IT use. This hypothesis also was supported (path coeff. = -.31, $p < .0001$). The influence of risk harm on BI is in the same numeric range as the effect of PU.

Although we did not hypothesize effects relating to TAM components in the research model, all relationships predicted by TAM were found. PEOU contributes positively to PU (path coeff. = .44, $p < .0001$) and BI (path coeff. = .14, p = .002). PU contributes positively to BI (path coeff. = .34, $p < .0001$). In order to test whether risk harm and risk likelihood add to predictiveness of TAM, we tested the research model without these factors. This model explains 19% of variance in BI, significantly less than the full research model ($F_{1, 619}$, $p < .0001$). We further tested whether risk harm or risk likelihood are mediated by TAM PEOU or PU belief factors by adding relationships between the two risk factors and PEOU and PU. None of these relationships was found to be significant.

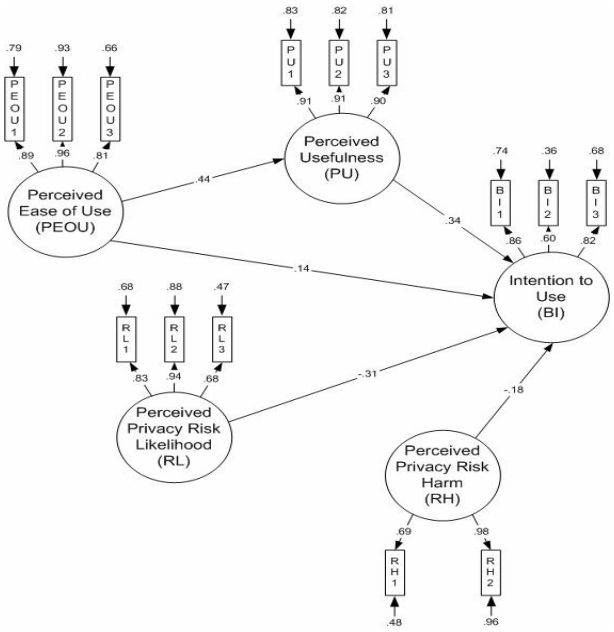

Figure 2: SEM Analysis of Research Model

Finally, we ran the research model separately on each of the university sample populations in order to ascertain how generalizable the model is between different IT implementations. Each university system offers students similar functionality for registering, adding and dropping classes, checking course grades, changing contact information, monitoring financial aid applications, and making advising appointments. However, user interface characteristics and instructions for use vary substantially between systems. Table 3 presents model path coefficients for each group and tests for significant differences between relationships. We find no significant differences between universities on any relationship except PEOU → PU, which does not directly influence BI. These findings suggest the research model is generalizable among different implementations of student registration and schedule management software.

Relationship	University 1 - Path Coeff. (n = 331)	University 2 - Path Coeff (n = 311)	Significance
PEOU → BI	.16	.11	$z = 0.64$, $p > .05$
PEOU → PU	.34	.50	$z = 2.46$, $p = .014$
PU → BI	.29	.39	$z = 1.43$, $p > .05$
Risk likelihood → BI	-.33	-.27	$z = -1.04$, $p > .05$
Risk harm → BI	-.21	-.13	$z = -0.83$, $p > .05$

Table 3: Model Comparison Between University Systems

DISCUSSION

We have argued previously that privacy risk is a key contributor to IT acceptance. In our extension of TAM, we find risk harm and risk likelihood as important as TAM's PEOU and PU factors in predicting BI. Because privacy risk factors have not previously been associated with IT acceptance (Lee et al., 2003) these findings make a valuable contribution to the IS literature.

The fact that these constructs have not been previously addressed in the TAM literature is likely due to the changing nature of technology and the increasing privacy risks that are associated with online computing. Privacy risks were less common in the offline, stand-alone systems and organizational networks that characterized IT before the widespread adoption of the Internet. But along with numerous benefits, the Internet has provided a ready mechanism for privacy breaches relating to identity theft,

phishing, and spyware. Our findings indicate that perceptions of privacy risk have emerged as important new predictors of IT acceptance in online computing environments, and this has implications both for research and practice.

Implications for Research

The primary implication of these findings for IS researchers is to question the assumption that current online computing is fundamentally similar to traditional computing, an assumption that underpins the application of TAM to predict individuals' acceptance and use of online IT. As pointed out by Lee et al. (2003), TAM is a mature theoretical model that has been tested across a wide range of IT. However, most of these tests used offline IT or were conducted before privacy risks became commonplace in online computing. Our finding that privacy risks directly influence BI without mediation by PEOU or PU presents a challenge to TAM. PEOU and PU are considered to be "fundamental determinants of user acceptance" of IT (Davis, 1989, p. 319). Yet effects of privacy risk factors in the present study are approximately as strong as the combined effects of PEOU and PU in predicting BI. Although TAM has been extended in many ways (Lee et al., 2003), we find no prior research has been directed toward privacy risks, including recent integrated approaches to IT acceptance, such as the unified theory of acceptance and use of technology (UTAUT) (Venkatesh, et al., 2003).

In order for online computing to continue to deliver benefits to users, it is necessary that users decide to accept and use this IT. Our findings suggest this decision is guided not only by the usefulness and ease of use that individuals perceive, but also by the privacy risk that is associated with IT use. This suggests future research should be directed toward finding ways to mitigate privacy risk. It is obvious that better security methods can help but it also will be important to understand how to manage perception of risk, especially when perceptions are overblown in relation to the inherent harm and likelihood associated with online computing.

In addition, further research should be conducted to identify characteristics of online computing that may also play a role beyond PEOU and PU in predicting acceptance of online IT. Several recent studies have presented findings that improve on TAM in online computing environments. For example, both frequency of prior IT use (Kim & Malhotra, 2005) and regularity of prior IT use (Wilson, Mao, & Lankton, 2005) have been identified as strong contributors to BI and continued IT use in online computing. More research should be conducted to quantify differences between traditional computing and online computing.

Implications for Practice

As discussed previously, it will be important for researchers to identify new ways of mitigating privacy risk. However, one practical method for organizations to reduce perceptions of privacy risk is to build a feeling of trust among users to assure them that the likelihood of risk is controlled and that the organization will minimize any harm that may arise. According to Milne and Boza (1998, pg. 267.) "Trust can be enhanced by building a reputation for fairness, by communication information sharing policies up front and stressing the relational benefits, and by constantly informing the consumers of the organization's activities to serve them better." We propose it is important for organizations to ensure that they can safely and securely manage IT users' private information, for example, by promising fast counter measures and "no harm" guarantees in the event of a breach.

Limitations

The present study addresses an online IT that subjects perceive to be a relatively secure and safe system. This is not surprising, given its university affiliation. In addition, while this system involves the exchange of information, there is no a online exchange of money. Thus, we anticipate our findings may *underestimate* the degree to which privacy risk plays a role in IT acceptance for online IT that are perceived to have greater privacy risks, such as financial fraud or transaction involving bank accounts and credit cards. Future research should address computing in "riskier" domains.

Another limitation in the present study is that use of the IT is quasi-voluntary. Alternative means exist to accomplish all activities that the IT supports; however, these typically require additional effort on the part of the student. Thus, results may be different in completely voluntary contexts, such as e-commerce IT where customers can choose among many different companies with which to do business. Potentially, privacy risk may be more important in voluntary contexts than in the present study, however, future research will be necessary to confirm this speculation.

Conclusion

Our rationale in conducting this research was to address the increase in privacy risk that we saw occurring in online computing, particularly as it affects individuals' perceptions and decisions toward use. We find that perceptions of privacy risk have become surprisingly important determinants of intention toward IT use, and this finding is troubling for the future of online computing. It is important for this reason to redouble efforts to reduce "frontier-style" online lawlessness. However,

we propose it is equally important to find ways to avoid over-dramatizing privacy risk and better matching perceptions with reality regarding risk.

REFERENCES

1. Ajzen, I., & Fishbein, M. (1980) Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.
2. Arbuckle, J., & Wothke, W. (1999) AMOS 4.0 user's guide. Chicago, IL: Smallwaters Corporation.
3. Bollen, K. A. (1989) Structural equation modeling with latent variables. New York: John Wiley & Sons Inc.
4. Conca, C. Medlin, D. & Dave, D. (2005) Technology-based security threats: taxonomy of sources, targets and a process model of alleviation", *International Journal Information Technology Management*, 4 (2) 166-177.
5. Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-329.
6. Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989) User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982-1002.
7. Drennan, J., Mort, G. S., and Previte, J. (2006) "Privacy, Risk Perception, and Expert Online Behavior: an exploratory study of household end users", *Journal of Organizational and End User Computing*: (18)1, 1-22.
8. Federal Trade Commission Identity Theft Clearing House, Retrieved from http://www.consumer.gov/idtheft/http://www.consumer.gov/idtheft/ on January 23, 2006.
9. Fishbein, M., & Ajzen, I. (1975) Belief, attitude, intention, and behavior. Reading, MA: Addison-Wesley.
10. Gable, R. K., & Wolf, M. B. (1993) Instrument development in the affective domain (second edition). Boston, MA: Kluwer Academic Publishing.
11. Gosh, A. K. and Swaminatha, T. (2001) "Software Security and Privacy Risks in Mobile E-Commerce: Examining the risks in wireless computing that will likely influence the emerging m-commerce market", *Communication of the ACM*, (44)2, 51-57.
12. Hoffman, D.L., Novak, T.P., & Peralta, M. (2004) "Building consumer trust online" Association for Computing Machinery. *Communications of the ACM*. (42)4, 80-86.
13. IBM, "IBM Survey: Consumers Think Cybercrime Now Three Times More Likely Than Physical Crime: Changing Nature of Crime Leads to Significant Behavior-Changes", Retrieved from http://www 03.ibm.com/press/us/en/pressrelease/19154.wss on January 27, 2006.
14. Kelloway, E. K. (1998) Using LISREL for structural equation modeling: A researcher's guide. Thousand Oaks, CA: Sage Publications.
15. Kim, S. and Leem, C. S. (2005) "Security of the internet-based instant messenger: Risk and safeguards", *Internet Research*, (15)1, 68-98.
16. Kim, S. S., & Malhotra, N. K. (2005a) A longitudinal model of continued IS use: An integrative view of four mechanisms underlying postadoption phenomena. *Management Science, 51*(5), 741-755.
17. Labuschagne, L. and Eloff, J. H. P. (2000) "Electronic Commerce: the information-security challenge", *Information Management & Computer Security*, (8)3, 54-159.
18. Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003) "The technology acceptance model: Past, present, and future", *Communications of AIS, 12*(50), 752-780.
19. Miller, R. (2006) Retrieved from http://news.netcraft.com/archives/security.htm on February 2, 2006.
20. Milne, G. R. and Boza, M.E. (1998) "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices", *Marketing Science Institute Working Paper Report*, 98-117.
21. Milne, G. R. and Culnan, M. J. (2004) "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices", *Journal of Interactive Marketing*, (18)3, 15-29.
22. Peterson, Robert A. (1994) "A meta analysis of Cronbach's coefficient alpha", *Journal of Consumer Research*, 21(2), 381-391.
23. Straub, D. W. and Welke, R. J. (1998) "Coping with systems risk: Security planning models for management decision making" *MIS Quarterly*, (22)4, 441-469.
24. Venkatesh, V. & Davis, F.D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science*, 46, 186-204.
25. Venkatesh, V. (2000) "Determinants of Perceived Ease of Use: Integrating Perceived Behavioral Control, Computer Anxiety and Enjoyment into the Technology Acceptance Model," *Information Systems Research* (11) 342-365.
26. Venkatesh, V., Morris, M. G., Davis, F. D., & Davis, G. B. (2003) User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27, 425-478.
27. Wilson, E. V., Mao, E., & Lankton, N. K. (2005) Predicting continuing acceptance of IT in conditions of sporadic use. In *Proceedings of the 2005 Americas Conference on Information Systems* (AMCIS), Omaha, NE.