Consumer E-Commerce Dissonance: Innovating Without Alienating Before Information Overload

Cory Taylor Cromer
Oregon State University

The Internet and its innovative technological advances, while presenting opportunities for shopping and convenience, have opened new threats for user privacy and the potential for information overload and consumer dissonance. Personal identifying information being collected on sites visited, the subsequent sharing of personal information, and the evolving perceived technical threats have lead to many consumers feeling that they have lost control. Government regulators, consumer advocacy groups, and e-businesses need to understand how Internet innovation affects the consumer and whether their marketing strategy is encouraging or limiting innovation.

INTRODUCTION

A 2005 survey found that due to new concerns about being confronted by technologies they don't understand on the web, a majority of consumers have stopped giving out personal information on the Internet, 30% say they have reduced their overall use of the Internet, and 25% say they stopped buying things online (Princeton Survey Research, 2005).

These increasing amounts of innovation and threats to privacy online can lead to people either decreasing the amount of time they spend online, or even choosing not to visit or purchase from specific websites that seem overwhelming (Phelps, Nowak & Ferrell, 2000). With this increasing behavior by online consumers for anonymity to protect their privacy, marketers need to take steps to understand this behavior in order to shift the mindset of the consumer from one of defensive and restrictive behavior, to an environment where the user experience builds trust and increases Internet usage, as e-businesses continue to innovate and add new technologies and content to their consumers (Miyazaki & Fernandez, 2001).

With increasing use of complementary technologies such as mobile devices, consumers are given more opportunities for Internet consumption, but also with new threats to privacy. Sheehan and Hoy (1999) have found significant correlations between privacy concerns and online privacy behavior. This introduces an innovation paradox that currently exists in cyberspace with consumer dissonance over evolving online innovation and that may increase privacy threats. At the aggregate level, amidst ever increasing online privacy concerns, Internet usage continues to increase, along with new innovative website design and technologies. It appears that fear levels pertaining to online privacy concern are not high enough for commerce to decline as online purchasing continues to grow at upwards of 25% over the previous year (Maguire, 2005). This suggests that consumers are becoming more selective of when and with whom they conduct business with online. Which raises the question, how are consumers making

these choices and alternating their behavior? Moreover, how can e-business continue to innovate without alienating their consumers?

When looking at this "online innovation dissonance" presented, a classic fear appeals model (Keller & Block, 1996) would suggest that consumers would decrease their Internet usage for both low and high levels of fear that would accompany the increasing innovation used by e-businesses. This model is not congruent with what is being seen in the marketplace as privacy fears are at their highest while Internet usage and online innovation are also at their highest (Ipsos Insight, 2005). Moreover, broadband Internet access was at an all time high in 2004 and growth is expected to triple in the next 5 years (Ipsos Insight, 2005). The Protection Motivation model (Rippetoe & Rogers, 1987; Rogers, 1983) is a theory that has been used extensively in public health and social sciences to measure the coping behavior of a person when they are confronted with a threatening event. The theory examines how information is taken through a cognitive mediating process that affects behavior.

The author develops a Protection Motivation model in the context of online privacy concerns in order to examine how the "online innovation paradox" and resulting consumer dissonance may be explained. Hypotheses are developed based upon the Protection Motivation framework in respect to online behavior and privacy. For a comprehensive test of the model, a study was developed with existing scales from the Protection Motivation literature modified for online consumers, and was administered to 482 online consumers in the United States. The results are presented and help explain why there is an increased use of the Internet in face of growing Internet privacy concerns. Finally, both theoretical and managerial implications are discussed with insights towards future research.

THEORETICAL DEVELOPMENT

Current Views of Online Consumers

Many consumers feel their privacy is not being adequately protected despite a variety of regulatory and self-regulatory programs. A recent survey of adult online users suggests that a strong majority of adult online users in the U.S. continue to agree, "consumers have lost all control over how personal information is collected and used by companies" (Privacy and American Business, 2005). Indeed, consumers have exhibited these concerns for a number of years (Taylor, 2003; Fox, 2000; Cranor, Reagle, & Ackerman, 1999) and continue to be concerned as new threats emerge as evidenced by the introduction of mobile technologies (Clarke, 2001; Milne & Rohm, 2003) and the growth of information and that can lead to identity theft (Saparito, 2005; Privacy Rights Clearinghouse, 2005). In addition, threats can range from being a hassle to experiencing social embarrassment (Goodwin 1991; Cranor et al. 1999).

Marketers have used consumer information in promotion and marketing efforts for decades, with increased usage by online marketers in trying to understand online consumer behavior (Fox 2000; Cranor et al., 1999). This has included both market level information and individual specific information that is needed to continue to innovate towards the changing online consumer landscape (Nowak & Phelps, 1995). Multiple studies have found that consumers are most willing to give up demographic and psychographic information in return for marketing offers (Wang & Petrison, 1993). Many consumers feel the invasion of privacy and a sense of innovation overload has occurred when personal information has been taken out of their control during an encounter with a new technology that they do not recognize on a website (Lwin & Williams, 2003). Goodwin (1991) suggests that the majority of consumers seek two types of control; environmental control and dissemination control. When consumers feel they have lost either environmental control or dissemination control, they may engage in certain types of behavior such as vigilant data management, refusing to provide information or giving false information, filing complaints, limiting their time online or not going online at all (Lwin & Williams 2003).

When faced with website innovation, online consumers who feel their privacy has been invaded or fear a lack of control may engage in falsification or fabrication of personal data (Lwin & Williams, 2003). Hiller and Cohen (2002) are diligent in recognizing that this type of online behavior may be the most costly not only to marketers, but also to government regulators and consumer advocacy groups. The central premise is that these groups are modeling consumer trends and making decisions on false or

fabricated information, even suggesting this could lead to inhibiting overall Internet innovation, especially e-commerce (Bolin 1998). For marketers this can directly lead to improper analysis that can have dramatic impacts on marketing costs and time (Lwin & Williams, 2003). Pitkow and Kehoe (1997) found that 10% of online consumers never provide personal information of any kind when prompted by websites requiring registration.

If online consumers feel helpless from information overload from changes in digital innovation and their privacy has been breached or threatened, they may engage in various types of consumer complaining behavior (Hoy & Sheehan 1999). Kehoe, Pitkow and Morton (1997) found that 19% of online consumers have contacted companies to have their names removed from email lists and 5% have engaged in retaliations as strong as email and website "bombing". In addition, online consumers may join an online advocacy group or mechanism (chat boards, online ratings) which serve to discredit the e-business (Nasir, 2004). Online consumers have also increased their visits to online infomediaries that provide information on companies and websites that keep and abuse consumer information (Hoy & Sheehan 1999). In addition to providing false information, consumers are increasingly using technologies such as anonymizers, cookie blockers, and remailers to keep their anonymity and use the Internet without having their behaviors linked to their real self, which can limit e-businesses ability to innovate for their consumers (Cranor et al., 1999).

MODEL DEVELOPMENT

Identity theft, unwanted intrusions, and having personal information shared with third parties continue to be issues consumers worry about while going online. Viewing this phenomenon through the lens of a classic fears appeal model (Keller & Block, 1996) would suggest that individuals would refrain from using the Internet, yet Internet usage and innovation remains at an all time high as mentioned earlier in the discussion of the online privacy paradox. That is, Internet usage and innovation remain high even while online privacy concerns are more prevalent than ever.

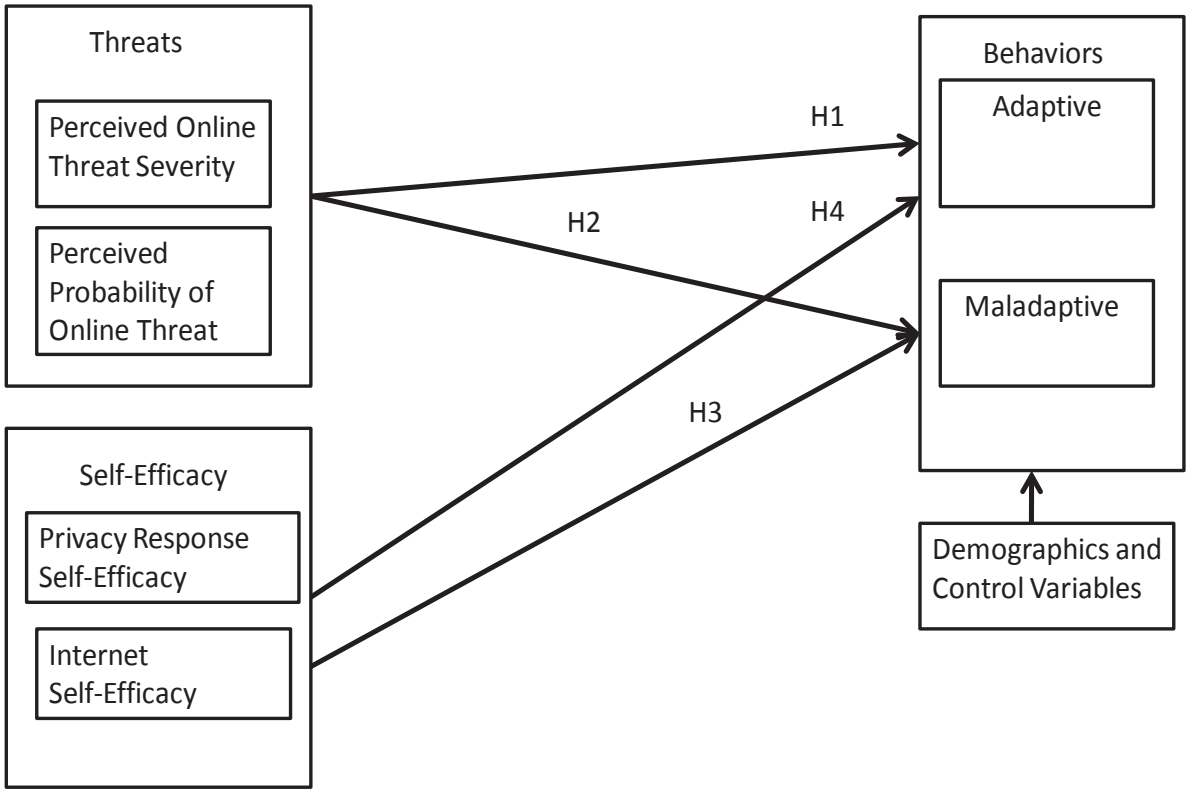
To address these issues, a protection motivation theory is employed which measures the coping behavior of a person when they are confronted with a new or unknown threatening event (Rippetoe & Rogers, 1987; Rogers, 1983). This model, used largely in health and social sciences, helps to explain how a person takes in information and passes it through a cognitive mediating process that affects behavior. The protection motivation model posits that individuals' motivation to protect themselves, through the cognitive mediating process depends upon the threat and coping modes.

STUDY 1: MODEL AND HYPOTHESIS

A protection motivation model was used to create a survey methodology to test and improve the generalizability of the results towards measuring the "online innovation paradox" of increased Internet usage and innovation along with increasing amounts of dissonance from consumers over privacy concerns. The model reflected in Figure 1 specifically addressed measuring Internet self-efficacy and privacy response self-efficacy while the other constructs remain the same as past studies using the protection motivation model.

It is anticipated that more hours spent on the Internet combined with visiting a wider variety of web sites with varying degrees of innovation, will raise the potential threat to privacy. This can create fear within the individual that leads them to cognitively evaluate the situation and their ability to protect their privacy. Depending on an individual's level of Internet self-efficacy, we assert that they can either address this dissonance with adaptive behaviors, or they can choose not to deal with the situation and reduce their hours on the Internet. For example, a recent survey found that 30% of consumers who changed their behavior due to fear of identity theft had reduced their overall use of the Internet (Princeton Survey Research 2005). Adaptive behaviors range from simple activities such as opting out of an email list, deciding not to provide certain information or avoiding the specific website, to more extreme measures such as filing an official complaint with a government agency.

FIGURE 1
CONCEPTUAL MODEL AND HYPOTHESIS
FOR ADAPTIVE AND MALADAPTIVE BEHAVIORS



This suggests four hypotheses to be tested in Study 1:

H1: Perceived online threat severity will have a:
- a. positive relationship with adaptive behavior
- b. positive relationship with maladaptive behavior

H2: Perceived threat probability will have a:
- a. positive relationship with adaptive behavior
- b. positive relationship with maladaptive behavior

H3: Internet Self-efficacy will have a:
- a. positive relationship with adaptive behavior
- b. negative relationship with maladaptive behavior

H4: Privacy Response Self-efficacy will have a:
- a. positive relationship with adaptive behavior
- b. negative relationship with maladaptive behavior

METHOD

A draft instrument was created using scales from previous literature to measure the constructs. In addition, new scale items were added where previous scales appeared to be lacking on coverage of the

domain. The final survey (see Appendix A) contained 38 items measuring the constructs of Internet self-efficacy, privacy response self-efficacy, threat severity and probability, and adaptive behavior and maladaptive behavior. Finally, given the noted heterogeneity in privacy behavior (Phelps, Nowak & Ferrell, 2000), demographic variables are also included as important covariates.

An online survey was sent to a pool of 2000 online consumers using a mailing list provided by a third party. Of the 2000, 482 respondents completed the full survey, 8 surveys were left out due to incomplete data. With the data gathered, individual constructs were tested for reliability using Cronbach's alpha (Cronbach, 1951) the reliability of all constructs were above .50 and are reported in Table 1. To check for possible response bias, early and late respondents were compared on demographic variables (Armstrong & Overton, 1977). No statistical significance was found.

Furthermore, reliability analysis was combined with discriminant and convergent validity analysis to eliminate items that had low item-item and item–scale correlation or increased alpha if deleted. There were none. Next, the relationships between the main constructs were examined using a Pearson product-moment correlation coefficient. Preliminary analyses were performed to ensure no violation of the assumptions of normality, linearity and homoscedasticity.

RESULTS

OLS regressions were used to test the four hypotheses. Multicollinearity was checked for each regression and all independent variables, an examination of the VIF statistics found no evidence of problematic multicollinearity in any regression. Furthermore, since interaction terms were included in the regression to test for moderating relationships, the continuous independent variables were mean centered (Aiken & West, 1991). The standardized beta coefficients were used to test the hypotheses. The overall regression model explaining adaptive behavior (model 1) was statistically significant ($p < .001$) with an adjusted R squared of .328. In addition, the overall model explaining maladaptive behavior (model 2) was statistically significant ($p < .001$) with an adjusted R squared of .362.

TABLE 1
REGRESSIONS RESULTS FOR ADAPTIVE AND MALADAPTIVE BEHAVIORS

	Model 1	Model 2
	Adaptive	Maladaptive
Internet Self-efficacy	.323***	-.282***
Threat Severity	.162***	.264***
Threat Probability	.084**	.235**
Privacy Response Self-efficacy	.212***	.118
Gender (Female)	-.062*	-.044*
Age	-.072	-.069
College Graduate	.054	.028
Income over $75K	.018	.024
Hours Spent Online excluding email	.039	.046
F value	9.8***	11.4***
Adjusted R-Square	.328	.362

*p<.10; **p<.05; *** p<.001

H1a, which states there is a positive relationship between adaptive behaviors and threat probability, was supported (B = .162, p < .001). H1b, which states there is a positive relationship between maladaptive behaviors and threat severity, is supported (B = .264, p< .001). For H2a, perceived threat probability had a positive significant relationship with adaptive behavior (B = .084, p < .05). For H2b, perceived threat severity had a positive significant relationship with maladaptive behaviors (B = .235, p < .001).

H3a, which states there is a positive relationship between Internet self-efficacy and adaptive behaviors, is supported (B = .323, p< .001). H3b, which states there is a negative relationship between Internet self-efficacy and maladaptive behavior, was supported (B = -.282, p< .001). For H4a, there was a positive significant relationship between Privacy Response Self-efficacy and Adaptive behaviors (B = .212, p < .001). For H4b, there was no significant relationship between Privacy Response Self-efficacy and maladaptive behavior. As suggested by Baron and Kenny (1986), to test for moderation effects, regressions were compared with and without the interaction terms of privacy response self-efficacy and Internet self-efficacy. While the overall model was found to be significant for both models, the interaction terms in both models were not significant.

DISCUSSION

Internet use by consumers has continued despite growing privacy concerns. Using hours online and website innovation as proxies for Internet self-efficacy, our results suggests that Internet self-efficacy within a protection motivation framework provides an explanation to this online innovation paradox. Through Internet self-efficacy, consumers are able to self-regulate their time spent on the Internet and engage in adaptive behaviors as a response to privacy threats. Internet self-efficacy provides confidence for consumers to shop online in the face of new, innovative technologies used by online marketplaces. In addition, Internet self-efficacious consumers are more likely to ask companies and watchdog groups for more education about changes in technologies and better control over personal information. However, Internet self-efficacy may have its limits as an effect on adaptive response depending on how consumers perceive risk that new Internet innovation poses to the public consumer. A 2005 survey found that due to new concerns about being confronted by technologies they don't understand on the web, a majority of consumers have stopped giving out personal information on the Internet, 30% say they have reduced their overall use of the Internet, and 25% say they stopped buying things online (Princeton Survey Research 2005). With this increasing demand by online consumers for anonymity to protect their privacy, public policy makers and marketers need to work together and take steps to understand this behavior in order to shift the mindset of the consumer from one of defensive and restrictive behavior to one where the user experience builds trust and increases Internet usage, as e-businesses continue to innovate and add new technologies and content to their consumers (Miyazaki & Fernandez, 2001). This could benefit the broader public of Internet users by building up a legitimization of innovative new technologies by validation from online consumers, watchdog groups, and e-business.

Privacy Response self-efficacy is effective for adaptive behaviors but not for maladaptive, suggesting they're being more proactive than reactive as they feel their privacy concerns are challenged. This distinction is important as it may provide additional understanding of the consumer dissonance, as (since?) many privacy concerns have been (stem from?) issues with consumers and online retailers. Nineteen percent of e-retailers reported some level of security breach within their last two years of business. Online consumers are making their voices heard; a study indicated that announcing an Internet security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on average, 2.1 percent of their market value within two days of the announcement resulting in an average loss of $1.65 billion in market capitalization per breach (Cavusoglu, Mishra, & Raghunathan, 2004).

IMPLICATIONS & FUTURE RESEARCH

Innovation on the web can provide consumers with much more valuable information and experiences. With the prevalence of web monitoring services (e.g. Aletra, Webmetrics), firms can also use this innovative technology to examine consumer behavior on the Internet. This enables firms to take a more proactive, rather than reactive stance, in situations that may have policy implications. When an issue arises firms are able to quickly see adaptive and maladaptive behaviors and can respond at Internet speed to mitigate the issue before it gains critical mass. Firms can respond much faster, and in a less expensive manner than they can by using traditional mass media.

More importantly, this paper highlights the opportunity and need for government regulators, consumer advocacy groups, and e-businesses to educate their consumers to become active and to have a fluid exchange of information that builds trust between a firm and consumer. Since the employment of new innovative information technology will only continue to increase (Ipsos Insight, 2005), firms that act now at implementing standards and guidelines will help build demand for other firms to follow similar guidelines during their design and technological innovations that consumers will begin to expect as norms. This will benefit firms, policy makers, and even government regulation in obtaining more accurate personal information in connection with online behavior, which will create a more accurate picture in which to make decisions. With an increase in Internet self-efficacy, consumers may feel less over-whelmed by innovations they do not recognize and may have more confidence to educate and adapt. Moreover, this may spur an increase in innovation by virtue of the fact that consumers are not avoiding new innovations or giving up in the face of them. From an e-consumer's point of view, it can be alarming at the lack of regulations on how new web innovations are deployed by firms to the average Internet shopper. Outside of some privacy issues, there is little control over how and when these innovations can be used, and more importantly, abused.

Although the current research supports this assumption, future research would benefit from additional measures aimed at the direct effect of Internet self-efficacy on online consumer behavior as well as a buffer against the online innovation environment. In addition, future research should investigate how consumers adapt their behavior based on their perception of risk of the innovation. Longitudinal data could be used to explore the reciprocal causality that may exist between Internet self-efficacy, innovation, and changes in e-consumer behavior.

REFERENCES

Aiken, L.S. & West, S.G. (1991). *Multiple Regression: Testing and Interpreting Interactions*, Thousand Oaks, CA: Sage Publications.

Armstrong, J.S., & Overton, T.S. (1977). Estimating Nonresponse Bias in Mail Surveys, *Journal of Marketing Research*, 14, 396-402.

Bandura, A. (1993). Perceived Self-Efficacy in Cognitive Development and Functioning, *Educational Psychologist*, 28, (2), 117-148.

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.

Bolin, S. (1998). E-Commerce: A Market Analysis and Prognostication, *Standard View*, 6, (3), 97-105.

Cavusoglu, H., Mishra, B., & Ragunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers Source, *International Journal of Electronic Commerce*, 9, (1), 70-144.

Clarke, R. (2001). Person Location and Person Tracking: Technologies, Risks and Policy Implications, *Information Technology and People*, 14, (2), 206-231.

Costello, S. (2001). Study: Surfers Balk at Providing Personal Data, *CNN.com*, August 15, available at: http://www.cnn.com/2001/TECH/internet/08/15/data.storing.rejected.idg/.

Cranor, L.F., Reagle, J., & Ackerman, M.S. (1999). Beyond Concern: Understanding about Online Privacy, AT&T Research (April 14, 1999). www.research.att.com/projects/privacystudy. Accessed November 20, 2005.

Cronbach, L.J. (1951) Coefficient Alpha and the Internal Structure of a Test, *Psychometrika,* 16, 297-334.

Culnan, M.J. & Bies, R.J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations, *Journal of Social Issues,* 59, (2), 323-343.

Eastin, M.S. & Larose, R. (2000). Internet Self-Efficacy and the Psychology of the Digital Divide, *Journal of Computer-Mediated Communication*, 6, (1), 83-104.

Goodwin, C. (1991). Privacy: Recognition of a Consumer Right, *Journal of Public Policy & Marketing*, 10, (Spring),149-66.

Hiller, J.S. & Cohen, R. (2002). *Internet Law and Policy,* Upper Saddle River, NJ: Prentice-Hall Inc.

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

Ipsos Insight, "Wireless Internet Access Climbs Nearly 30% in 2004," Press Release, Ipsos Insight Marketing Research Consultancy, 2004 (available at http://www.ipsos-insight.com).

Kehoe, C., Pitkow, J. & Morton, K. (1997). Eight WWW User Survey, (accessed March 7, 2000), Retrieved from http://www.cc.gatech.edu/gvu/user_surveys/survey-04-1997/

Keller, P.A. & Block, L.G. (1996). Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration, *Journal of Consumer Research*, 22, 448-59.

Lwin, M.O. & Williams, J. (2003). A Model Integrating the Multidimensional Development Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online, *Marketing Letters,* 14, 4 (December), 257-272.

Maguire, J. (2005, August 2). State of E-Commerce: Online Shopping Trends. Retrieved from http://www.ecommerce-guide.com/news/trends/article.php/3524581

Miyazaki, A.D. & Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping, *Journal of Consumer Affairs*, 35, (1), 27-45.

Nasir, V.A. (2004). E-Consumer Complaints About On-Line Stores, *Journal of Consumer Satisfaction, Dissatisfaction and Complaining*, 17, 68-88.

Nowak, G.J. and Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When Privacy Matters, *Journal of Direct Marketing*, 9, (Summer), 46-60.

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.

Princeton Survey Research Associates International (2005). *Leap of Faith: Using the Internet Despite the Dangers*, Washington, D.C., Retrieved from http://www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm. Accessed November 2, 2005.

Privacy and American Business, (2005). New Survey Reports an Increase in ID theft and Decrease in Consumer Confidence, Retrieved from http://www.pandab.org/deloitteidsurveypr.html. Accessed September 12, 2005.

Privacy Rights Clearinghouse, (2005, April 20). A Chronology of Data Breaches Reported Since the ChoicePoint Incident, Retrieved from http://www.privacyrights.org/ar/ChronDataBreaches.htm. Accessed November 10, 2005.

Rippetoe, P.A. & Rogers, R.W. (1987). Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat, *Journal of Personality and Social Psychology*, 52, (3), 596-604.

Rogers, R.W. (1983). Cognitive and Physiological Processes in Attitude Change: A Revised Theory of Protection Motivation, *Social Psychophysiology* (J. Cacioppo & R. Petty (Eds.), 153-76.

Saparito, B. (2005). Are Your Secrets Safe, *Time*, New York: Mar 7, 2005, 165, (10), 46-48.

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

Wang, P. & Petrison, L.A. (1993). Direct Marketing Activities and Personal Privacy: A Consumer Survey, *Journal of Direct Marketing,* 7, (1), 7-19.

Woon, I.M.J., Tan, G.W., & Low, R.T. (2005). Twenty-Sixth Conference on Information Systems.

APPENDIX A

SURVEY ITEMS

Construct	Items	Source
Internet Self Efficacy (alpha=.90)	• I feel confident understanding terms/words relating to Internet hardware. • I feel confident understanding terms/words relating to Internet software. • I feel confident describing functions of Internet hardware. • I feel confident trouble shooting Internet problems. • I feel confident explaining why a task will not run on the Internet. • I feel confident using the Internet to gather data. • I feel confident learning advanced skills within a specific Internet program. • I feel confident turning to an on-line discussion group if needed.	Eastin and Larose 2000

Privacy Response Self-Efficacy (alpha=.76)	• Requesting an online business to remove my name and address from any lists they use for marketing purposes. • Requesting an online business not to sell or give my name and address to another company. • Requesting that an online business reveal what personal information, besides billing information, they had about me in their customer records. • Refusing to give information to an online business because I thought it was not really needed or was too personal. • Deciding not to purchase something from an online business because I wasn't sure how they would use my personal information. • Filing an online complaint with a government agency about what I felt was a misuse of my personal data by an online business. • Deciding not to register at a website to get information or to shop there because I found their Privacy Policy too complicated or unclear.	Eastin and Larose 2000
Perceived Threat Severity (alpha=.91)	• I am concerned about having my identity stolen while online. • I am concerned about E-mail eavesdropping while online. • I am concerned about losing date privacy while online. • I am concerned about losing financial information while online.	Woon, Tan, Low 2005
Perceived Threat Probability (alpha= .91)	• How likely is it that one's identity can be stolen while online? • How likely is it for one's email conversations to be read by eavesdroppers while online? • How likely it is for one's privacy to be invaded while online? • How likely it is for one's financial information to be stolen while shopping online?	Woon, Tan, Low 2005
Maladaptive Behavior (alpha= .70)	• To avoid risk on the Internet I often avoid going online. • I often ignore the danger online and hope bad things don't happen. • I have little control of what happens online and accept this fact. • I feel hopeless about being able to protect myself online.	Adapted from Westin 2004 (yes/no)
Adaptive Behavior (alpha =.58)	In the last year I have: • Asked an online business to remove my name and address from any lists they use for marketing purposes. • Asked an online business not to sell or give my name and address to another company. • Asked an online business to see what personal information, besides billing information, they had about me in their customer records. • Refused to give information to an online business because I thought it was not really needed or was too personal. • Decided not to use or purchase something from an online business because I wasn't sure how they would use my personal information. • Filed a complaint with a government agency about what I felt was a misuse of my personal data by an online business. • Decided not to register at a website to get information or to shop there because I found their Privacy Policy too complicated or unclear.	Adapted from Westin 2004 (yes/no)