2008

An Empirical Investigation on Customer's Privacy Perceptions, Trust and Security Awareness in E-commerce Environment

Anil Gurung
Marshall University, gurung@marshall.edu

Xin Luo

M. K. Raja

Recommended Citation
Gurung, A., Luo, X., & Raja, M. K. (2008). An empirical investigation on customer's privacy perceptions, trust and security awareness in E-commerce environment. Journal of Information Privacy and Security, 4(1), 42-60.

An Empirical Investigation on Customer's Privacy Perceptions, Trust and Security Awareness in E-commerce Environment

Anil Gurung, Neumann College, USA, agurung@acm.org
Xin Luo, the University of New Mexico, USA, luo@mgt.unm.edu
M.K Raja, the University of Texas at Arlington, raja@uta.edu

ABSTRACT

Privacy concerns of the users have been listed as one of the hindrances in the growth of e-commerce. Understanding the consequences of privacy and its relationship with risk perceptions may help in finding solutions to this problem. Internet users may use different strategies to protect their privacy so that they can become confident in taking part in e-commerce. In this study, we investigate how users can lower their risk perceptions in the context of e-commerce. The relationships among privacy, risk, trust and internet security measures are empirically investigated to predict the behavioral intention to take part in e-commerce. Theoretical contributions and implications are discussed.

KEY WORDS

Internet security awareness, risk beliefs, trust beliefs, and privacy concerns

INTRODUCTION

Digitally enabled commercial transactions between and among organizations and individuals, also known as e-commerce, involve the exchange of value across organizational or individual

boundaries in return for products and/or services (Laudon & Laudon, 2006). In order to survive in the highly competitive global economy, businesses must leverage technologies such as data warehousing and data mining to collect customer information, analyze their characteristics and behaviors, build relationships with existing customers, and draw potential ones. As such, gathering information about customers is a necessary task for managers to gain a better understanding of consumer preferences. Despite its exponential growth, e-commerce is faced with the predicament of an increasing number of users and their corresponding apprehension. On one hand, e-commerce has steadily grown since the dot-com bubble burst in 2001; on the other hand, users are hesitant to proactively take part in e-commerce transactions where they are required to divulge their private information such as date of birth, social security number, home telephone number, etc. These privacy concerns are further exacerbated by the inherent flaws of the Internet, originally designed for easy access and information sharing. Personal information may galvanize as well as hamper the further development of e-commerce, which as of today, is still in its infancy. Protecting users' privacy has been considered an important factor for the success of e-commerce, and is an inevitably challenging task for managers to balance customers' privacy and information collection for maximum online sales and profits.

Recent IS research has found that consumers are very concerned about the use, treatment, and potential transfer of their private information (Flavian & Guinaliu, 2006; Liu, Marchewka, Lu, & Yu, 2004; Malhotra, Kim, & Agarwal, 2004; H. Smith, Milburg, & Burke, 1996; Stewart & Segars, 2002). Past literature shows that there has been limited research in the area of privacy regarding the actions taken by users to protect their privacy. Because of the paucity of research in the area of privacy protection tools and privacy, their relationship has remained a rather unexplored charter. It can be argued that greater privacy concerns can lead to greater use of

personal security tools in order to lower potential risks. Awareness of internet security measures does not necessarily mean their use *per se*. Users may be aware of such security measures while their use will depend upon skill and privacy concern levels. Use of security measures may help the users lower their risk perceptions. The purpose of this study is to investigate how internet security awareness can impact risk beliefs and intention to engage in e-commerce. Specifically, this research attempts to investigate the following research questions:

RQl : How does the awareness of internet security measures impact the risk perception of e-commerce?

RQ2: Does awareness of internet security measures, perceived risk and trust influence consumer intentions to engage in e-commerce?

Privacy regulations may vary across countries. The European Union directive on Data Protection of 1995 mandates that all European nations pass privacy laws to protect citizens' privacy. In many European countries, personal information cannot be collected without consumers' consent and they also have the right to review the data. The context, for the purpose of this study, will be the United States and the data collection will be done entirely in the U.S.

LITERATURE REVIEW

Privacy Concerns and Strategies for Privacy Protection

Not a new concept, privacy has been defined as the right of an individual to be left alone and able to control the release of his or her personal information (Warren & Brandeis, 1890). It also refers to an individual's ability to control the terms by which his or her personal

information is acquired and used (Westin, 1967). Both widely acknowledged definitions point out the magnitude of an individual's right to control the way their personal information is collected and released. Additionally, information privacy concerns refer to an individual's subjective views of fairness within the context of information privacy (Campbell, 1997). In the arena of ecommerce, consumers' privacy concerns often surface when new information technologies with increased complexity and enhanced capabilities for collection, storage, use, and communication of personal information come into play (Liu et al., 2004). Knowing about information collection and usage beyond original transaction are the main influences on the degree to which users feel privacy concerns (Sheehan & Hoy, 2000). Furthermore, privacy concerns or unwillingness to disclose personal information are seen as a major threat to e-commerce and the digital economy (Culnan, 2000; Malhotra et al., 2004).

Privacy research has dealt with different issues such as technology, consumer, organizational, national, and privacy impacts on the practice of research (Chan et al., 2005). With regard to technology issues, it is important to find out how new technological advances influence privacy concerns, what the impacts of privacy protection strategies are on privacy concerns, and what the attributes of a technology that will create new privacy issues are. Privacy protection strategies refer to the use of tools and methods to maintain privacy. This may include using personal security measures such as anti-spyware tools, firewalls, disabling cookies, increasing security levels within browsers, and using anonymizers, etc. Using such privacy protection strategies has been suggested to alleviate user privacy concerns.

Marketing literature on consumer privacy suggests that there is a lack of awareness of privacy protections which may increase the risk perceptions of the users (Patterson, O'Malley, & Evans, 1997). Furthermore, users who are knowledgeable of privacy practices and options for

safeguarding their own information may experience more perceived control and thereby feel less privacy concerns (Foxman & Kilcoyne, 1993; Nowak & Phelps, 1997; Phelps, Nowak, & Ferrell, 2000). Sheehan and Hoy (1999) reported that, as privacy concerns rise, users are likely to provide incomplete information to websites, notify Internet Service Providers about unsolicited mail, and request removals from lists. However, there has been scant research in IS literature studying users' strategies to protect the privacy of their information.

Privacy protection actions include industry self-regulation and procedural fairness (M. Culnan, 2000; M. Culnan & Armstrong, 1999). However, it is doubtful that such measures to maintain privacy have been successful. Since the privacy concerns of users have not been well addressed, they have resorted to using their own strategies to protect their privacy. A recent survey of online shoppers reported the growing confidence of the online shoppers (Saunders, 2004). In that survey, online shoppers' confidence levels increased despite privacy concerns because the users may have become smarter about their online habits. Further, the survey found that the users are taking more measures to keep their online flnancial accounts secure. As Goodhue and Sträub (1991) indicated that awareness is an important factor in an individual's belief about information security, taking protective measures gives them a sense of perceived security. This perspective is supported by the study of Dinev and Hu (2007), who found that technology awareness leads to positive user behavioral intention for the use of protective technologies against information security threats. Therefore, we believe that, in the same vein, security awareness might be associated with consumer's behavioral intention for e-commerce transactions. The security awareness in this study is defined as having the knowledge and using the technology to protect oneself on the Internet. Such knowledge would encompass checking

and downloading system updates, using anti-virus and anti-spyware tools, using personal firewalls, and checking the security settings in the web browser etc.

Privacy Concerns and Trust

As an important factor to mitigate the privacy concerns of the users, trust has been established in research as an important determinant in consumer behavior. The need to trust online businesses seems magnified in the online environment where geographical proximity to the brick-and-mortar store does not exist, so a consumer cannot rely on physical cues such as neighborhood location, physical size, presence of customers, and interior décor of the store to help assess that store's trustworthiness. Hoffman et al. (1999) suggested that the primary reason many Internet users have yet to use e-commerce or provide personal information to a vendor is due to the fundamental lack of trust with online transactions which often times requires users to input credit card and other private information. Companies seek to gain consumers' trust by use of web seals, privacy policy, visual aesthetics, and navigation quality of their online stores, etc. Trust in companies increases the likelihood of users to take part in ecommerce transactions. This implies that the perceived risks of users arising from privacy concerns are relieved, to some extent, by developing trust. The privacy research has studied the impacts of risk and benefits of users in taking part in ecommerce. Consumers make their calculations of risk which can be attributed to some extent, their privacy concerns and the benefits of taking part in e-commerce and reach their decision whether to take part in the e-commerce transaction. Culnan and Bies (1999) proposed that users have a "privacy calculus" to weigh the potential risks and benefits of providing personal information in exchange for economic or social gains. Similarly, Dhillon et al. (2002) stated that users make "value focused" privacy-based assessments about the firms when they transact. Many researchers have studied consumer attitudes to examine the effects of

privacy concerns. Yet, there has been little empirical evidence of how privacy concerns and trust affect consumer behavior.

Risk and Trust Beliefs

Bauer (1960) introduced the concept of risk perception and defined it as "a *combination of uncertainty plus seriousness of outcome involved'*. Having been measured in terms of certainty and consequences (Cunningham, 1967), risk has been viewed as the uncertainty associated with the outcome of a decision (Sitkin & Pablo, 1992). When a consumer is uncertain that their buying goals will be achieved successfully, risk is perceived to be a factor. Jarvenpaa and Tractinsky (1999) provided empirical evidence that risk perceptions reduced online shoppers' behavioral intention to purchase books. Malhotra et al. (2004) contended that both trust belief and risk belief significantly drive one's intention to release personal information through the Internet. The categories of risks have been identified in the literature - product and transaction risks (Chang, Cheung, & Lai, 2005). Product risk refers to the uncertainty that the purchase will match the acceptance levels in buying goals. Perceived transaction risk is the uncertainty that may result during the process of transaction. Transaction risks include authentication, privacy, security, and non-repudiation of transaction. Authentication risk is the perception that the seller is not whom they claim to be. Privacy risk refers to the possibility of theft of private information or illegal disclosure (Pavlou, 2003). Security risk relates to the safety of the data transmitted over the internet (Chang et al., 2005). Non-repudiation means the rejection of the transaction by the seller (Chang et al., 2005).

Mayer et al. (1995) proposed a trust model with its antecedents and outcomes. They defined trust as the *"willingness of a party to be vulnerable to the actions of another party*

based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party." In IS research, trust refers to a belief that one can rely upon a promise made by another (Pavlou, 2003). Furthermore, trust beliefs include the online consumers' beliefs and expectations about trust-related characteristics of the online seller in the context of e-commerce (McKnight & Chervany, 2002). E-commerce consumers want online vendors to be willing and able to act in the consumers' best interest, to be honest in transactions (not divulging personal information to other vendors), and to be capable of delivering the ordered goods as promised.

Most IS studies support_ that trust plays a significant role in determining a customer's actions regarding a vendor. In the same vein, trust is a critical factor when a user assesses the believability of online information content or when selecting an exchange site from which to purchase a product. Empirical research has shown that trust increases customer intention to purchase a product from a company (Jarvenpaa, Tractinsky, & Vitale, 2000) as well as behavioral intention to return to that company (Doney & Cannon, 1997). Trust, as defined in this study, is the belief that companies will not break the trust of consumers when they engage in e-commerce.

RESEARCH MODEL AND HYPOTHESES DEVELOPMENT

We developed a model to study how users can use privacy protection strategies to alleviate their privacy concerns and are willing to take part in e-commerce. Theoretical frameworks of trust and risk (Jarvenpaa, Tractinsky, Saarinen, & Vitale, 1999; Mayer et al., 1995) and the Theory of Planned Behavior or TPB (Ajzen, 1991) are employed as

theoretical underpinnings for the proposed model. Figure I displays the proposed research model and eight hypotheses.

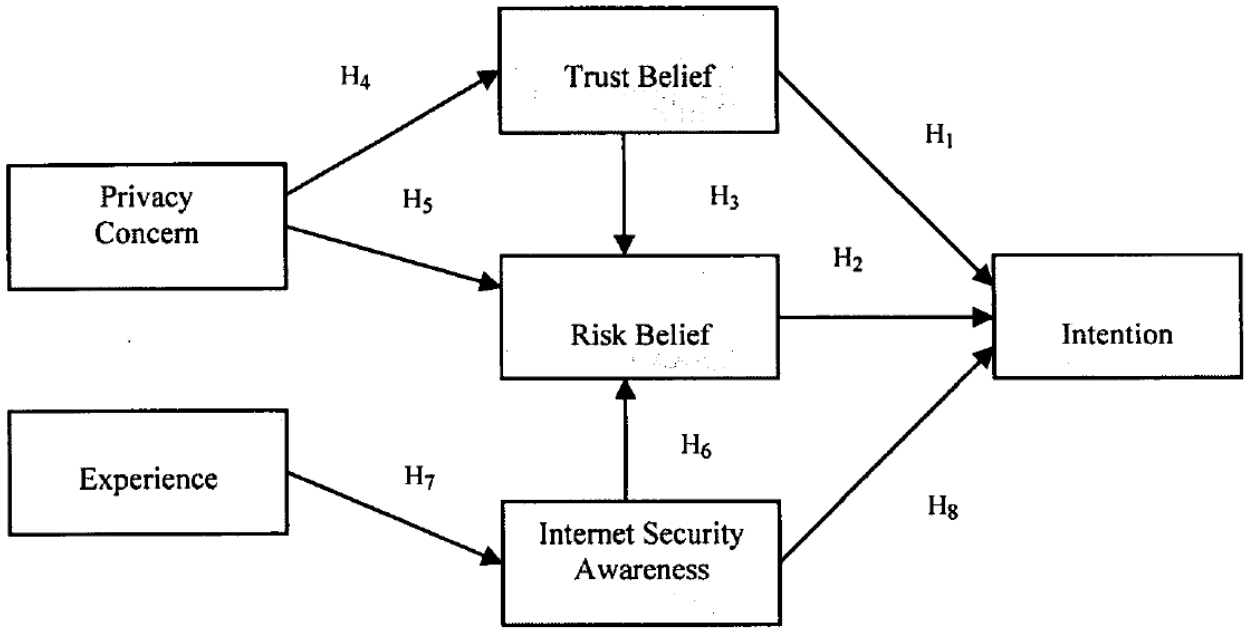

Figure 1: The Research Model

TPB suggests beliefs affect a person's attitudes which, in turn, influence behavioral intention thus predicting the actual behavior. According to TPB, three conceptually independent determinants of intention are attitude toward the behavior, subjective norm and perceived behavioral control. Attitude refers to the degree to which a person has a favorable or unfavorable appraisal of the behavior in question. Subjective norm refers to the perceived social pressure regarding the performance of the behavior. The degree of perceived behavioral control relates to the perceived ease of difficulty of performing the behavior. The relative importance of attitude, subjective norm, and perceived behavioral control in the prediction of intention depends on a specific context.

In an e-commerce environment, trust beliefs are formed by users based on the information available on companies. Trust in a website can generate a favorable attitude in a consumer and may also improve the attitude indirectly by lowering the risk perception of the consumer (Jarvenpaa et al., 1999). The impact of trust on intention to transact in e-commerce is based on the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980). TRA postulates that salient beliefs, such as expectations of an outcome, influence a person's intention to conduct a behavior. Past studies in ecommerce have shown that trusting beliefs in specific online companies are correlated with transaction intentions with those companies (Gefen, 2000; D. H. McKnight & Chervany, 2002; Pavlou, 2003). Sitkin and Pablo (1992) suggested that perceived risk may mediate the effect of trust on intention and behavior. Few studies have investigated the effect of trust on perceived risk. A significant negative effect between trust and perceived risk was found (Jarvenpaa et al., 1999; Jarvenpaa et al., 2000; Kimery & McCord, 2002; van der Heijden, 2003). Data collected from online auction marketplace supported that buyers' trust in sellers facilitated online transactions by reducing perceived risk (Pavlou & Gefen, 2004). Therefore, we hypothesize that:

H_1: Trust in online companies will have a positive relationship with the intention to purchase from the online companies.

H_2: A lower risk perception will have a positive association with the intention to purchase from the online companies.

As noted by Malhotra et al (2004), it has been established in the trust-risk literature that personal traits influence trust and risk beliefs (Mayer et al., 1995; D. McKnight,

Cummings, & Chervany, 1998). Consumer's concerns about privacy influence how the consumer will trust an online company or perceive risk in purchasing from the company. A negative relationship between privacy concerns and trust, a positive relationship between privacy concerns and risk, and a negative relationship between trust and risk have been studied (Malhotra et al., 2004). Some researchers have suggested that privacy protection may be an important antecedent to trust building, in essence, online vendors can build trust if they convince the consumer that online transaction will take place as expected by the consumer (Culnan & Armstrong, 1999). Liu et al. (2004) proposed that trustworthiness of a website may depend on beliefs of users that their privacy is maintained. Thus, the following hypotheses will be tested:

H_3: There is a negative association between risk perception and trust in online companies.

H_4: There is a negative association between privacy concerns and trust in online companies.

H_5: There is a positive association between privacy concerns and risk perception.

A study on consumer privacy by Dommeyer and Gross (2003) found that users had little knowledge of direct marketing practices and regulations. They reported that users were some-what aware of privacy protection strategies. According to Campbell et al. (2001), internet users who have a high level of awareness of security measures are likely to engage in more risky activities, such as online purchases, banking, and providing personal information over the internet Hu and Dinev (2005) found that the awareness of privacy protection tools such as anti-spyware software is the most significant determinant of user behavior in taking active measures

to protect against Spyware intrusion and clean spyware from infected systems. Internet users with concerns for privacy may participate in potentially risky activities only after having personal privacy safeguards such as encrypted transactions, anonymous browsing, or authentic-ation (i.e. digital certificates) (Campbell et al., 2001). Internet security awareness provides users with adequate confidence for participating in online transactions by alleviating their fears about their privacy concerns. This suggests that risk perception is somewhat reduced by the awareness and the use of protection strategies since the users may perceive the security. Users perceive better protection when they are aware of and use different protection strategies. Furthermore, the security awareness may possibly be related with internet experience. Past experience may generate knowledge and consequences that reinforce consumer's behavior and shape their beliefs, attitudes, and willingness to take part in e-commerce. Prior studies on technology adoption have found the relationship between experience and use of technology (Shim & Drake, 1990; Thompson, Higgins, & Howell, 1994). With the increased level of internet experience, it is likely that users will be more aware of protective measures. As they are more experienced with a system, they may get acquainted with its additional features. Therefore, we hypothesize that:

H_6: The awareness of internet security has negative association with risk perception of e-commerce transaction.

H7: The internet experience has positive association with security awareness.

Hg: The awareness of internet security will have positive relationship with the intention to transact in e-commerce.

METHODOLOGY

Sample

The relationships hypothesized in the research model are empirically tested by collecting data from a survey. The sample is business undergraduate students enrolled in a required course in the College of Business at a Midwestern university in the United States. Since it is a required course, the sample represents a cross-section of all the majors in the college. A total of 233 usable responses were collected based on the number of students present in the class. The sample is comprised of 51.3% male and 48.7% female respondents. 29.4% were between 17 and 20 years old; 44.5% were 21to 29 years old; 13.5% were 30 to 39; 9.2% were 40 to 49 and 3.4% were above 49 years. The average internet experience is 6.8 years.

Instrument Validation

As for descriptive statistics, 37% of the respondents were in their early twenties, 34% were in their late twenties and 9% were in their thirties. Out of a total of 233 respondents, 115 were male and 113 were female. Five respondents did not provide gender information. A description of means and standard deviations of the constructs is given in Table 1.

Table 1: Construct Means and Standard Deviations

N = 233	Privacy	Trust	Risk	Sec Aware	Intention	Experience
Mean	5.40	5.53	3.18	5.09	5.82	5.92
Std Deviation	1.24	0.95	1.27	1.44	1.40	1.40

The study used validated scales from the literature wherever possible. Few items are newly developed. All items were set in a seven-point scale ranging from Strongly Disagree (1) to Strongly Agree (7). Validated measures for privacy concerns were adapted from Smith et al.

(1996) and Pavlou et al. (2007). Individuals' privacy concern refers to their insecure feeling of their privacy regarding the information practices of the organizations. Trust refers to individual trust in online companies. The validated measures were adopted from Bhattacherjee (2002). Risk beliefs refer to the expectation of a potential loss when personal information is given to online companies. The measures were adapted from Jarvenpaa et al (2000). Security awareness refers to the degree to which individuals are aware of and use personal security methods and tools to protect their respective identities online. The security awareness construct is operationalized by use of security measures since awareness is a precursor to use. Items for security awareness were adapted from an online safety study conducted by America Online and the National Cyber Security Alliance. Experience relates to the internet experience of internet users. Intention refers to the behavioral intention to take part in e-commerce activities, i.e. making purchases, in this study. The list of measures is provided in Appendix A. In a confirmatory factor analysis, two items one each from security awareness and privacy concerns were dropped because of cross-loadings as shown in Table 3.

RESULTS

The research model was analyzed using partial least squares (PLS) which is a form of the structural equation modeling method. PLS has been favored by researchers working with complex models emphasizing causality prediction (Joreskog & Wold, 1982). It uses a component-based approach to estimation, thereby, placing a minimal demand on sample size, normality assumption and residual distributions (Chin, 1998; Lohmoller, 1989). In this study, PLS-Graph Version 3.0 was used to assess the psychometric properties of all measures and also to test the structural model.

Measurement Model

The psychometric properties of measures in PLS were assessed in terms of item loadings, internal consistency or reliability, and convergent and discriminant validity. The convergent validity of the constructs is assessed by examining the average variance extracted (AVE). Table 2 shows that the AVE for all the constructs is above 0.50, as prescribed by Chin (1998). The composite reliability, which is similar to Cronbach's alphas, demonstrates the internal consistency of each construct. As shown in Table 2, all the values are well above the 0.70 standard (Barclay, Thompson, & Higgins, 1995; Fornell & Larcker, 1981), the lowest being .897 for security awareness. Discriminant validity is confirmed if the construct shares more of its variance with its measures than with other constructs in the model (Barclay et al., 1995). In PLS, discriminant validity can be assessed by comparing AVE with square of the correlations among the latent variables (Chin, 1998). Table 2 shows that, for all the constructs, the square root of AVEs is greater than the values in the corresponding rows and columns, thus demonstrating acceptable discriminant validity. This indicates that all constructs share considerably more variance with their indicators than with other constructs. As shown in Table 3, all items load with their respective constructs.

Table 2: Correlations of Latent Variables

	Composite Reliability	Privacy	Trust	Risk	Int Sec Awa	Intention	Experience
Privacy	.903	**.652**					
Trust	.913	0.027	**.580**				
Risk	.916	0.338	-.437	**.731**			
Int Sec Awa	.897	0.140	0.310	-.024	**.686**		
Intention	.956	-.137	0.531	-.255	0.281	**.916**	
Experience	1	0.00	0.110	-.098	0.197	0.13	**1**
Square Root of AVE		**.81**	**.76**	**.85**	**.83**	**.96**	**1**

Note: Average Variance Extracted (AVE) is shown on diagonal

Table 3: Confirmatory Factor Analysis Results

	Trust	Int Sec Awa	Risk	Privacy	Experience	Intention
PRV1	.001	.101	.035	.860	-.061	.038
PRV2	-.055	.099	.038	.860	.007	-.016
PRV3	-.013	.053	-.026	.852	.044	-.052
PRV4*	.023	.367	.020	-.211	.008	-.088
PRV5	-.070	-.060	.005	.837	-.062	.133
TRU1	.724	.059	.007	-.050	.004	-.052
TRU2	.731	.177	.083	.039	.017	-.368
TRU3	.750	.181	.028	.129	-.017	-.403
TRU4	.753	.214	-.033	.015	.022	.001
TRU5	.763	.077	-.074	.020	.075	.264
TRU6	.709	.179	.012	.034	.093	.318
TRU7	.706	-.047	.007	-.007	.869	-.092
TRU8	.721	-.169	-.038	.004	-.025	-.059
RSB1	-.114	.115	.812	.024	.009	.219
RSB2	-.040	-.029	.848	-.016	-.004	.006
RSB3	.021	-.102	.963	.018	.004	.031
RSB4	.021	-.104	.963	.018	.005	.027
SAW1	.046	.783	.007	-.034	-.032	-.117
SAW2	.139	.828	-.105	.008	-.013	.098
SAW3	.123	.843	-.134	.089	.093	.056
SAW4	.120	.765	-.057	.213	-.080	.079
SAW5*	.077	.194	.175	.243	-.096	.524
INT1	.231	.244	.121	-.258	-.137	.722
INT2	.272	.288	.053	-.175	-.045	.788
EXP	.008	.016	-.001	.021	.885	.027

*Dropped items from final analysis

Structural Model

PLS was also used to test the structural model. Except for the measures of security awareness, all the measures were modeled as reflective measures. The security awareness measures were modeled as formative measures. The theoretical model and hypothesized relationships were estimated using 200 iterations of the boostrapping method (Chin, 1998). Path coefficients and explained variances for the research model are shown in Figure 2. Path coefficients in PLS are similar to standardized beta

weights in regression analysis. To examine the specific hypotheses, t-statistics for the standardized path coefficients were assessed and p-values based on a two-tail test with a significance level of .05 were calculated. The results are given in the Figure 2. A summary of results from hypothesis testing are tabulated in Table 4.

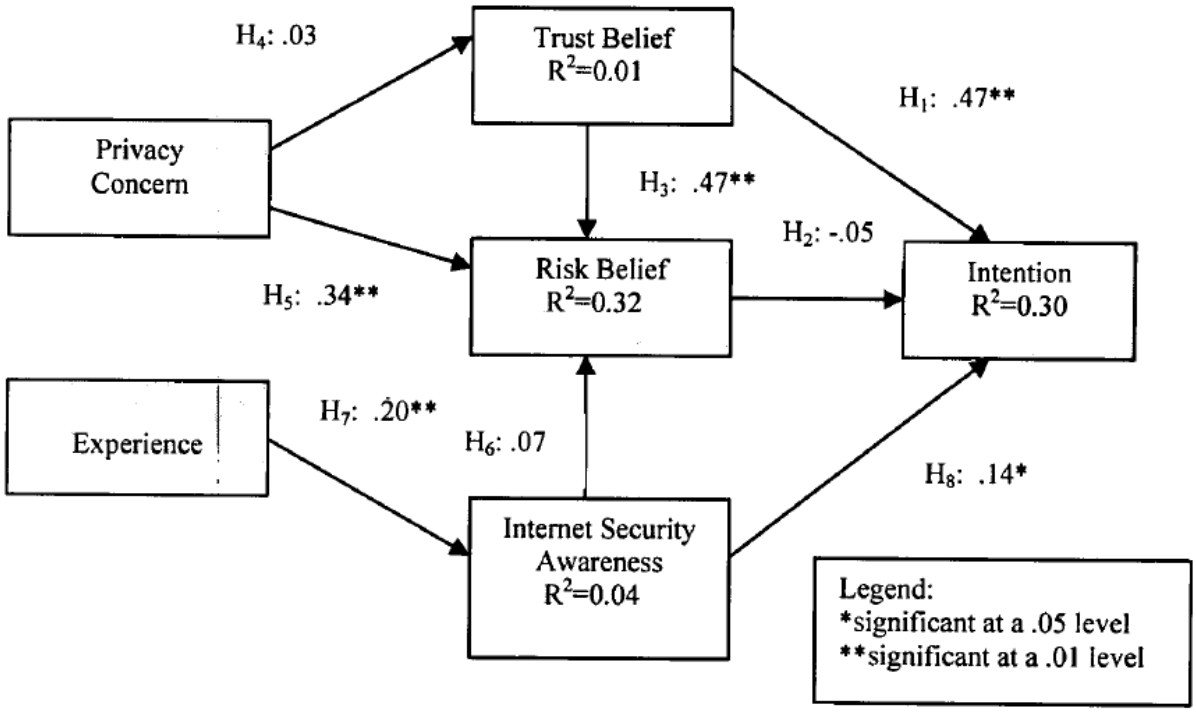

Figure 2: Path Model

Table 4: Summery of Hypothesis Tests

Hypothesis	Path Coefficient	P-value	Support
H1: TRU -> INT	.47	< .01	Yes
H2: RSK -> INT	-.05	n.s.	No
H3: TRU -> RSK	.47	< .01	Yes
H4: PRV -> TRU	.03	n.s.	No
H5: PRV -> TRU	.34	< .01	Yes
H6: AWA -> RSK	.07	n.s.	No
H7: EXP -> AWA	.20	< .01	Yes
H8: AWA -> INT	.14	< .05	Yes

DISCUSSION

The objective of this study is to understand how awareness of internet security measures affect the risk perception and what factors are important for intention to engage in e-commerce. First, we discussed the literature on privacy, trust, and risk beliefs in the context of e-commerce. Then, we defined and integrated the internet security awareness construct with the constructs of privacy concerns, trust and risk beliefs as predictors for intention to take part in e-commerce. The operationalization of internet security awareness construct has been carried with the belief that awareness of the internet security measures is necessary precondition to perform-ance of these security measures. The antecedents to purchase intention account for 30% of the variance. The explained variance for risk beliefs is 31.8%. These results provide a partial support for the theoretic model proposed in this study. The amount of variance in intention suggests that there may be other important variables that can strengthen the model.

Trust beliefs and internet security awareness are significant predictors of intention. There is no support for risk beliefs being the predictor of intention. Besides, internet security awareness also does not have a significant relationship with risk beliefs. As hypothesized, experience is significant with internet security awareness. Trust has been established as an important aspect of e-commerce adoption. It has often been noted in e-commerce trust literature that trust beliefs impact the intention to engage in e-commerce. However, none of these studies describe or include the factors consumers undertake influencing their intentions. This study contributes to the e-commerce literature by incorporating security awareness of consumers and variables associated with the behavioral intention to engage in e-commerce. Statistical results indicate that inclusion of security awareness as a predictor to behavioral intention is promising. This study

should be taken as a first step toward including the factors related to actions of consumers to help them take part in e-commerce.

The empirical findings provide interesting insights. The findings of this study provide support that security awareness can be an important predictor for behavioral intention to engage in e-commerce. Internet experience helps raise the security awareness of the consumers. More experience may lead to better awareness of various internet security measures. Security awareness, along with the trust beliefs, may become important factors predicting purchase intention. Privacy concerns have a significant relationship with risk beliefs. The results indicate that trust may lower the risk beliefs fueled by privacy concerns of consumers to a significant extent. However, the risk beliefs were not significant with intent to purchase contrary to previous studies. One explanation would be that awareness and use of internet security measures along with trust beliefs help to engender the willingness to partake in e-commerce.

LIMITATIONS AND IMPLICATIONS

As Dennis and Valacich (2001) indicated, all research is imperfect because different strategies carry comparative strengths and weaknesses, this study suffers from several method-logical and theoretical limitations. First, data was collected through university students who may be an accurate representation of the population. Studies with the consumer population would have enhanced the generalizability of the results. Future research is expected to step further into true consumer population to improve generalizability, which inevitably exists in survey-based empirical studies. Secondly, this study suffers from common method variance. The responses were self-reported. Some studies have shown that self-reported measures of IS usage are not actual enough to reflect the actual usage of the system (Sträub, Limayen, & Karahanna-Evaristo, 1995). Last, but not least, the explained variance of the intention reflects that many important

variables have been precluded from the model. Future research may overcome the parsimony by extending the research model and is expected to examine additional e-commerce-powered paradigms.

Perhaps this study is one of the first attempts to investigate the role of security awareness to predict behavioral intention of e-commerce purchases. Future research can be undertaken to explain the concept and role of security awareness in ecommerce adoption. Instead of being limited to measuring intention, future studies should measure actual behaviors.

CONCLUSION

This study contributes to the e-commerce literature by giving an empirical evidence of the proposed model that includes privacy, trust, risk perceptions and security awareness to predict intention to engage in e-commerce. This research shows promise that consumers can enhance their online experience by lowering risk perceptions with the awareness of internet security measures. In the absence of legislation to protect privacy, users may resort to personal measures to protect their identity while engaging in online transactions. Implications for practice would be to develop and promote trust in websites by protecting the privacy of users, raising consumer awareness of privacy protection strategies, and educating users in ways to protect their privacy.

REFERENCES

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50(2), 179-211

Ajzen, I., & Fisbbein, M. (1980). *Understanding attitudes and predicting social behavior.* Englewood Cliffs, NJ: Prentice-Hall.

Barclay, D., Thompson, R., & Higgins, C. (1995). The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. *Technology Studies: Special Issue on Research Methodology,* 2(2), 285-324.

Bauer, R. (1960). Consumer Behavior As Risk Taking. In D. Cox (Ed.), *Risk Taking and Information Handling in Consumer Behavior.* Cambridge, MA: Harvard University Press.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems,* 79(1), 211-241.

Campbell, A. J. (1997). Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy. *Journal of Direct Marketing 11(3), 44-51*.

Campbell, J., Sherman, R. C, Kraan, E., & Birchmeier, Z. (2001). *Internet privacy awareness and concerns among college students.* Paper presented at the American Psychological Society, Toronto, Canada.

Chan, Y., Culnan, M. J., Greenaway, K., Laden, G., Levin, T., & Smith, H. J. (2005). Information Privacy: Management, Marketplace, and Legal Challenges. *Communications of the Association for Information Systems 16*, 270-298.

Chang, M. K., Cheung, W., & Lai, V. S. (2005). Literature Derived Reference Models for the Adoption of Online Shopping. *Information & Management, 42(4),* 543-559.

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 295-336). London, UK: Lawrence Erlbaum Association.

Culnan, M. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing,* 79(1), 20-26.

Culnan, M., & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science,* 70(1), 104-115.

Culnan, M. J., & Bies, R. J. (1999). Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-First Century. In C. J. Bennett & R. Grant (Eds.), *Visions of Privacy: Policy Choices for the Digital Age* (pp. 149-167). Toronto, ON: University of Toronto Press.

Cunningham, S. M. (1967). The Major Dimensions of Perceived Risk. In D. Cox (Ed.), *Risk Taking and Information Handling in Consumer Behavior*. Cambridge, Mass.: Harvard University Press.

Dennis, A., & Valacich, J. (2001). Conducting Research in Information Systems. *Communications of the Association for Information Systems,* 7(5), 1-41.

Dhillon, G., Bardacino, J., & Hackney, R. (2002). *Value Focused Assessment of Individual Privacy Concerns for Internet Commerce.* Paper presented at the Proceedings of the Twenty Third International Conference on Information Systems, Barcelona, Spain.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in The Formation of User Behavioral Intention Toward Protective Information Technologies. *Journal of Association for Information Systems, 8(7), 386*-408.

Dommeyer, C. J., & Gross, B. L. (2003). What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, And Use Of Privacy Protection Strategies. *Journal of Interactive Marketing, 17(2),* 34-51.

Doney, P. M., & Cannon, J. P. (1997). An Examination of The Nature of Trust in Buyer-Seller Relationships. *Journal of Marketing, 61(2),* 35-51.

Flavian, C., & Guinaliu, M. (2006). Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site. *Industrial Management & Data Systems, 106(5),* 601-620. -

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models With Unobservable Variables and Measurement Error. *Journal of Marketing Research (JMR), 18(1*), 39-50.

Foxman, E. R., & Kilcoyne, P. (1993). Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing, 12,* 106-119.

Gefen, D. (2000). E-commerce: The Role of Familiarity And Trust. *Omega, 28(6),* 725-737.

Goodhue, D. L., & Straub, D. W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information & Management, 20(1),* 13-27.

Hoffman, D., Novak, T., & Peralta, M. (1999). Building Consumer Trust in Online Environments: The Case For Information Privacy. *Communications of the ACM, 42(4),* 80-85.

Hu, Q., & Dinev, T. (2005). Is Spyware an Internet Nuisance or Public Menace?

Communications of the ACM, 48(8), 61-66.

Jarvenpaa, S. L., Tractinsky, N., Saarinen, L., & Vitale, M. (1999). Consumer Trust in An Internet Store: A Cross-Cultural Validation. *Journal of Computer-Mediated Communication,* 5(2).

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer Trust in an Internet Store. *Information Technology and Management, 1*(l-2), 45-71.

Joreskog, K. G., & Wold, H. (1982). The ML and PLS Techniques for Modeling Latent Variables: Historical and Comparative Aspects. In K. G. Joreskog & H. Wold (Eds.), *Systems under Indirect Observation: Causality, Structure, Prediction* (pp. 263-270). New York: North Holland

Kimery, K. M., & McCord, M. (2002). Third-party Assurances: Mapping the Road to Trust in E-Retailing. *Journal of Information Technology Theory and Application,* 4(2), 63-81.

Laudon, K. C., & Laudon, J. (2006). *Essentials of Management Information Systems:* Prentice Hall.

Liu, C., Marchewka, J., Lu, J., & Yu, C. (2004). Beyond Concern: A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. *Information & Management, 42*(1), 127-142.

Lohmoller, J. B. (1989). *Latent Variable Path Modeling with Partial Least Squares.* New York: Springer-Verlag.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, The Scale, and a Causal Model. *Information Systems Research, 15(*4), 336-355.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review, 20(*3), 709-734.

McKnight, D., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *Academy of Management Review, 23*(3), 473-490.

McKnight, D. H., & Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce, 6*(2), 35-53.

Nowak, G. J., & Phelps, J. (1997). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters. *Journal of*

Direct Marketing, *11*(4), 94-108.

Patterson, M., O'Malley, L., & Evans, M. (1997). Database Marketing: Investigating Privacy Concerns. *Journal of Marketing Communications, 3,* 151-174.

Pavlou, P. A. (2003). Consumer Acceptance Of Electronic Commerce: Integrating Trust and Risk With The Technology Acceptance Model. *International Journal of Electronic Commerce,* 7(3), 69-103.

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research, 15(1),* 37-59.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105-136.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19(1),* 27-41.

Saunders, C. (2004). Consumers' Confidence Increasing in E-Commerce, Despite Threats. Retrieved November 2004 http://www.ecommerceguide.com/news/trends/article.php/3440101

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond To Privacy Concerns. *Journal of Advertising, 28*(3), 37-51.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

Shim, S., & Drake, M. F. (1990). Consumer Intention to Utilize Electronic Shopping. *Journal of Direct Marketing, 4*(3), 22-33.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the Determinants of Risk Behavior. *Academy of Management Review,* 17(1), 9-38.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167-196.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research, 13*(1), 36-49.

Straub, D., Limayen, M., & Karahanna-Evaristo, E. (1995). Measuring System Usage: Implications for IS Theory Testing. *Management Science, 41*(8), 1328-1342.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1994). Influence of Experience on

Personal Computer Utilization: Testing a Conceptual Model. *Journal of Management Information Systems, 11*(1), 167-187.

Van der Heijden, H., Verhagen, T., and Creemers, M. (2003). Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives. *European Journal of Information Systems, 12*(1), 41.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

Westin, A. F. (1967). *Privacy and Freedom.* New York, NY: Atheneum.

Appendix A

Construct	Items
Privacy Concerns	1. I am concerned that online companies are collecting too much information about me. 2. It usually bothers me when online companies ask me for personal information. 3. I have my doubts regarding how well my privacy is protected by online companies. 4. My personal information could be misused when transacting with online companies. 5. Overall, I am very concerned for my privacy.
Trust	1. This online company has the skills and expertise to perform transactions in an expected manner. 2. This online company has access to the information needed to handle transactions appropriately. 3. This online company is fair in its conduct of customer transactions. 4. This online company is fair in its customer service policies following a transaction. 5. This online company is open and receptive to customer needs. 6. This online company keeps its customers' best interests in mind during most transactions. 7. This online company makes good-faith efforts to address most customer concerns. 8. Overall, this online company is trustworthy.
Risk	1. There would be high potential for loss associated with giving information to this online company. 2. It would be risky to give information to this online company. 3. Providing this online company with information would involve many unexpected problems. 4. There would be too much uncertainty associated with providing information to this online company.

Appendix A – Continued

Internet Security Awareness	1. I regularly download security updates and "patches" for operating systems and other software. 2. I always use "firewalls" to protect my computer from internet intruders. 3. I always use anti-virus software and keep it up to date. 4. I always use anti-spyware software and keep it up to date. 5. I maintain the computer security regularly by checking the security settings on my web browser.
Experience	On average, how much time per week do you spend on the Web? (None; 0-30 min., 30-60 min., 1-2 hrs., 2-4 hrs., 4-8 hrs., 8+ hrs.)
Intention	1. What is the extent to which you will buy from this online company? 2. I predict that I would consider buying a product from this online company.

Anil Gurung is an Assistant Professor in the Division of Business and Information Management at Neumann College. He received his Ph.D. from the University of Texas at Arlington and MBA from Missouri State University. Current research interests are in the areas of information security and privacy, ecommerce, and cultural and social aspects of business computing. He has published in various journals such as *Journal of Global Information Technology Management* (JGITM), *International Journal of Information Systems and Change Management* (IJISCM), *Journal of Organizational and End User Computing* (JOEUC) and *International Journal of web- based Learning and Teaching Technologies* (IJWLTT). Prior to joining academia he worked in aviation and tourism.

Xin Luo is an Assistant Professor of Management Information Systems in Robert 0. Anderson School of Management at The University of New Mexico, USA. He received his Ph.D. in Information Systems from Mississippi State University. His research interests center around information security, E-commerce/M-commerce, wireless

communications technology, and global IT adoption and management. His research articles have appeared in *Communications of the ACM, Journal of the AIS, communications of the AIS, Journal of Organizational and End User Computing, International Journal of Information Security & Privacy, Information Systems Security, and Journal of Internet Banking and Commerce, etc.*

M. K. Raja is a Professor of Information Systems at the University of Texas at Arlington. His current research interests include Information Security Systems, Software, Networks and Organizations. He has published a number of articles in major computing and Information Systems journals. He serves on the editorial board and as a reviewer for a number of journals. He is a Certified Information System Security Professional, Certified Information Systems Auditor and a Certified Computing Professional. He has served as a consultant to Fortune 500 companies.

Expert Opinion

Interview with:

Peter B. McCarthy, Assistant Secretary for Management and CFO

United States Department of the Treasury

http://www. ustreas.gov/

Conducted by **Nathaniel J. Melby,** Winona State University, nmelby@winona.edu

JIPS: *Briefly describe your current position, and tell us a little bit about your previous job experience.*

PBM: Since its establishment in 1789, the United States Department of the Treasury has served as the steward of the nation's finances. Today it collects over $2 trillion annually for the federal government (through the 1RS), manages over $8 trillion in federal borrowings (through the Bureau of Public Debt), produces the nation's supplies of coins and currency (through the U.S. Mint and the Bureau of Engraving and Printing), regulates national banks and thrift institutions (through the Office of the Comptroller of the Currency and the Office of Thrift Supervision), and prepares the government's annual financial statements (through the Financial Management Service), among many other responsibilities. Treasury employs approximately 110,000 people and will spend over $18 billion in fiscal 2009 in undertaking its duties.

Treasury combines two functions - the Assistant Secretary for Management and the Chief Financial Officer — into a single position. In filling this role, I am responsible for Budgeting, Financial Reporting and Internal Control, Human Resources, Information Technology, Procurement, Emergency Preparedness, Privacy and Treasury Records, and Facilities Management. I was nominated for this position by the President on April 4, 2007 and, following confirmation by the U.S. Senate, was sworn in on August 3, 2007.

Prior to joining Treasury, I spent 27 years in the corporate banking business in Chicago, New York, Dublin, Tokyo and London. The banks that I worked for are all components of what is today J.P. Morgan Chase and Co. Following my retirement

from banking in 2002, I also spent 4 years in a management role at the Institute of International Finance, a Washington-based non-profit organization.

JIPS: *What would you describe as major challenges for IT in its role in the Department of the Treasury today? As the Assistant Secretary for Management, and CFO of the Department of the Treasury, how does your role interface with information and technology management?*

PBM: The overriding challenge for Treasury, as for all agencies of the federal government, is one of resource management -- attracting and retaining employees with the technical skills we need, and securing adequate appropriations from Congress. In fiscal 2009, Treasury will spend $3 billion on IT initiatives, and it is vitally important that every penny is wisely spent.

Treasury's Chief Information Officer reports to the Assistant Secretary for Management, so I have direct oversight responsibilities in this area.

JIPS: *What would you consider to be future challenges for the protection of privacy and security in government organizations?*

PBM: Treasury faces twin challenges in the years ahead.

On the privacy front, the most evident challenge involves protecting vast amounts of personal data which are, by necessity, collected, used and stored by the Internal Revenue

Service. Clearly the IRS could not carry out its responsibilities to collect taxes, provide refunds and, in the current environment, distribute economic stimulus payments, without detailed information concerning millions of taxpayers. Ensuring that such information is not inadvertently shared with, or made available to, inappropriate parties requires significant investments in systems and high degrees of training and personal awareness among IRS staff.

On the security front, Treasury's challenge is to constantly direct sensitive communications through secure channels and into secure storage devices. The Department is in possession of information that is critical to our national security. It also generates analysis regarding the behavior of domestic and international financial markets. In the wrong hands, such information might be misused to destabilize markets or to profit unfairly from knowledge that is not in the public domain. Treasury works closely with other federal agencies, particularly intelligence and law enforcement agencies, to ensure that its sensitive information is kept safe from adversaries and intruders.

JIPS: *What do you see as the future direction for the sharing of information in government organizations? Is this need increasing or declining? What drives this demand?*

PBM: The government is committed to meeting its responsibilities under the Freedom of Information Act (FOIA) which, as a general matter, entitles individuals to request information of a non-sensitive nature. The resulting administrative burdens are heavy. At Treasury, for example, 1,827 FOIA requests were received from the public in March, 2008

alone. Each request must be individually assessed for appropriateness, and then must be responded to. The government is also required, of course, to respond to requests for information relating to legal actions and to provide information in response to Congressional inquiries.

As information continues to be generated and accumulated by government, and as the Public grows ever more accustomed to transparency in government, there is every Reason to believe that demands for information will continue to grow.

JIPS: *From your professional experience, do you see historic and future needs for Privacy and security assurance being addressed best by organizational strategy, or by Technical capability?*

PBM: Technical capability in government is unquestionably important, just as it is in The private sector. However, organizational strategy is increasingly viewed as a key Factor in assuring privacy and security. Just last month. Treasury completed a Reorganization that combines its various headquarters responsibilities for Privacy, Treasury Records, and Disclosure into a single unit. A new Deputy Assistant Secretary position has been created to provide direction to this unit, and the incumbent Will report directly to the Assistant Secretary for Management. Organizational Changes such as this serve to elevate the importance and visibility of our privacy and Disclosure efforts, and to remind all Treasury employees of their responsibilities to Safeguard departmental information.

Peter B. McCarthy serves as Treasury's Assistant Secretary for Management and Chief Financial Officer. He is the principal policy adviser to the Secretary and Deputy Secretary on the management of the annual planning and budget process and on Matters involving the internal management of the Department and its bureaus. Prior To joining the Treasury Department, Mr. McCarthy was the Deputy Managing Director of the Institute of International Finance. He also worked in the banking Industry for twenty-seven years with First Chicago, Chase Manhattan, and Bank One. Mr. McCarthy graduated from Cornell University with a BA in Government, and Received an MBA in Finance from Southern Methodist University.

Nathaniel J. Melby is a Ph.D. Candidate in the Graduate School of Computer and Information Sciences at Nova Southeastern University. He has a B.S. in information systems from the University of Wisconsin-La Crosse, and an M.B.A. in technology and training from the University of Wisconsin-Whitewater. He currently works for a Fortune 500 company as a telecommunications engineer. His current research interests include information security, telecommunications, and distributed computing.