2008

Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online

Gaurav Bansal
University of Wisconsin - Milwaukee, gbansal@uwm.edu

Fatemeh "Miriam" Zahedi
University of Wisconsin - Milwaukee, zahedi@uwm.edu

David Gefen
Drexel University, gefend@drexel.edu

Recommended Citation

Bansal, Gaurav; Zahedi, Fatemeh "Miriam"; and Gefen, David, "Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online" (2008). *AMCIS 2008 Proceedings*. 178.
http://aisel.aisnet.org/amcis2008/178

Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online

Gaurav Bansal
University of Wisconsin – Milwaukee
gbansal@uwm.edu

Fatemeh "Mariam" Zahedi
University of Wisconsin – Milwaukee
Zahedi@uwm.edu

David Gefen
Drexel University
gefend@drexel.edu

ABSTRACT

Privacy policy statements and privacy-assurance cues are among the most important website features that online providers could use to alleviate web customers' privacy concerns. This study examines the moderating role of privacy concern on how privacy assurance cues and argument quality contribute to increased trust, and the subsequent decision to disclose health information online. This study has both theoretical and managerial contributions. The results provide insight about the dual roles of privacy policy statements, and privacy assurance and trust cues. The study highlights the differential impacts such mechanisms have on high privacy concerned and low privacy concerned web users in the context of disclosure of health information online.

KEYWORDS

Privacy Assurance Cues, Privacy Policy Statement Quality, Trust, ELM

INTRODUCTION

Evidence suggests that privacy of health information is a major concern for individuals (Bodenheimer et al. 2003; Westin 2003). Moreover, research shows that a trusted online environment results in an increased tendency by customers to disclose private information online (e.g., McKnight et al 2002; Malhotra 2004). Privacy policy and privacy-assurance cues are among the most important website features that online providers could use in creating such a trusted online environment and through it alleviating web customers' privacy concerns (Milne and Culnan 2002; 2004). Currently, the examination of the role of the online privacy policies in creating a trusted environment has been either limited to their mere presence (as a "trust cue"), or has been ignored in the literature (Milne and Culnan 2004). Such an investigation is of importance since privacy concern and the need for trust have been identified as major issues hampering the growth of web-based health care (Medical News Today 2006), Metzger (2006) notes with surprise that no studies have investigated the effects of privacy policy content variations on consumer attitudes and behavior. This paper poses the following research question: Does privacy concern moderate the effect of privacy policy statement "quality" and privacy assurance cues on enhancing trust in the context of disclosing private health information online?

The study utilizes the elaboration likelihood model (Petty and Cacioppo 1986) which states that people in the high elaboration likelihood state (high privacy concern in this case) are more likely to engage in thoughtful processing of an information message (privacy policy statement), and, therefore, should tend to be more persuaded by argument quality (privacy policy statement quality) than by peripheral cues (privacy assurance cues). In contrast, those in the low elaboration likelihood state (low privacy concern in this case), lacking the motivation to deliberate thoughtfully, should tend to be motivated by peripheral cues.

The study develops scales to measure privacy policy statement quality in terms of a second-order construct "adequacy" of the policy as well as its "understandability." Furthermore, we measure information quality as well as the website design quality, along with other privacy-assurance cues, including third party assurance and company information as peripheral cues. Trusting intentions and intention to disclose health information serve as dependent constructs. The research methodology is a controlled lab experiment with random assignment of context stimuli. The data analysis method is the structural equations modeling.

LITERATURE REVIEW

Milne and Culnan (2002) reported on the evolution of online privacy policy statements posted by US companies and argue that both the contents (related to fair usage of information—adequacy of privacy policy statement) and format (understandability) of the privacy policy are important in creating a trusting environment (Milne and Culnan 2002). However, these privacy policy statements vary in terms of their placement, length, ease of reading, and the level of guaranteed protection (Liu et al. 2002). Furthermore, not all people are equally influenced by the "quality" of such statements. Moreover, Milne and Culnan (2002) observed that experience with the company, reputation of the company and presence of privacy seals could serve as alternatives to privacy notices. This is supported by Benasi (1999), who has argued that displaying seals of approval may add trustworthiness and credibility to corporate website, hence suggesting that the company is willing to have its privacy practices audited. However, recent studies note that privacy seals are no guarantee that websites do not infringe upon user privacy (e.g., Pollach 2006).

OVERARCHING THEORY: THE ELABORATION LIKELIHOOD MODEL (ELM)

Cognitive energy spent on processing a message may vary among individuals in different contexts (Petty et al 1986). The variations in cognitive elaboration, *ceteris paribus*, may affect the extent of a message's influence. According to Petty and Cacioppo (1986), elaborating on a message requires ability and motivation. The elaboration likelihood model (ELM) suggests that when elaboration is high, the recipient experiences a central route of persuasion, but when elaboration is low, the recipient experiences a peripheral route (Petty et al. 1986). When elaboration is low, influence typically acts through very simple decision criteria and cues such as design, endorsements, and attractiveness. Individuals use these cues either because they are not deeply involved in the issue, are not motivated enough to do so, or don't have sufficient knowledge about the subject matter. They do not devote the necessary cognitive energy or find themselves unable to expend the effort (Petty et al. 1986). It has also been noted that non-experts rely less on argument quality and instead focus on peripheral cues such as design and source credibility (Petty et al. 1981). "Internet shoppers, especially those who perceive a high risk associated with online transactions may proactively search for and carefully examine an e-tailer's privacy practices to alleviate their concerns about the privacy of their information" (Pan et al. 2006 p.332).

RESEARCH MODEL

The conceptual model is reported in Figure 1 and discussed below.

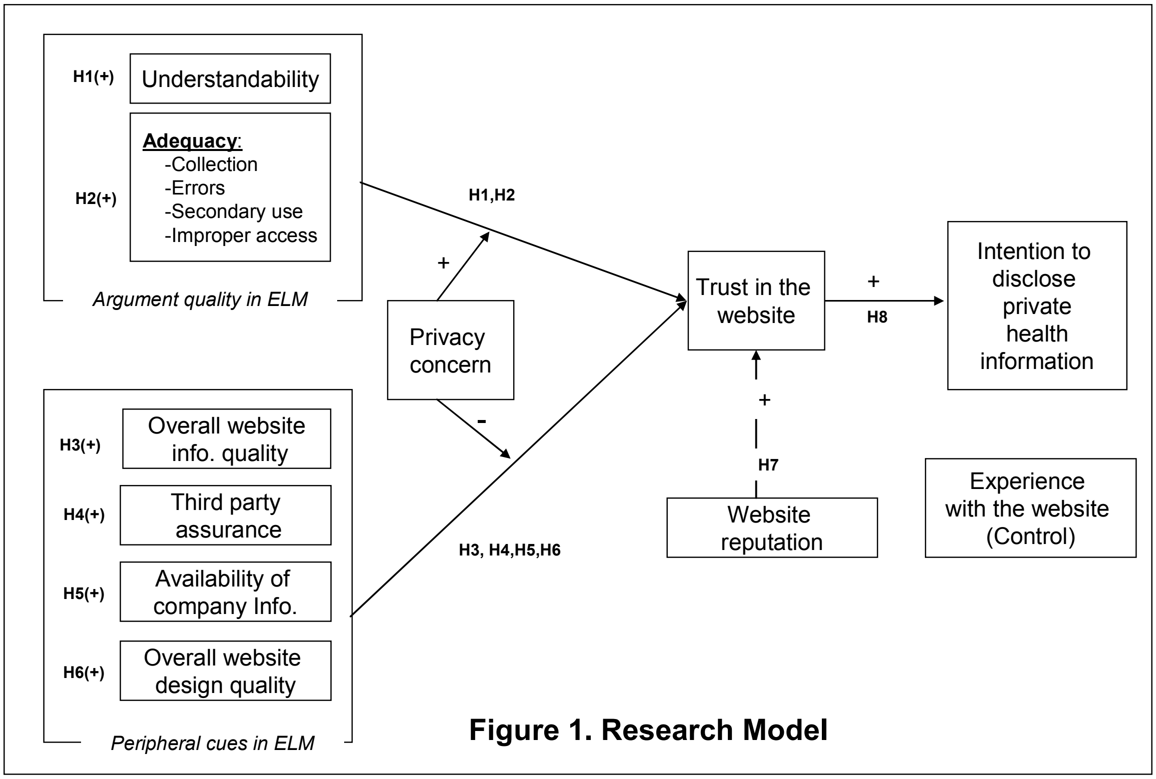

Figure 1. Research Model

Argument Quality (AQ)

Perceived Privacy Policy Understandability

The role of understandability of privacy-policy statements in increasing trust is an important and understudied issue. Pan et al. (2006) argue that a clearly stated privacy disclosure may be useful in alleviating privacy-related concerns. In turn, such a privacy policy may be expected to result in lower perceived risk (Miyazaki et al. 2000), and more trust in the store's fair information practices. Plain language should contribute to building the trust in the vendor by reinforcing the notion that the web vendor is forthcoming and hence would be reliable.

In various legal studies (e.g., Kimble 1994-1995), it has been argued that plain language improves comprehension, whereas traditional style (i.e., legalese) does not communicate as well and may produce unnecessary confusion. Pan et al. (2006) argued that straightforward privacy policy will result in more consumer trust in an online store than a long legalistic policy.

Even though it is known that readability of such statements might be associated with trust, studies have found that websites are posting rather lengthy and incomprehensible privacy policy statements. Analyzing 40 online privacy policy statements, Westin (2004) has reported that average educational level of 14.1 years of schooling are needed to read the policies. 49% of US adult population has no college education (March 2000 US Census data). Similarly, Milne et al. (2006) reported that during the time period of their study (2001 – 2003), readability of privacy policy statements actually went down.

Research from notices and labels literature (Szykman et al. 1997) suggests that highly involved people read the food notices and labels more carefully than less concerned individuals. Similarly, it could be argued that individuals with high privacy concern (PC) would read the privacy policy statements more thoroughly and then make an informed decision. The argument has support in ELM, which suggests that it is the highly involved as opposed to low involved people who will be influenced via central route or argument quality (understandability of the privacy policy statement). In other words, PC should moderate the influence of understandability of privacy policy.

Hypothesis 1. For individuals with high privacy concern (and not for those with low privacy concern), perceived understandability of the privacy policy statement is associated with trust in the website.

Perceived Adequacy of Privacy Policy Statement

Even though it is suggested (Earp et al. 2003) that the mere presence of a privacy policy statement builds trust, Earp et al. (2005), on the basis of their study of 50 websites and survey of over 1000 internet users, suggested that discrepancy exists between users' expectations and what privacy policies state. Other studies that examined the compliance of privacy policy statements with Federal Trade Commission's (FTC) fair information principles (FIP) concluded that there are many grave discrepancies. For instance, Adkinson et al. (2002) reported that only 60% notified visitors about the type of private information collected, fewer than half provided a choice about the use of information, and slightly more than half provided information about steps taken to provide security. Similarly, Peslak (2006) reported "limited compliance" with FIP principles (Peslak 2006). A study of the Fortune E-50 found that only two of the top 50 e-companies fully complied with the four FTC FIPs. Access and Security FIP had the largest degrees of non-compliance (Ryker et al. 2002).

Absolute compliance with FIPs is important but is a rather elusive target. Hence, this study focuses on the perceived adequacy of such statements, and argues that it should be important in determining trust intentions. This is somewhat supported by Meinert et al. (2006) who observed that willingness to provide information increases as the level of privacy guaranteed by the statements increases. Also Milne and Boza (1999) have argued that privacy notices that are perceived to be informative and reassuring that disclosing personal information is not risky, build trust in the website.

Based on FTC (2000) fair Information Practices in the Electronic Marketplace Report to Congress, Miyazaki and Krishnamurthy (2002 p. 35) noted that "common practice suggests that there are four fair information practice principles" namely: notice, choice, access, and security. These are the privacy policy guidelines which corporations should adhere to as part of their fair information practices.

Unrelated to this, Smith et al. (1996) have developed and validated a scale to measure privacy concerns. They argued that privacy concerns is a second order construct comprising of concerns related to collection, unauthorized secondary use, errors and unauthorized access. Table 1 (below) juxtaposes the FTC's principles and Smith et al.'s constructs and demonstrates that both documents support the same underlying definitions.

Smith et al. 1996	FTC 2000
Collection	**Notice:** Data collectors must disclose their information practices collecting personal information from consumers.
Unauthorized Secondary use (internal and external)	**Choice:** Consumers must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided.
Errors	**Access:** Consumers should be able to view and contest the accuracy and completeness of data collected about them.
Unauthorized access	**Security:** Data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

Table 1. Privacy Concerns and Fair Information Practices Principles

Based on this overlap, we thus define privacy policy statement adequacy as a second order construct, comprising of perception of the Web users that the website (via privacy policy statement) is demonstrating adequate measures to handle their information privacy concerns related to collection, unauthorized secondary use, errors, and unauthorized access. Based on the ELM, individuals with high PC should be influenced by the adequacy of the privacy policy statement.

Hypothesis 2. For individuals with high privacy concern (and not for those with low privacy concern), perceived adequacy of the privacy policy statement is associated with trust in the website.

Peripheral Cues

Perceived Website Information Quality. The study by Nicolaou et al. (2006 p.335) demonstrated that users' "cognitive beliefs about the favorable or unfavorable characteristics of the currency, accuracy, completeness, relevance, and reliability" of the information during an exchange session can help build trusting beliefs. Since low PC individuals look for cues to deduce the quality of a website's privacy-policy statement, they are more likely to rely on the contents of websites for which they have to expend cognitive energy anyways. Hence, information quality is a strong cue for judging a website's privacy policy.

Hypothesis 3. For individuals with low privacy concern, perceived website information quality is associated with trust in the website.

Other Cues. Trust seals like BBBOnline™ and TRUSTe™ increase consumer perceptions of a site's trustworthiness through transference. Research (Consumers International 2002) has found that website presentation quality (design quality) and availability of the contact details of the physical entity behind the website are associated with trust in the website. Web users rely on design quality of the website to ascertain the degree of trust they can assign to the website. High design quality lowers risk beliefs associated with the website, and hence enhance the degree of trust. Users who lack the necessary motivation to delve deeper use such cues to quickly make an impression about the trustworthiness of the site. This is in line with the ELM. The individuals with low PC are in a low elaboration state and rely on these peripheral cues for trust formation or enhancement.

Hypothesis 4. For the low PC individuals, perceived presence of third party endorsements is associated with trust in the website.

Hypothesis 5. For the low PC individuals, perceived presence of company information is associated with trust in the website.

Hypothesis 6. For the low PC individuals, perceived website design quality is associated with trust in the website.

Website Reputation

The ELM considers source credibility as a peripheral cue, and one could argue that reputation is equivalent to source credibility. However, reputation, particularly in the online environment, is far more important and universal variable than a peripheral cue. Reputation is the collective social knowledge about the trustworthiness of a website. It is often defined "in terms of the perception of a company's honesty with and concern towards its customers" (Metzger 2006 p. 157). Chiles et al. (1996) argued that reputation fosters the belief that a seller will act in the interest of the consumer. In the case of health infomediaries, Song and Zahedi (2007) have reported significant relationship between trust and reputation. Empirical research by Jarvenpaa et al. (1999, 2000), and Teo et al. (2007) similarly suggest that seller's reputation is an important characteristic that influences buyers' trust.

Hypothesis 8. Reputation of a website is positively associated with trust on the website.

Trust

Trust is the expectation that other individuals or companies with whom one interacts will not take undue advantage of a dependence upon them. It is the belief that the trusted party will behave in an appropriate manner and will fulfill their expected commitments (Luhmann 1979). Perceptions that the vendor is reliable encourage consumers to provide personal information to it (Dinev and Hart 2006, McKnight et al. 2002). Research shows that trust reduces perceived risk (Gefen et al. 2003), and hence provides the necessary comfort to the web user in disclosing one's information online. Hence we argue that,

Hypothesis 9. Trust in a website is associated with intention to disclose private health information.

Operationalization of Variables

To ensure construct validity we used items from existing scales wherever possible. The items measurement was semantic differential (0-10), to minimize common method bias. Table 2 shows the sources of items for each construct.

Construct	Reference
Perceived overall website information quality	Nikolaou and McKnight, ISR 2006
Understandability of the Privacy Policy Statement	Self developed
Privacy Policy Adequacy (Collection, Errors, Secondary Use, Improper Access)	Adapted from Smith et al. 1996, FTC(2000)
Perceived Presence of third party assurances	Self developed
Availability of company information	Self developed
Perceived overall website design quality	Self developed
Trust	Gefen et al. 2003
Prior positive experience with the website	Song and Zahedi 2007
Intention to disclose health information	Malhotra et al. 2004
Health information privacy concern	Malhotra et al. 2004

Table 2. Operationalization of Variables

METHODOLOGY

Study Design

The model was tested using a controlled lab experiment with online access. The protocol contained three different health websites. The three websites ranged in their degree of trust and reputation. Participants were students in a large Midwestern University. They were randomly assigned to view one of the three websites. After viewing the website, the participants were first asked to answer a set of questions about the contents of the website to ensure that they had examined the website and were then required to respond to the instrument. A total of 674 observations were collected.

To examine the moderating effect of privacy concerns we divided the data set into two based on the privacy concerns of the individuals. To decide upon the privacy concern level of the participants, we used the privacy concern items and created a single factor. Respondents with positive factor scores were categorized as high PC and those with negative factor scores as low PC. There were 316 respondents in the high PC dataset as opposed to 359 in the low PC one. The demographics for the two data sets are given in table 3 (below). We separately analyzed the two datasets and the results are shown in figure 2 and 3.

High PC dataset			Low PC dataset		
# Female	# Male	Average Age	# Female	# Male	Average Age
215	101	19.67	184	175	20.57

Table 3. Demographics

ANALYSIS AND RESULTS

Data Analysis

Data analysis was carried out in multiple steps. First we conducted the exploratory factor analysis (EFA) to examine the discriminant validity of the model in each context. No cross-loadings above 0.40 were observed and all the items loaded together into the intended factor, supporting the discriminant validity of the proposed constructs. We examined the reliability of the measures, known to be of critical importance. The Cronbach Alpha values were analyzed separately for the two datasets and are greater than 0.738, well above the suggested cut off point of 0.70.

Indices	High PC		Low PC		Specifications
	Measurement Model	Estimation Model	Measurement Model	Estimation Model	
Normed	1.485	1.486	1.544	1.553	<3.00 or <5.00
SRMR	.053	.055	.053	.056	<0.100
RMSEA	.039	.039	.039	.039	<0.060
CFI	.954	.953	.954	.952	>0.90
TLI	.950	.950	.950	.948	>0.90

Table 4. Fit Indices

In order to control for common method variance, we used past prior experience as a control variable. We also estimated the measurement model. Factor loadings coefficients for all items were high, and the t-values were well above the 2.54 threshold (ranging from 10.01 to 47.97), supporting the statistical significance of factor loadings.

The fit indices for the measurement and estimation models are reported in Table 4. Most fit indices for the measurement model are desirably within their respected thresholds, providing further support for the model fit. Next, the data were analyzed with a structural equations modeling approach using MPlus 4.1 (Muthén and Muthén 2007). Estimated models are reported in Figure 2 and 3.

Results

The results are shown in Figures 2 and 3. Figure 2 shows the results for high PC individuals and figure 3 shows the results for low PC individuals. Hypothesis H1 is supported. Understandability of the privacy policy statements leads to trust only in the case of individuals with high PC (Figure 2) and not in the case of low PC individuals (Figure 3). Adequacy of privacy policy statements (H2) increases trust, in both high PC individuals (Figure 2), supporting arguments from ELM, and, contrary to the hypothesis, also in low PC individuals (Figure 3).

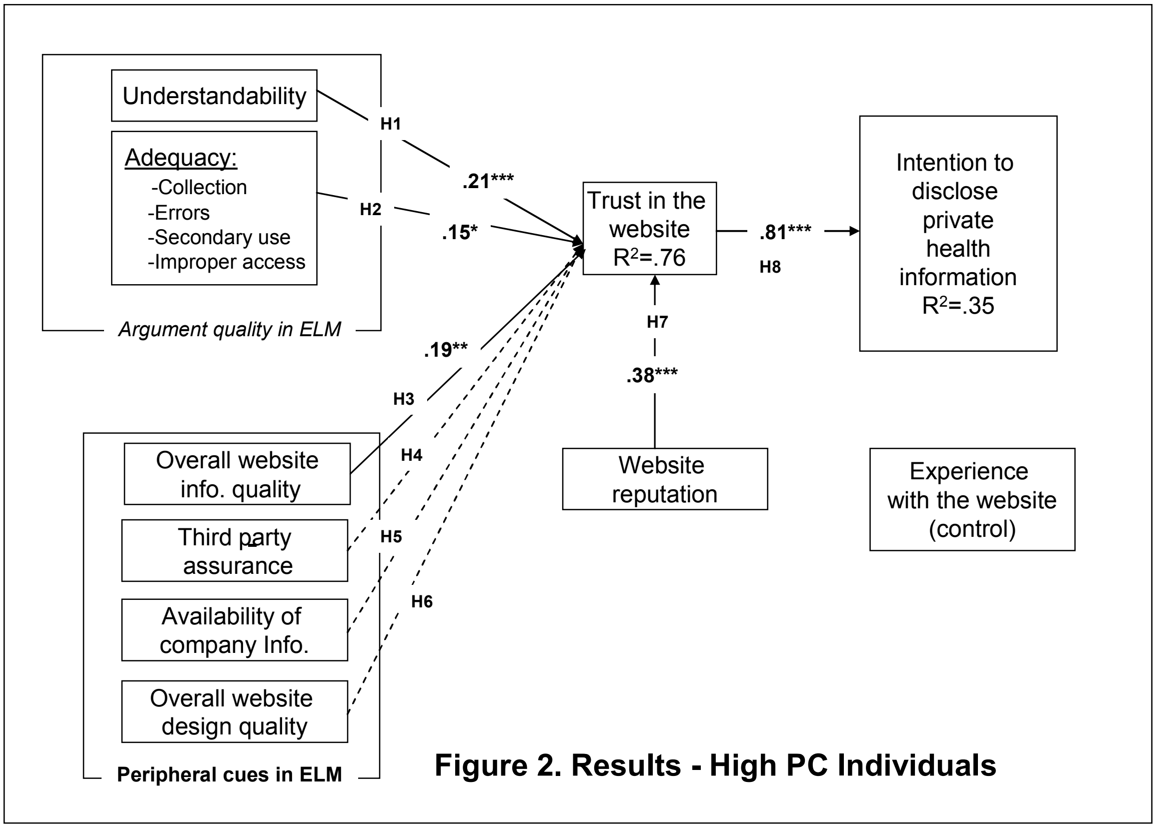
Understandability
Adequacy:
-Collection
-Errors
-Secondary use
-Improper access
Argument quality in ELM
H1
.21***
H2
.15*
Trust in the website R^2=.76
.81***
H8
Intention to disclose private health information R^2=.35
H7
.38***
Website reputation
Experience with the website (control)
.19**
H3
H4
H5
H6
Overall website info. quality
Third party assurance
Availability of company Info.
Overall website design quality
Peripheral cues in ELM

Figure 2. Results - High PC Individuals

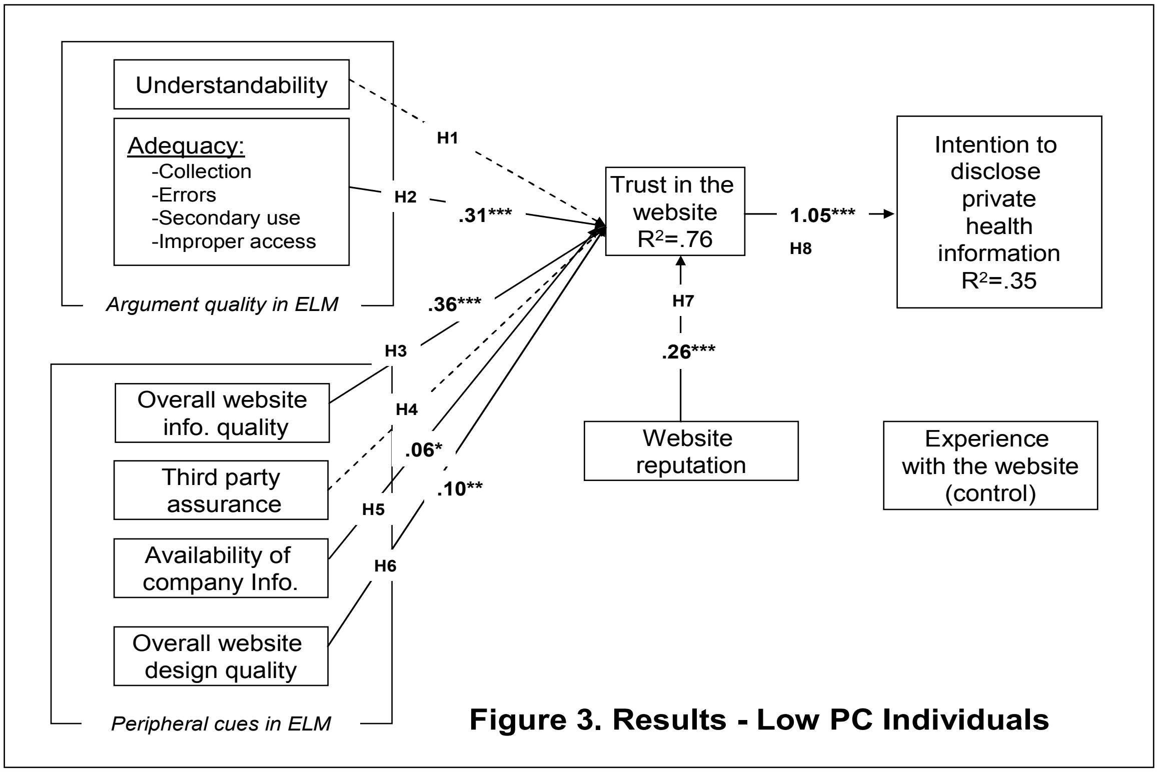
Understandability
Adequacy:
-Collection
-Errors
-Secondary use
-Improper access
Argument quality in ELM
H1
H2
.31***
Trust in the website R^2=.76
1.05***
H8
Intention to disclose private health information R^2=.35
H7
.26***
.36***
H3
H4
.06*
.10**
H5
H6
Website reputation
Experience with the website (control)
Overall website info. quality
Third party assurance
Availability of company Info.
Overall website design quality
Peripheral cues in ELM

Figure 3. Results - Low PC Individuals

The argument that peripheral cues increase trusting intentions in the case of low PC individuals was supported. The impact of perceived overall website information quality (H3) is significant and higher for low PC individuals. Third party endorsements did not increase trust in high PC individuals, as hypothesized. However, they did not lead to increased trust in low PC individuals either. H5 and H6 are significant for low PC individuals (Figure 3) and not significant for high PC individuals (Figure 2), hence supporting H5 and H6 as hypothesized. Website reputation was associated with trust in both high PC (Figure 2) and low PC (Figure 3) individuals, supporting H7. The relationship between trust and intention to disclose is direct and positive for both the cases (Figure 2 and Figure 3), supporting H8.

DISCUSSION

Previous research showed that privacy policy statements impact trust in a website and lead to intention to disclose private information. Previous research, however, did not deal with the dynamics of the influence process, and is therefore of somewhat limited assistance in unraveling the complexities of influence patterns and effects. This study addresses some of this gap in the privacy / trust literatures by elaborating on two alternating means of influence (central route and peripheral route), explaining which influence process is most effective, and presents a theoretical model that can serve as the basis for further explanation of the role of cognition in trust and the intention to disclose.

The results of this study show distinct behavioral differences among individuals with high as opposed to those with low privacy concern in forming their trust to disclose private health information. This adds to the trust literature by highlighting the influence of privacy concern as a significant personal factor. On a managerial level the study raises the need for web designers to consider the importance of the understandability and adequacy of their privacy policy statements in promoting trust of individuals with high privacy concern. This work shows that understandability is a major central route on which managers need to focus in creating their health privacy policies. Furthermore, website managers should include adequate information about how they collect data, provide visitors with the option about the use of disclosed by internal or external entities, how errors are handled, and the security measures to protect disclosed personal information. Such statements should be clear and understandable in order to have trust-enhancing influence for individuals with high privacy concern.

Our results reveal that for individuals with low privacy concern, trust cues plays a role in increasing their trust, particularly information quality, availability of company information and the quality of system design. The results indicate that privacy statements are understood within the general structure of the website information quality and website design. This is particularly important for health websites, for which the quality of health information plays a critical role for their legitimacy.

Furthermore, among individuals with low privacy concern, policy statement adequacy also influences trust in a higher degree. This latter finding is in apparent contrast with the ELM. Nonetheless, in comparing the influence of reputation on trust for high vs. low concern individuals, reputation has a far higher impact on trust for high PC individuals than those with low PC. It seems that high and low PC individuals have two different strategies for their trust formation in disclosing their private health information. The high PC individuals strongly rely on reputation (outside the website contents) and use the central route of understandability and adequacy as secondary sources for trust building. On the other hand, individuals with low PC rely heavily on the contents of the website and use the central and peripheral routes in their trust formation, and less on sources external to the website contents (reputation). This observation of differences in trust formation strategies depending on the level of PC adds another dimension to the ELM distinction of central and peripheral routes, namely internal and external routes.

This work has both theoretical and managerial contributions. The study highlights the differential impact such mechanisms have on high privacy concerned and low privacy concerned web users in the context of disclosure of health information online. Theoretically our findings show that there is an external route, reputation in this case, on which web users rely on. The results show that reputation plays a central route for individuals with high PC. This finding provides a basis for extending the ELM by adding the source of the route as internal and external. The managerial contribution of this result is in alerting website managers to the importance of providing information, links, testimonials and other sources that testify to the extent of websites' reputation.

Another interesting finding in this study is the lack of support for third party seals in both high and low PC cases for disclosing health information. It raises the question about the reason for such a definitive lack of support. Is it because there are no universally recognizable third parties whose assurance could be of any guarantee for protecting personal health information? Or, are third party assurances of little value regardless of the status of assurance providers?

Limitations

The study has limited generalizability since the participants were college students living in the Midwest. All items were self reported, including the intention to disclose. The study should be examined in other contexts as well, since context could impact the users' behavior (Bansal et al. 2008, Johns 2006). Moreover, this study should be repeated with samples drawn form other population types, including older or less educated individuals.

Conclusions

While information systems researchers have made substantial progress in examining behavioral aspects related with trust and technology adoption, little has been done to examine privacy concern, intention to disclose private information and the role of privacy policy statements. As the reliance on the Internet for collecting health information increases, we will need a deeper understanding of what makes people trust websites enough to disclose their private health information. Our study makes a contribution in this direction.

REFERENCES

Adkinson, W., Eisenrach, J. and Lenard, T. (2002) Privacy online: A report of the information practices and policies of commercial web sites, retrieved from http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf [last accessed July 15, 2007]

Bansal, G., Zahedi, F.M. and Gefen, D. (2008) Context and personality do matter: trust and privacy concern in disclosing sensitive information online, working paper, *University of Wisconsin – Milwaukee*.

Benassi, P. (1999) TRUSTe: An online privacy seal program, *Communications of the ACM*, 42, 2, 56-59.

Bodenheimer, T. and Grumbach, K. (2003) Electronic technology: A spark to revitalize primary care?, *Journal of the American Medical Association*, 290, 2, 259-264.

Chiles, T.H. and McMackin, J.F. (1996) Integrating variable risk preferences, trust, and transaction cost economics, *Academy of Management Review*, 21, 1, 73-99.

Consumers International (2002) *Credibility on the Web* (ISBN: 1-902391-39-X).

Dinev, T. and Hart, P. (2006) An extended privacy calculus model for e-commerce transaction, *Information Systems Research*, 17, 1, 61-80.

Earp, J.B., Anton, A.I., Aiman-Smith, L and Stufflebeam, W. H. (2005) Examining Internet privacy policies within the context of user privacy values, *IEEE Transactions of Engineering Management*, 52, 2, 227-237.

Earp, J.B. and Baumer, D. (2003) Innovative web use to learn about user behavior and online privacy, *Communications of ACM*, 46, 4, 81-83.

Federal Trade Commission (2000) Privacy online: Fair information practices in the electronic marketplace: A report to the Congress, Retrieved from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [last accessed April 27, 2008]

Gefen, D., Karahanna, E. and Straub, D.W. (2003) Trust and TAM in online shopping: An integrated model, *MIS Quarterly*, 27, 1, 51-90.

Hui, K-L., Teo, H.H. and Lee, S.T. (2007) The value of privacy assurance: An exploratory field experiment, *MIS Quarterly*, 31, 1, 19-33.

Jarvenpaa, S.L., Tractinsky, N. and Vitale, M. (2000) Consumer trust in an Internet store, *Information Technology Management*, 1, 45-71.

Jarvenpaa, S.,L., Tractinsky, N., Saarinen, L. and Vitale, M. (1999) Consumer trust in an Internet store: A cross-cultural validation, *Journal of Computer Mediated Communications,* 5, 2, 44-71.

Johns, G. (2006) The essential impact of context on organizational behavior, *Academy of Management Review,* 31, 2, 386-408.

Kimble, J. (1994–1995) Answering the critics of plain language, *Scribes Journal of Legal Writing*, 51.

Liu, C. and Arnett, K. (2002) An Examination of Privacy Policies in Fortune 500 Web Sites, *Mid-American Journal of Business*, 17, 1, 13-22.

Luhmann, N. (1979) *Trust and Power*, John Wiley and Sons, London, U.K.

Malhotra, N.K., Kim, S.S. and 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. and Schoorman, F.D. (1995) An integration model of organizational trust, *The Academy of Management Review*, 20, 3, 709-735.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. (1998) Initial trust formation in new organizational relationships, *Academy of Management Review*, 23, 3, 473-490.

McKnight, D.H., Choudhury, V. and Kacmar, C. (2002) Developing and validating trust measures for e-commerce: An integrative typology, *Information Systems Research*, 13, 3, 334-359.

Medical News Today (2006) Health Care IT Implementation Delayed by Privacy Concerns,, retrieved from http://www.medicalnewstoday.com/medicalnews.php?newsid=58143 [last accessed Mar 12, 2007].

Meinert, D.B., Peterson, D.K., Criswell, J.R. and Crossland, M.D. (2006) Privacy policy statements and consumer willingness to provide personal information, *Journal of Electronic Commerce in Organizations,* 4, 1, 1-17.

Metzger, M.J. (2006) Effects of site, vendor, and consumer characteristics on web site trust and disclosure, *Communication Research*, 33, 3, 155.

Milne, G.R. and Boza, M. (1999) Trust and concern in consumers' perception of marketing information management practices, *Journal of Interactive Marketing,* 13, 1, 5-24.

Milne, G.R. and Culnan, M.J. (2002) Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 U.S. Web Surveys, *The Information Society,* 18, 5, 345-360.

Milne, G.R. and Culnan, M.J. (2004) Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices, *Journal of Interactive Marketing,* 18, 3, 15-29.

Milne, G.R., Culnan, M.J. and Greene, H. (2006) A longitudinal assessment of online privacy notice readability, *American Marketing Association*, 25, 2, 238-249.

Miyazaki, A.D. and Fernandez, A. (2000) Internet privacy and security: An examination of online retailer disclosures, *Journal of Public Policy & Marketing*, 19, 1, 2000, 54-61.

Miyazaki, A.D. and Krishnamurthy, S. (2002) Internet seals of approval: effects of online privacy policies and consumer perceptions, *The Journal of Consumer Affairs*, 36, 1, 28-49.

Muthén, L.K. and Muthén, B.O. (2007) *Mplus Statistical Analysis with Latent Variables* (Version 4.1), Muthén & Muthén, Los Angeles, CA.

Nicolaou, A. and McKnight, D.H. (2006) Perceived information quality in data exchanges: effects on risk, trust, and intention to use, *Information Systems Research,* 17, 4, 21.

Pan, Y. and Zinkhan, G.M. (2006) Exploring the impact of online privacy disclosure on consumer trust, *Journal of Retailing* (82:4), 2006, p. 331.

Peslak, A.R (2006) Internet privacy policies of the largest international companies, *Journal of Electronic Commerce in Organization*, 46-62.

Petty, R.E. and Cacioppo, J.T. (1986) *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*Springer-Verlag, New York.

Petty, R.E., Cacioppo, J.T. and Goldman, R. (1981) Personal involvement as a determinant of argument-based persuasion, *Journal of Personality and Social Psychology,* 41, 5, 847-855.

Pollach, I. (2006) Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions, *Journal of Organizational and End User Computing*, 18, 1, 23-49.

Ryker, R., Lafleur, E., McManis, B. and Cox, K.C. (2002) Online privacy policies: An assessment of the Fortune E-50, *The Journal of Computer Information Systems*, 42, 4, 15-20.

Song, J. and Zahedi, F.M. (2007) Trust in health infomediaries, *Decision Support Systems*, 43*,* 2007, 390-407.

Teo, T.S.H. and Liu, J. (2007) Consumer trust in e-Commerce in the United States, Singapore and China*, Omega*, 35, 1, 22.

Smith, J.H., Milberg, S.J. and Burke, S.J. (1996) Information privacy: Measuring individuals' concerns about organizational practices, *MIS Quarterly*, 20, 2, 167-196.

Szykman, L.R., Bloom, P.N. and Levy, A.S. (1997) A proposed model of the use of package claims and nutrition labels, *Journal of Public Policy and Marketing*, 16, 2, 228-241.

Westin, A.F. (2004) How to craft effective online privacy policies, *Privacy and American Business*, 11, 6, 1-2.

Westin, A.F. (2003) Social and Political Dimensions of Privacy, *Journal of Social Issues*, 59, 2, 431-453.