DEMYSTIFYING PERSONALITY AND PRIVACY: AN EMPIRICAL INVESTIGATION INTO ANTECEDENTS OF CONCERNS FOR INFORMATION PRIVACY

Melinda Korzaan
Middle Tennessee State University

Nita Brooks
Middle Tennessee State University

Timothy Greer
Middle Tennessee State University

Abstract

Given the ubiquitous nature of technology, privacy remains a focal issue. The purpose of this paper is to incorporate individual personality variables into a research model that helps explain and predict concerns about information privacy, computer anxiety, and behavioral intentions. The personality traits investigated include morality, self efficacy, risk taking, trust, and anxiety. Data was collected via a survey instrument that was completed by undergraduate college students. Analysis of the data indicates that morality and self efficacy have a positive, significant influence on individual concerns for information privacy (CFIP). Risk taking was found to have a negative, significant influence on CFIP. In addition, anxiety exerted a significant influence on computer anxiety. Both CFIP and computer anxiety were positively related to behavioral intentions. Individuals who possess high levels of morality and self efficacy and low levels of risk taking are more likely to be concerned about information privacy. Practitioners can benefit by establishing privacy statements, policies, and standards that emphasize low risk to the individual as well as highlight ethical responsibility and integrity in their practices regarding personal information. The results provided here further empirical knowledge by expanding an existing theoretical model to incorporate the role of individual characteristics in influencing concerns for information privacy. The study also provides insight for practitioners in establishing their information privacy statements, policies, and standards.

Keywords: information privacy, behavioral intentions, personality traits, self efficacy, anxiety

Introduction

Today individuals and organizations rely heavily on technology: high speed mobile devices, constant access to the Internet, etc. This reliance has lead to an increase in the amount of personal data that organizations capture, store, exchange, and use in order to conduct their operations. The disclosure of personal information by organizations, whether intentional or un-intentional, is currently a very sensitive issue and illegal in some countries. Some organizations are so leery of disclosing personal information that they won't disclose the information to the individual themselves when the information could be very beneficial. This situation arose during the mad cow scare in 2004 (Andersen, 2004). Large supermarket chains chose not to notify customers that may have purchased tainted meat in 2004. This would have alerted the customer as to how much personal information the company had stored. Organizations involved were very concerned as to how customers might react.

In another case, Google, the largest online search engine has been involved in a U.S. federal subpoena to hand over "search queries" on their customers. The question posed by many was whether Google's fight regarding this subpoena was to protect *privacy* or to protect their competitive advantage? When Google launched the popular free email service gmail in 2004, the online application came under heavy scrutiny from privacy advocates. The company openly stated that they would search the emails of users. Google was surprised that privacy became an issue with their email service (McCullagh, 2006; Orlowski, 2004; Rohde, 2004). Whether it's a rewards card, shopping basket analysis, or some other method, many corporations capture data on their customers. Once this data is captured, it can be analyzed, integrated, exchanged, and retrieved by the organization, which undoubtedly leads to concerns relating to data privacy, accuracy, and accessibility.

The issue of data privacy, accuracy, and accessibility were first presented by Mason (1986), the same decade that personal computers emerged at the forefront of office automation and innovation. Interestingly enough, recent research has shown that privacy is the most significant of the issues presented by Mason (Peslak, 2006). Smith, Milberg, and Burke (1996) presented a conceptual model that identified four underlying factors of information privacy concerns exhibited by individuals. The study showed that privacy is a complex construct with underlying factors pertaining to the collection, unauthorized secondary use (internal), unauthorized secondary use (external), and errors of personal information and data. Stewart and Segars (2002) extended Smith et al. (1996) by empirically validating the concern for information privacy (CFIP) construct and found that privacy concerns served as a mediator between computer anxiety and behavioral intentions. This research project builds on Stewart and Segars (2002) by examining the impact of personality traits on information privacy concerns, computer anxiety, and behavioral intentions. The personality traits incorporated into the theoretical model will further explain the behavior of individuals toward organizational processes and practices of collecting personal information. The personality characteristics included in the theoretical model are morality, self efficacy, risk taking, trust, and anxiety.

The purpose of the study is to identify the role personality characteristics play in influencing information privacy concerns, computer anxiety, and behavioral intentions. The study contributions include expanding previous research in CFIP and providing additional insight as to why individuals are concerned about privacy and how it influences their behavior pertaining to the collection of personal information.

Concern for Information Privacy

Concern for information privacy (CFIP) was first empirically introduced and examined by Smith, et al. (1996). In their original conceptualization of the construct, four different categories were recognized to reference information privacy practices in organizations: collection, unauthorized secondary use (internal), unauthorized secondary use (external), and errors. These four categories exemplify areas in which the individual exhibits concern about the use of their personal information and data.

The category of collection includes the general perceptions of the individual regarding the quantity or amount of data captured by the organization. Unauthorized secondary use, both internal and external, refers to exploiting collected data for alternative (secondary) uses without the consent of the individual from whom the data was originally gathered. External unauthorized secondary use specifically focuses on data being used by a party other than the organization that originally collected the data – a third party. The final category, errors, highlights the view that the data will be captured incorrectly or that the data will be modified to where it is no longer accurate. The framework presented by Smith, et al. (1996) was empirically examined and validated by Stewart and Segars (2002). The CFIP construct was found to be multi-dimensional and to mediate the relationship between computer anxiety and behavioral intentions.

The research presented here aims to extend this model by examining key personality traits to more accurately explain and predict CFIP. Further, this research will enhance what is known about how individual traits specifically relate to concern for information privacy. These theoretical and practical contributions will allow organizations to implement business decisions that work to alleviate and diminish concerns for information privacy. The remaining constructs in the proposed model are discussed and specific hypotheses presented in the following sections. An analysis of the model and a discussion of results are also provided.

Computer Anxiety

Understanding the reasons individuals accept or resist information technology is a core challenge in IS research (Davis, Bagozzi, and Warshaw, 1989). The quest to understand individual reactions to information technology has lead to the examination of computer anxiety as a key concept related to resistance to computers. Computer anxiety is defined as a "tendency of individuals to be uneasy, apprehensive, or fearful about current or future use of computers" (Stewart and Segars, 2002 p. 44).

Research has focused on understanding computer anxiety from many different perspectives. Physiological responses, such as increased heart rate, have been associated with computer anxiety as have more cognitive responses such as fear. Studies have examined the impact of gender (Sternberger, 1999) and age on computer anxiety. How individuals' level of expertise or familiarity with computers influences their level of computer anxiety has also received attention (Harrison and Rainer, 1992).

Computer anxiety has played a role in the study of Social Cognitive Theory acting as a mediator enhancing the model's explanatory capacity (Compeau, Higgins, and Huff, 1999). Stewart and Segars (2002) have also explored computer anxiety's role in predicting an individual's behavioral intentions.

Morality

Morality is a personal value that is central to an individual's cognitive structure (Abdolmohammadi and Baker, 2006). As a personal value, morality is comparable to a stable individual trait, because personal values represent "enduring beliefs that transcend specific situations" (Abdolmohammadi and Baker, 2006 p. 12). Morality encompasses consistent beliefs about human virtues such as trustworthiness, honesty, respect for authority, sincerity, and a regard for rules and laws (Leach, Ellemers, and Barreto, 2007; Abdolmohammadi and Baker, 2006).

The theoretical link between morality and privacy originates in the moral basis for the right to information privacy. This basis includes values such as personal dignity, self-identity, and autonomy (Michelfelder, 2001). Individuals who possess high levels of individual morality would logically have a tendency to place a high level of importance on these foundational ideals of information privacy.

Personal values (such as morality) are recognized in the literature as influential forces on attitudes and behaviors (Abdolmohammadi and Baker, 2006). Individuals who possess a high level of morality as an integral part of their cognitive makeup would reasonably view the right to information privacy as an inalienable right and moral sanction. They would likely have a higher degree of concern for maintaining the integrity of personal information and protecting the sacredness of an individual's right to have their own personal information for the purpose of maintaining personal identity and personal expression. Their attitude toward a right to information privacy would likely be influenced by the degree of their moral disposition. Therefore, it is hypothesized that the morality will be positively related to concerns for information privacy.

H1. Morality will be positively related to CFIP.

General Self Efficacy

General self-efficacy is defined as an individual's estimate of his or her abilities to function across a variety of situations (Bandura, 1997). It differs from task specific self-efficacy and has been considered a trait-like construct (Chen, Gully, Whiteman, and Kilcullen, 2000). An individual with a high level of general self-efficacy has a high regard for his or her abilities to control a given situation – *an internal locus of control* (Langford and Reeves, 1998).

Research has shown that individuals with a greater desire for control also have greater concern for privacy of their information (Phelps, D'Souza, and Nowak, 2001). When individuals with a high regard for their abilities place their personal information in the hands of others, where it is out of their control, they would be expected to have a higher level of concern. We therefore hypothesize that the individual's general self-efficacy beliefs will be positively related to concern for information privacy.

H2. Self Efficacy will be positively related to CFIP.

Risk Taking

Risk-taking behavior is often represented by and referred to as an individual's risk propensity (MacCrimmon and Wehrung, 1990) – an individual's willingness to take risks. Sitkin and Pablo (1992) proposed that individuals can be categorized by their risk propensity; individuals that are risk-seeking are more likely to take risks than those that are risk-averse (lower propensity). Individuals that are risk-seekers tend to view situations involving risk as having the likelihood of a positive outcome (or higher probability of gain) compared to those that are risk-averse (Sitkin and Pablo, 1992).

It is recognized that sharing personal information with a company would be seen as bearing some level of risk. Previous research indicates that an individual's risk beliefs about sharing sensitive personal information are related to concern for information privacy (Malhotra, Kim, and Agarwal, 2004). Since individuals with a higher propensity for risk view situations involving risk more positively, it is hypothesized that an individual's level of risk taking or risk propensity will be negatively related to concern for information privacy.

H3. Risk taking will be negatively related to CFIP.

Trust

An individual's propensity to trust is defined as a trait that is "stable across situations" (Mayer, Davis, and Schoorman, 1995 p. 716) and that specifically highlights the individual's "generalized expectation about the trustworthiness of others" (Mayer, et al., 1995 p. 715). This type of trust is also referred to as dispositional trust and is seen as a "personality-driven feature of an individual" (Pennanen, Kaapu, Paakki, 2006 p. 2).

Trust is an important factor that facilitates an individual's ability to deal with uncertainty and risk (McKnight, Choudhury, and Kacmar, 2002). Individuals with a higher propensity to trust would be expected to exhibit less concern or fear in sharing personal information as they inherently believe that others are generally trustworthy and have good intentions. It is anticipated that the greater the expectations of the individual regarding the trustworthiness of others, the lower the level of concern will be regarding information privacy.

H4. Trust will be negatively related to CFIP.

Anxiety

Anxiety represents an individual's general predisposition to experience anxiety when faced with challenges or difficulties (Spielberger, 1983). This general tendency is often referred to as trait anxiety. Trait anxiety represents the likelihood that a person will experience specific instances of state anxiety – anxiety that exists in certain situations (Spielberger, 1983).

Computer anxiety focuses specifically on an individual's fear of interaction with computers and is considered a form of state anxiety (Chua, Chen, and Wong, 1999). Previous research has indicated that there is a direct and positive relationship between an

individual's trait-anxiety and computer anxiety (Thatcher and Perrewe, 2002). It is therefore hypothesized here that trait anxiety will be positively related to computer anxiety.

H5. Anxiety will be positively related to Computer Anxiety.

The concern for information privacy construct emphasizes fear of the potential misuse of data and the possible incorrect collection of data from individuals. Individuals that exhibit a high level of computer anxiety are inherently distrusting of technology. It is therefore expected that this would influence concern for privacy infractions. Stewart and Segars (2002) empirically tested and found support for this relationship. It is included here to accurately represent previous research findings.

H6. Computer anxiety will be positively related to CFIP.

Behavioral Intentions

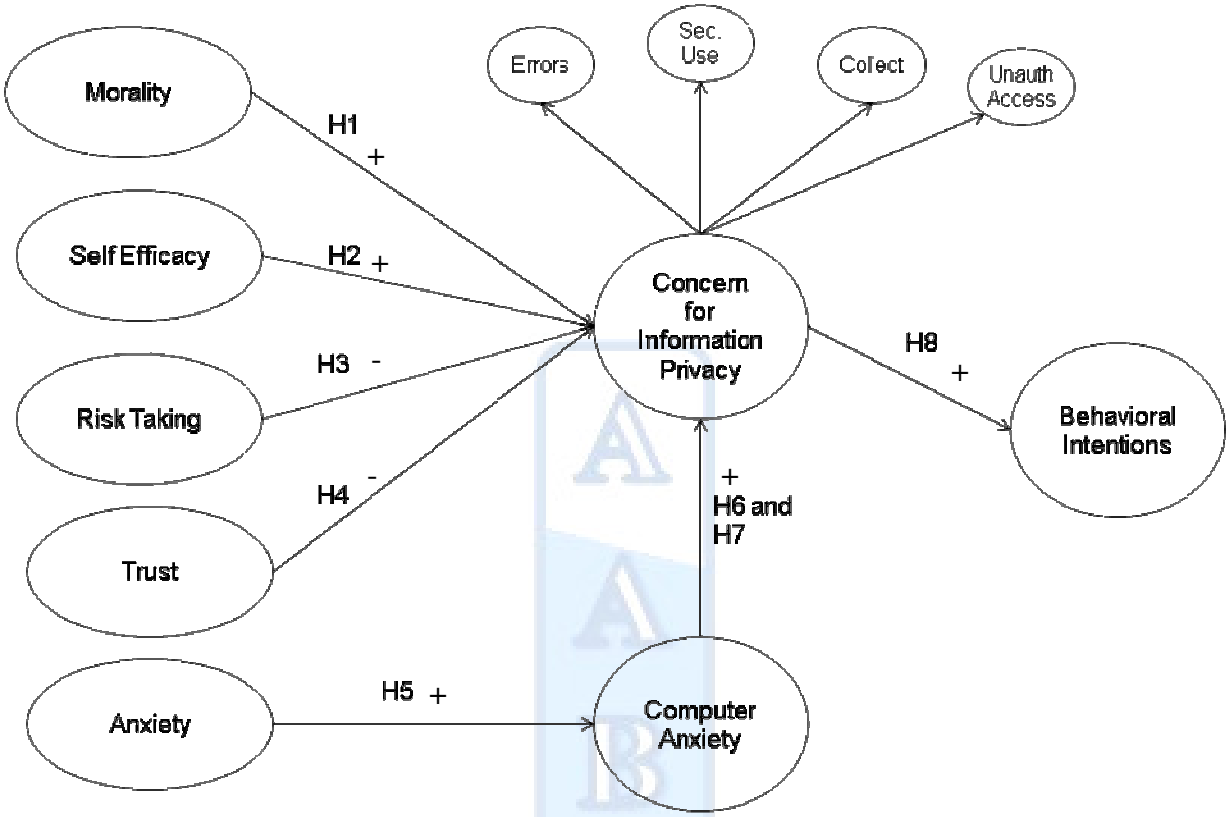
Previous research has empirically supported the notion that an individual's concern for information privacy will serve to mediate the relationship of computer anxiety and behavioral intention (Stewart and Segars, 2002). This analysis acknowledges the relationship as proposed by Smith, et al. (1996) and includes it to be consistent with previous theoretical examinations of the CFIP construct. It is therefore hypothesized that

H7. The relationship between computer anxiety and behavioral intentions will be fully mediated by CFIP.

The direct relationship between CFIP and behavioral intentions is also hypothesized here as highlighted by Stewart and Segars (2002). The higher the individual's level of CFIP, the more likely they will be to invoke the necessary measures to protect their privacy. Such measures might include the decision not to provide information online or not to register for mailing lists.

H8. CFIP will be positively related to behavioral intentions.

Figure 1: Proposed Model



Methodology

Information was gathered from undergraduate college students enrolled in an introductory computer course. IRB approval was requested and received for the data collection. Survey participants were informed that their participation was voluntary and that their individual responses would remain strictly confidential. Measurement items were adapted from existing instruments and were evaluated on a 7-point Likert scale. Items for the five personality traits: morality, anxiety, trust, self efficacy, and risk taking, were adapted from the International Personality Item Pool (IPIP). The IPIP is an online resource created by a collaboration of researchers to provide measurement items for personality characteristics (Goldberg, 1999; Goldberg, Johnson, Eber, Hogan, Ashton, Cloninger, and Gough, 2006). The CFIP measurement instrument developed by Smith et al. (1996) was used in this study to measure CFIP, and both computer anxiety and behavioral intention measures were adapted from Stewart and Segars (2002). There were 230 usable surveys completed. Of the total respondents, 61% were male and 39% were female. Ninety-nine percent (99%) of the students were between the ages of 18 and 24, thereby representing the typical age range seen in a traditional college student population. The survey technique is commonly used in studies evaluating privacy concerns and individual characteristics (Smith et al, 1996; Stewart and Segars, 2002). Refer to Appendix A for the complete survey instrument.

Structural equation modeling with Amos was used to analyze the data (Kline, 1998), and the two-step modeling approach was employed (Anderson and Gerbing, 1988). First, a confirmatory factor analysis was conducted assessing the convergent and discriminant validity of the constructs. Convergent validity was determined by evaluating composite reliabilities (Chin, 1998; Bock, Zmud, Kim, and Lee, 2005) and average variance extracted (Chin, 1998; Fornell and Larker, 1981). Discriminant validity was evaluated by comparing the correlation of each paired construct to the average variance extracted (Bock et al., 2005; Fornell and Larker, 1981). Once convergent and discriminant validity were confirmed, the second step consisted of testing the structural model. The structural model was evaluated by conducting a path analysis, which analyzes not only the significance of the hypothesized relationships but also includes an overall evaluation of the model fit (Kline, 1998).

Results

Results from assessing construct validity confirm that the measures used in this study uphold adequate convergent and discriminant validity thresholds. Assessment of convergent validity is illustrated in Table I. Average variance extracted exceeds .50, and composite reliabilities exceed .70 for every construct in this study (Chin, 1998; Bock et al., 2005). Assessment of discriminant validity is illustrated in Table II. For each pair of constructs, the correlation between the constructs is less than the average variance extracted for each of the individual corresponding constructs (Fornell and Larker, 1981; Bock et al., 2005). Confirmation was also found for modeling concern for information privacy as a second order construct. All path loadings for each of the first order factors (errors, collection, unauthorized secondary use, and unauthorized access) are significant ($p<.001$) and comparable to values found in prior studies, ranging from $\beta=.68$ to $\beta=.86$ (Steward and Segars, 2002).

Table I: Composite Reliabilities and Average Variance Extracted

Construct	Average Variance	Composite Reliability
Behavioral Intentions	.51	.76
Computer Anxiety	.53	.81
CFIP	.58	.85
Morality	.56	.78
Anxiety	.53	.84
Trust	.54	.90
Self Efficacy	.52	.84
Risk Taking	.54	.82

- Composite reliabilities are .70 or greater (Chin, 2998; Bock et al., 2005), and average variances extracted are .50 or greater (Fornall and Larker, 1981; Bock et al., 2005).

Table II: Discriminant Validity

	BI	CANX	CFIP	MORAL	ANX	TRUST	SE	RISK
BI	.714							
CANX	.120	.728						
CFIP	.366	-.053	.762					
MORAL	.032	-.073	.343	.745				
ANX	.007	.337	.044	-.016	.726			
TRUST	-.099	-.113	.100	.318	-.225	.733		
SE	.130	-.196	.180	.346	-.309	.197	.722	
RISK	-.018	.058	-.254	-.266	-.044	-.018	.197	.734

- The shaded numbers shown on the diagonal are the square root values of the average variance extracted.
- For each construct pair, the correlation between the constructs is less than the average variance extracted (Fornell and Larcker, 1981; Bock et al., 2005).
- BI: Behavioral Intentions; CANX: Computer Anxiety; CFIP: Concern for Information Privacy; MORAL: Morality; ANX: Anxiety; TRUST: Trust; SE: Self Efficacy; RISK: Risk Taking

Table III provides a summary of hypothesis testing. All relationships were significant as hypothesized, except for H4, H6, and H7. Trust did not have a significant influence on CFIP with a β=-.001 and p-value=.711(H4). The relationship between computer anxiety and CFIP was also non-significant with a β=-.001 and p-value =.983(H6). Because H6 was not supported, H7 was also not supported because the relationship between computer anxiety and behavioral intentions cannot be mediated by CFIP if the relationship between computer anxiety and CFIP is non-significant (Baron and Kenny, 1986).

Morality (β=.233, p-value=.003) as hypothesized in H1 and self efficacy as hypothesized in H2 (β=.154, p-value=.044) both had a positive, significant influence on CFIP. The relationship between risk taking and CFIP (H3) was negative and significant (β=-.216, p-value=.004). General, trait-like anxiety (H5) was found to exert a strong, positive influence on the specific, state-like characteristic of computer anxiety (β=.337, p-value<.001). In turn,

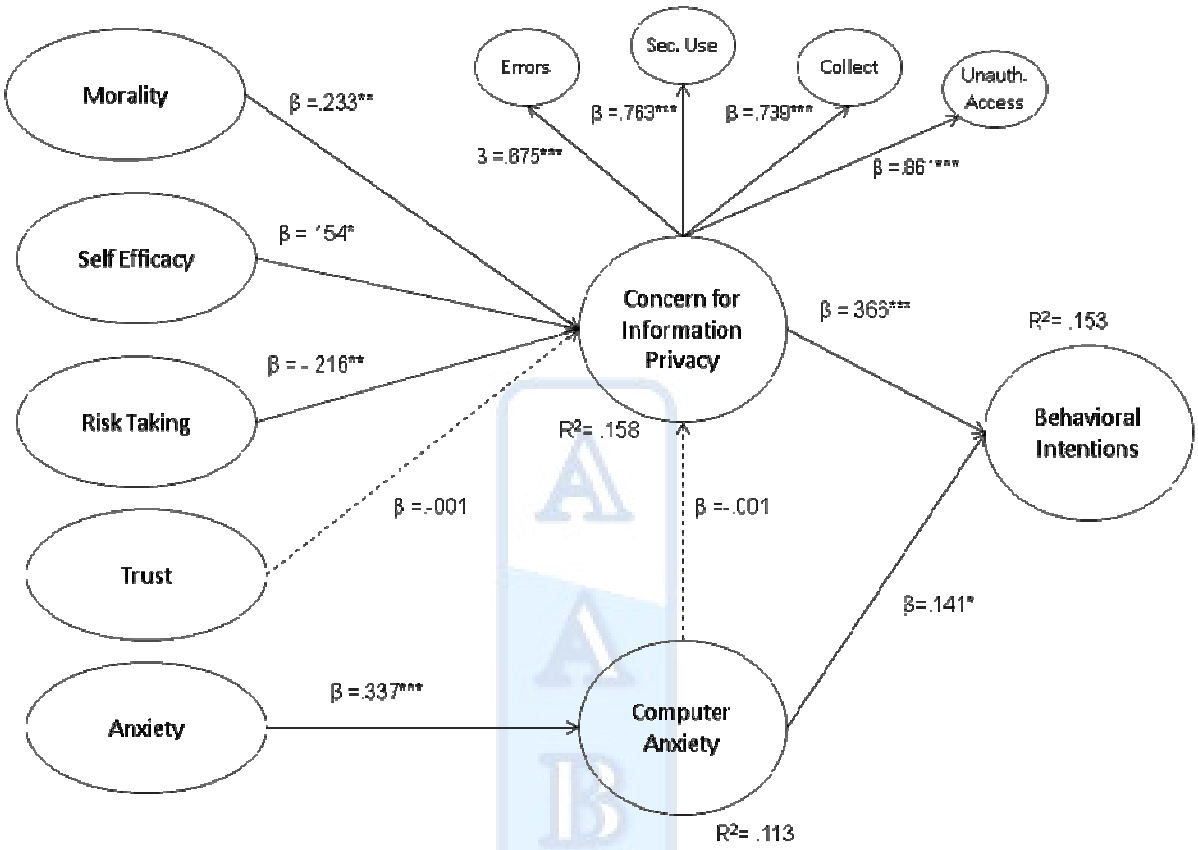
although the relationship between computer anxiety and behavioral intentions was not mediated through CFIP, the direct relationship between computer anxiety and behavioral intentions was found to be positive and significant with β=.141 and p-value=.022. Lastly, H8, was supported with CFIP exerting a significant, positive influence on behavioral intentions (β=.366, p-value<.001). The final model is displayed in Figure 2. Evaluation of overall fit indices indicate good model fit and the amount of variance explained in the three dependent variables (CFIP, computer anxiety, and behavioral intentions) was noteworthy as well. For CFIP, 15.8% of the variance was explained, computer anxiety was 11.3%, and behavioral intention was 15.3%.

Table III: Hypothesis Testing Results

Hypothesis	Relationship	B	P-value	Hypothesis Outcome
H1	Morality -> CFIP	.233	.003	Supported
H2	Self Efficacy -> CFIP	.154	.044	Supported
H3	Risk Taking -> CFIP	-.216	.004	Supported
H4	Trust -> CFIP	-.001	.711	Not Supported
H5	Anxiety -> Computer Anxiety	.337	<.001	Supported
H6	Computer Anxiety -> CFIP	-.001	.983	Not Supported
H7	Computer Anxiety -> Behavioral Intentions Computer Anxiety -> Behavioral Intentions will be fully mediated by CFIP	.141	.022	Not Supported. The relationship between Computer Anxiety (Independent Variable) and CFIP (Mediator) is not significant [H6].
H8	CFIP -> Behavioral Intentions	.366	<.001	Supported
	CFIP R^2	.16		
	Computer Anxiety R^2	.11		
	Behavioral Intentions R^2	.15		

- The conditions for full mediation occur when (1) a significant relationship exists between the independent variable and the mediator – (path a), (2) a significant relationship exists between the mediator and the dependent variable (path b), and (3) when path a and path b are controlled, then a once significant relationship becomes non-significant (Baron and Kenny, 1986).

Figure 2: Final Model



- * p<.05; ** p<.01, *** p<.001

Fit Measures	RMSEA	GFI	AGFI	NFI	CFI	Evaluation of Fit
Thresholds	≥ .05	≥ .90	≥ .80	≥ .90	≥ .90	
Figure 2	.072	.945	.890	.894	.937	Good

Discussion and Conclusion

The purpose of this research study was to develop and examine a model focused on understanding how personality variables directly and indirectly influence an individual's concern for information privacy (CFIP) and behavioral intentions. In addition, further examination was conducted to build upon previous research and to better comprehend the relationship between CFIP, computer anxiety, and behavioral intentions.

Of the five personality variables examined, morality (H_1), self-efficacy (H_2), and risk-taking (H_3) significantly and directly impacted CFIP, and, as hypothesized, anxiety was found to significantly impact computer anxiety (H_5). This indicates that individuals with high levels of morality and self-efficacy will tend to exhibit higher levels of concern for information privacy.

Individuals with lower levels of risk propensity, or those that tend to be risk averse, will also exhibit higher levels of CFIP.

Anxiety, as examined in this model, represented an individual's trait anxiety; the individual's general tendency to experience anxiety in challenging or difficult situations. As hypothesized, the individual's level of trait anxiety directly impacted state anxiety, which is represented here specifically as computer anxiety. This finding supports previous research (Thatcher and Perrewe, 2002) and highlights the importance of including the personality trait in models examining computer anxiety.

Counter to our hypothesis (H_4), trust was not found to significantly relate to concern for information privacy. It is possible that the relationship between trust and CFIP is more complicated than presented. As noted by McKnight, et al. (2002), trust relates to an individual's ability to deal with uncertainly in situations. Since this sample was drawn from an educational institution, it might be that the trustworthiness of the university was not a salient issue and thus did not impact how concerned individuals were with the privacy of their personal information. Additional research should be conducted with other targeted samples to examine the perceived uncertainty and risk of the information sharing environment and to extend what is known about the relationship between trust and CFIP. Furthermore, a limitation of this study was the use of a college student sample and research findings cannot be claimed to generalize. Therefore, future studies of other samples also need to be conducted to examine if the current results generalize to other populations.

Contrary to the findings provided by Stewart and Segars (2002), for this sample, the direct relationship between computer anxiety and CFIP (H6) was not supported. Consequently, the mediating role of CFIP on the relationship between computer anxiety and behavioral intentions was not supported (H7). As indicated by the steps followed in testing the mediation hypothesis, it was found that computer anxiety significantly impacted behavioral intentions. As seen in Figure 2, the final model includes this relationship. The different samples used in the studies could be a potential reason for the dissimilar findings just mentioned. The sample in this study was drawn from a group of college students from a specific geographical region in the U.S. The sample used in the Stewart and Segars (2002) study reflected customers from several different regions in the U.S. These disparities could be attributed to the differences in education across the groups or other unknown demographic differences. The final hypothesis (H8) addressing the relationship between CFIP and behavioral intentions, as found in previous research, was supported.

Overall, the model proposed, provided an R^2 of .158 – explaining approximately 16% of the variance in CFIP. As a potential response to these findings, organizations should work to emphasize the importance of information integrity and acknowledge the importance of integrity in maintaining a person's identity. Systems should emphasize individuals' control of their personal information and include provisions that lower the risk perceived in collecting and accessing personal information. By implementing appropriate policies and procedures, organizations can work to ease the individual's tensions regarding sharing personal information and implement standards that provide increased awareness of the individual's control of his or her personal information.

References

Abdolmohammadi, J.J. & Baker, C. R. (2006). Accountants' value preferences and moral reasoning. *Journal of Business Ethics,* 69(1), 11-25.

Andersen, P. (2004, January 22). Mad cow: Privacy vs. protection. *InformationWeek*, available at: http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=17500675.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin,* 103(3), 411-423.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York, NY: W.H. Freeman.

Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173-1182.

Bock, G., Zmud, R. W., Kim, Y., & Lee, J. (2005). Behavioral intention formation in knowledge sharing: Examining the roles of extrinsic motivators social-psychological forces, and organizational climate. *MIS Quarterly*, 29(1), 87-111.

Chen, G., Gully, S.M., Whiteman, J., & Kilcullen, R.N. (2000) Examination of relationships among trait-like individual differences, state-like individual differences, and learning performance. *Journal of Applied Psychology,* 85(6), 835-847.

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). Mahway, NJ: Lawrence Erlbaum Associates.

Chua, S.L., Chen, D., & Wong, A.F.L. (1999). Computer anxiety and its correlates: A meta-analysis. *Computers in Human Behavior*, 15(5), 609-623.

Compeau, D. R., Higgins, C. A., & Huff, S. (1999) Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 23(2), 145-158.

Davis, F.D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8), 982-1003.

Fornell, C. & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18(1), 39-50.

Goldberg, L.R. (1999). A broad-bandwidth, public domain, personality inventory measuring the lower-level facets of several five-factor models. In I. Mervielde, I. Deary, F. DeFruyt, & F. Ostendorf (Eds.), *Personality Psychology In Europe*, Vol. 7, (pp. 7-28). Tilburg, The Netherlands: Tilburg University Press.

Goldberg, L.R., Johnson, J.A., Eber, H.W., Hogan, R., Ashton, M.C., Cloninger, C.R., & Gough, H.C. (2006). The international personality item pool and the future of public domain personality measures. *Journal of Research in Personality,* 40, 84-96.

Harrison, Allison W. & Rainer, Kelly Jr. (1992). The influence of individual differences on skill in end-user computing. *Journal of Management Information Systems,* 9(1), 93-111.

International Personality Item Pool: A Scientific Collaboratory for the Development of Advanced Measures of Personality Traits and Other Individual Differences, available at: http://ipip.ori.org/.

Kline, R. B. (1998). *Principles and Practice of Structural Equation Modeling*. New York: The Guilford press.

Langford, M. & Reeves, T.E. (1998). The relationship between computer self-efficacy and personal characteristics of the beginning information systems student. *Journal of Computer Information Systems*, 38(4), 41-45.

Leach, C.W., Ellemers, N. & Barreto, M. (2007). Group virtue: The importance of morality (vs. competence and sociability) in the positive evaluation of in-groups. *Journal of Personality and Social Psychology*, 93(2), 234-249.

MacCrimmon, K.R., & Wehrung, D.A. (1990). Characteristics of risk taking executives. *Management Science,* 36(4), 422-435.

McCullagh, D. (2006, January 26). Court date set for Google lawsuit. *CNET News.com*, available at: http://news.cnet.com/Court-date-set-for-Google-lawsuit/2100-1030_3-6031941.html.

McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research*, 13(3), 334-361.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users information privacy concerns: the construct, scale, and causal model. *Information Systems Research*, 15(4), 336-355.

Mason, R.O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 10(1), 5-12.

Mayer, R.C., Davis, J.H., & Schoorman, F.D. (1995). An integrated model of organizational trust. *Academy of Management Review*, 20(3), 709-734.

Michelfelder, D.P. (2001) The moral value of informational privacy in cyberspace. *Ethics and Information Technology,* 3(2), 129-1325.

Orlowski, A. (2004, April 3). Google mail is evil – privacy advocates. *The Register*, available at: http://www.theregister.co.uk/2004/04/03/google_mail_is_evil_privacy/.

Pennanen, K., Kaapu, T., & Paakki, M.K. (2006). Trust, risk, privacy, and security in e-commerce. *Proceedings of the ICEB + eBRF Conference,* Tampere, Finland.

Peslak, A.R. (2006). PAPA revisited: A current empirical study of the Mason framework. *The Journal of Computer Information Systems*, 46(3), 117-123.

Phelps, J.E., D'Souza, G., & Nowak, G.J. (2001) Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing,* 15(4), 2-17.

Rohde, L. (2004, April 15). Privacy issues plague Google's gmail. *PCWorld*, available at: http://www.pcworld.com/article/115692/privacy_issues_plague_googles_gmail.html.

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.

Spielberger, C.D. (1983). *Manual for state-trait anxiety inventory*. Palo Alto, CA: Consulting Psychologists Press.

Sternberger, C. S. (1999). *An examination of state anxiety and computer attitudes related to achievement on paper-and-pencil and computer-based mathematics testing of nursing students*. Unpublished doctoral dissertation, Purdue University.

Stewart, K.A. & Segars, A.H. (2002). An empirical examination of the concern for information privacy instrument", *Information Systems Research,* 12(1), 36-49.

Thatcher, J.B. & Perrewe, P.L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly,* 26(4), 381-396.

Appendix A: Measurement Scales

Behavioral Intentions (Source: Stewart and Segars, 2002)

How likely are you, within the next three years to …

1. Refuse to give information to a business or company because you think it is too personal?
2. Take action to have your name removed from direct mail lists for catalogs, products, and services?
3. Refuse to purchase a product because you disagree with the way a company uses personal information?

Concern for Information Privacy (Source: Smith et al., 1996)

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by clicking the bubble that corresponds to your response on the scale.

Collection

1. It usually bothers me when companies ask me for personal information.
2. When companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many people.
4. I am concerned that companies are collecting too much personal information about me.

Unauthorized Access

1. Companies should devote more time and effort to preventing unauthorized access to personal information.
2. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.
3. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Errors

1. All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.
2. Companies should take more steps to make sure that personal information in their files is accurate.
3. Companies should have better procedures to correct errors in personal information.
4. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Secondary Use

1. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provide the information.
2. When people give personal information to a company for some reason, the company should never use the information for any other purpose.
3. Companies should never sell the personal information in their computer databases to other companies.

4. Companies should never share personal information with other companies unless it has been authorized but the individuals who provided the information

---

Computer Anxiety (Source: Stewart and Segars, 2002)

1. Sometimes I am afraid that information systems' departments may lose my data.
2. I am anxious and concerned about the pace of automation in the world.
3. I am easily frustrated by computerized bills.
4. I am sometimes frustrated by increasing automation in my home.

Personality Traits (Source: International Personality Item Pool http://ipip.ori.org; Goldberg, 1999; Goldberg et al., 2006)

The following phrases describe people's behaviors. Please use the rating scale below to describe how accurately each statement describes you. Describe yourself as you generally are now, not as you wish to be in the future. Describe yourself as you honestly see yourself, in relation to other people you know of the same sex as you are, and roughly your same age. So that you can describe yourself in an honest manner, your responses will be kept in absolute confidence.

Please read each statement carefully, and then click on the bubble that corresponds to your response on the scale.

Morality

1. Like harmony in my life.
2. Try to follow the rules.
3. Respect authority.

Anxiety

1. Get stressed out easily.
2. Worry about things.
3. Fear for the worst.
4. Am afraid of many things.
5. Get caught up in my problems.

Trust

1. Trust others.
2. Believe that others have good intentions.
3. Trust what people say.
4. Believe that people are basically moral.
5. Believe in human goodness.
6. Think that all will be well.
7. Distrust people. (R)
8. Suspect hidden motives in others. (R)

Self Efficacy

1. Have excellent ideas.
2. Am quick to understand things.
3. Can handle complex problems.

4. Think quickly.
5. Formulate ideas clearly.

Risk Taking

1. Enjoy being reckless.
2. Take risks.
3. Seek danger.
4. Know how to get around the rules.