Consumers’ privacy concerns and willingness to provide marketing-related personal information online
Changi Nam, Information and Communications University
Chanho Song, Information and Communications University
Euehun Lee, Chan Ik Park, Information and Communications University

Consumers’ privacy concerns and willingness to provide marketing-related personal information online have been utilized for the purpose of targeted marketing. However, Internet users are generally reluctant to provide personal information, being concerned about the potential for its illegal and unethical use; these concerns have been reinforced by media scrutiny on the issue. To relieve the concern, trust relationship needs to be developed between businesses and customers. This study proposed and empirically tested a model that incorporates three antecedents and their impact on customers’ willingness to disclose their personal information through a mediator, perceived privacy concerns. Implications for businesses and policy makers are presented.

[to cite]:

[url]:
http://www.acrwebsite.org/volumes/12442/volumes/v33/NA-33

[copyright notice]:
This work is copyrighted by The Association for Consumer Research. For permission to copy or use this work in whole or in part, please contact the Copyright Clearance Center at http://www.copyright.com/.
INTRODUCTION

The Internet has triggered revolutionary changes in our lives. People consider it to be a reliable source of information on products and services (Gervey and Lin, 2000). However, the use of the Internet for consumer purchasing has not been growing as fast as its other uses as an information source. One explanation for this disparity in growth rates may be consumers’ reluctance to provide personal information on the Internet. For example, Ernst and Young’s survey (1999) indicated that the most important reason why consumers do not make purchases on the Internet is their concern about sending out credit card information. A survey showed that only 24.9% of consumers felt comfortable using their credit card for purchasing on the Internet (Graeff and Harmon 2002). Media scrutiny of Internet fraud, hacking, and identity theft has heightened people’s awareness of the risks of conducting transactions on the Internet.

While Internet marketing is perceived as either a threat or a nuisance by many consumers, it is a valuable tool for both online and offline businesses. Rapid advances in information technology and the increase of Internet use enable companies to gather, store, and exchange consumer data that can be used for developing more accurately targeted marketing. A typical Internet marketing strategy focuses on a long-term relationship and a series of business transactions with a customer. This strategy becomes possible through the collection of data on customers’ buying patterns, preferences, and personal information. These databases, however, require consumers to share their personal information, whether voluntarily or involuntarily. In most cases, the nature of e-commerce requires consumers to disclose a certain amount of personal information (e.g., their name, address, and telephone number) and payment information (e.g., their credit card number). The problem is that consumers have generally shown increasing concerns over privacy due to an increase in questionable and illegal activities in the Internet, such as the precipitous rise of junk mail, identity theft, and fraud. Thus, issues of privacy and security in e-commerce have been receiving more attention by researchers in different fields (e.g., Caudill and Murphy 2000; Culnan and Armstrong 1999). Consumers’ growing concern over their privacy is a significant problem for the potential growth of e-businesses. According to a survey of Internet marketers, 92% believe that greater consumer confidence of online privacy would lead to an increase in online purchasing (Javis 2000).

A crucial question is what makes consumers voluntarily share their personal information with businesses. The present paper proposes and empirically tests a model of how individuals’ willingness to share personal information is determined. More specifically, this paper examines relationships between three factors related to consumers’ privacy concerns and one dependent variable: consumers’ willingness to disclose personal information.

LITERATURE REVIEW AND RESEARCH MODEL

Privacy concerns in the Internet era

Privacy is often understood as the right to be left alone (Cheskin Research and Studio Archetype/Sapient 1999). The invasion of privacy on the Internet is commonly regarded as the unauthorized collection, disclosure, or other use of personal information (Wang, Lee, and Wang 1998). Even before the Internet era, consumers’ personal information was often collected, analyzed, and exchanged for various marketing purposes such as direct marketing and telemarketing. However, pre-electronic consumer transactions provided a natural protection of consumer privacy, particularly where transactions were made in cash and consumers refused to release personal information. Since then, Internet commerce has eroded the benefits of such anonymity (Caudill and Murphy 2000). In fact, Internet has facilitated collection, process, and exchange of personal data in both speed and scope. Now, some commentators argue that it is almost impossible for consumers to transact businesses on the Internet without revealing information about themselves (Rust, Kannan, and Peng 2002). This also caused increased attention to the issue of consumer privacy showing dramatic increase in mass media coverage of the topic in all media formats between 1990 and 2001 (Roznowski 2003). It identified retailers as the most prevalent problem source.

Due to the nature of Internet-based business transactions, one of the major research trends in online marketing or e-commerce has been consumers’ concern about their privacy. In a telephone survey, only 24.9 percent responded that they were comfortable using their credit card to make purchases on the Internet (Graeff and Harmon 2002). According to an October 2001 report by Forrester Research, about 60 percent of online users are wary of giving out personal information online, inhibiting roughly $15 billion of potential e-commerce revenue in 2001 (Kelley, Denton, and Broadbent 2001). Privacy concerns regarding Internet marketing are not limited to the better known cases of junk-mailing and illicit cookie distribution, but to the selling of consumer databases for direct marketing purposes. Thus, Rust et al. (2002) even argued that the Internet will inevitably cause individual privacy to disappear, and that a specialized market for privacy will emerge. In other words, consumers may have to pay for a certain degree of comparative privacy in the future, but the underlying degree of privacy will continue to be eroded.

In the light of the perceived and actual erosion of consumer privacy, one comprehensive study examined four groups of input factors: types of personal information, the amount of control that consumers were given over how the information is used, the potential consequences for and benefits to consumers, and the consumer characteristics associated with overall privacy concerns, and found that 45 percent of people were very concerned about the way in which their personal information is used by companies, and most respondents wanted more control over the gathering and use of their personal information (Phelps, Nowak, and Ferrel 2000). Another study focused on procedural justice and found that fair procedures to protect consumers’ privacy can alleviate their concerns by building trust (Culnan and Armstrong 1999). In a study that was

---

1 This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).
not specific to the Internet, Phelps, D’Souza, and Nowak (2001) conducted a national mail survey to test a model of consumer privacy concerns about direct marketing, and found that consumers’ attitudes towards direct marketing and their desire for control over the use of their personal information were associated with privacy concerns.

A number of studies have surveyed consumers’ attitudes towards various marketing tactics, including the gathering and use of personal data, both online and offline. For example, Graeff and Harmon (2002) studied consumers’ awareness and concerns regarding the general collection and use of personal data. One of their findings was that a majority of consumers believe it is easier to obtain their personal information through the Internet than through other means. Even though there has been increasing awareness of the erosion of privacy, consumers are aware of the benefits of using the Internet, and some—24.9 percent of the respondents—do feel comfortable making credit card purchases on the Internet (Graeff and Harmon 2002). In particular, younger Internet users tend to have positive views on information collection for marketing purposes (Gervey and Lin 2000), while older consumers tend to feel less comfortable making credit-purchases on the Internet (Graeff and Harmon 2002). In comparison with female consumers, male consumers show fewer privacy concerns, and feel more comfortable making purchases on the Internet (Graeff and Harmon 2002). Another study examined the role of e-consumers’ personality trait on their shopping, surfing, and information seeking behaviors on the web, and suggested that e-consumers with low interpersonal trust tend to have high security concerns which in turn lead to lower intent to purchase on the Web (Das, Echambadi, McCardle, and Luckett 2003).

According to consumers, two of the most important attributes of commercial Websites are ease of use (e.g., simplicity, speed, convenience) and security (e.g., privacy, trustworthiness, transaction security) (Gervey and Lin 2000). Bush, Bush, and Harris (1998) found that security and privacy issues are major barriers to using the Internet as a marketing tool. Hershel and Andrews (1997) also reported that many users are reluctant to purchase products because of uncertainty regarding the privacy and security of information transactions. Thus, it is of great importance that e-businesses find a way to reduce consumer privacy concerns.

Antecedents of privacy concerns

Reducing privacy concerns and, in turn, increasing consumers’ willingness to disclose personal information, is one of vital keys to the success of e-commerce. Research in this field identifies antecedents that lead to a decrease in privacy concerns, namely (1) consumer trust in the e-vendor, and (2) the value provided by the Website. Trust is widely considered to be vital in allaying the privacy concerns of consumers. Considering that consumers in the Internet market are likely to interact with unfamiliar vendors, trust is an even more important construct in e-commerce than in traditional business transactions. In her review of consumers’ trust in online shopping, Grabner-Krauter (2002) claimed that trust arises in two environmental conditions, the uncertain and the risky, and further categorized the uncertainties as system-dependent and transaction-specific. Trust plays an important role in consumers’ overcoming their perceptions of risk and insecurity in online business transactions (McKnight, Choudhury, and Kacmar 2002). Based on the theory of reasoned action (Fishbein and Ajzen 1975), Liu, Marchewka, and Ku (2004) also proposed a privacy-trust-behavioral intention model to explain consumer’s behavioral intention for online transaction. Their laboratory experiment showed that four dimensions of privacy strongly influenced the level of trust, which in turn influenced a customer’s behavioral intentions to purchase from or visit a Website. A joint research project by Cheskin Research and Studio Archetype/Sapient (1999) on consumer trust in e-commerce concluded that trustworthiness is a result of a consumer’s experience of a website over time. According to the report, it is the brand image, navigation, consequent consumer fulfillment, presentation, up-to-date technology, and the logos of security-guaranteeing companies that constitute the essential characteristics of a website that communicate trustworthiness to a visitor. In the same way as for offline transactions, the trusting process in online transactions begins when an individual perceives that a company may be worthy of trust. Such a perception can be strengthened over time, and is eventually transformed into personifications of character, such as dependability, reliability and honesty. Using structural equation modeling, it has been found that trust is one of the most important determinants of a customer’s attitude towards using Internet banking (Suh and Han 2002).

Building consumers’ trust, a core component of social exchange theory and relationship marketing can be one of the solutions for enhancing e-retailing. Campbell (1997) viewed trust as an effective way of managing consumer privacy concerns, and noted that if consumers know that the personal information collected has the potential to build a relationship in which they could participate in the transfer of goods or services, their privacy concerns might be diminished or superseded by their desire to participate. Phelps and his colleagues (2001) found that a consumer’s attitudes towards direct marketing and desire for information control as antecedents to privacy concerns are related to subsequent purchase behavior. The second category of antecedents concerns how value provided by an e-vendor can reduce privacy concerns and increase the use of e-shopping. Exchange theory and a cost-benefit perspective suggest that consumers might be willing to provide information if they receive more than a certain level of value in exchange for their privacy disclosures.

In the field of Web research, the most important values perceived by consumers who accept the technology-based retailing of a product are two beliefs, both related to the utility and ease of using e-retailing (Gefen, Karahanna, and Straub 2003; Phelps et al. 2000). In addition, Chen and Dubinsky (2003) posit that values such as e-retailer reputation and the perceived quality and price of a product influence privacy concerns, which represent one type of perceived risk. Empirical evidence by Phelps and associates (2000) shows that privacy concerns will be reduced if consumers experience shopping benefits such as time saving and wider selection. Another study suggests that ‘having a mutually beneficial relationship with an online entity will have an influence on privacy concern’ (Sarathy and Robertson 2003).

Research model and hypotheses

Information gathered during e-business transactions are considered to be both a blessing and a curse to both businesses and consumers. Consumers are greatly concerned about the erosion of their privacy and are reluctant to share their information or to conduct business transactions in the Internet environment. Information collected using the Internet has enabled effective and efficient marketing strategies to benefit both businesses and consumers.

Research has shown that value and trust are separate but interrelated and complementary constructs. A study of Internet banking examined the effect of trust on customers’ attitude and behavior, and showed the effect on trust of perceived ease of use and perceived utility and the effect of trust on attitudes towards Internet usage and purchasing intentions (Suh and Han 2002). Each of these aspects has different types of sub-constructs and some are included
in both ‘trust’ and ‘value’ antecedents (Chen and Dubinsky 2003; Gefen et al. 2003). We investigated the three most prominent constructs of trust and/or value in the model—convenience of a website, a website’s reputation, and a third-party certificate—to identify their effects on consumers’ privacy concerns and willingness to disclose personal information. The research model is depicted in Figure 1.

Nowadays, a growing proportion of consumers are aware that their personal information can be collected, shared, and sometimes even stolen by unknown numbers of businesses, organizations, or criminals for financial gain. For example, “phishing” (a newest scams leading to identity theft) is estimated to cost victims more than $1.2 billion between April 2003 and April 2004 (Lepofsky 2004). Thus, consumers are starting to protect their privacy by refusing to disclose personal information or, where possible, providing deceptive information. Meanwhile, for the collected information to be useful, it must be accurate and up to date. To maximize usefulness of the collected information, Internet websites need to reassure users that their privacy is well protected. Milne and Boza (1999) showed that building trust was a key element in reducing the privacy concerns of consumers and improving relationships between consumers and businesses. Trust is developed through the effective communication of privacy safeguards, market signals that effectively convey high reputation and credibility, and previous favorable consumer experiences of perceived value. The development of trust between direct marketers and consumers reduces consumers’ perceived risk, which then improves consumers’ willingness to share their personal information with marketers.

The characteristics of an Internet website may impact on users’ privacy concerns. According to the Technology Acceptance Model (TAM), perceived ease of use and utility are major values provided by a website (Zeithaml, Parasuraman, and Malhotra 2002) and are key determinants of users’ technology acceptance (Gefen et al. 2003). Even though Salisbury and his colleagues (2001) showed that ease of navigation and usefulness were not significantly related to purchasing intention, a meta-analysis showed a weighted average correlation between ease of use and intention to use of .51 (Saeed, Hwang, and Yi 2003). Meanwhile, web security was related with purchase intention (Salisbury et al., 2001), and this suggests that users’ perception of web security is related to their perception of security.

Similarly, in his discussion of the nature of and conditions for online trust, Koehn (2003) recommended several guidelines for Internet retailers. For example, to maximize knowledge-based trust, Koehn (2003) recommends that Internet retailers should avoid poor spelling, grammar, and syntax that may cause doubts about their identity. For respect-based trust, purchasing processes should be user-friendly and customer-oriented.

Online consumers are also influenced by user interfaces (Chen and Dubinsky 2003), and are likely to shop at well-designed Websites (Liang and Lai 2002). A meta-analysis also indicated that system quality, including interface, navigation, and aesthetics, influences consumers’ behavior by changing their perceptions of ease of use, usefulness, trust, and shopping enjoyment (Saeed et al. 2003). Based on reviews of existing literature on this subject, we developed a hypothesis about the relationship between users’ perceived convenience of a website and their privacy concerns.

**Hypothesis 1:** The perceived convenience of a website is negatively related to users’ privacy concerns.

Another determinant that may influence Internet users’ sense of trust and privacy concern is a website’s reputation. Consumers develop a perception of the reputation of a retail outlet based on the service quality they experience, the nature of the store’s advertising, and the opinions of friends and relatives (Assael 1998). As the reputation of a store is equivalent to the total perception based on a consumer’s experience, knowledge, and belief in relation to that store, it has a strong effect on the consumer’s perception of the value offered by the store. This perception helps consumers to evaluate the differences between stores and choose between them. According to Sheehan and Hoy (2000), online users are less concerned about their privacy when they are interacting with companies with whom they are familiar. Consumers may feel familiar with a company when they have heard a positive evaluation of the company. Chen and Dubinsky (2003) also proposed that there is a positive relationship
between an e-retailer’s reputation and perceived risk that includes financial, performance, and privacy matters, but did not find a significant relationship. Chen and Dubinsky (2003) tried to explain this non-significant relationship by proposing that product price is a moderator. Specifically, the relationship between an e-retailer’s reputation and perceived risk might be stronger when the product being purchased is expensive. A study showed that an e-retailer with a good reputation tends to be more trusted and perceived as more credible than those with a poor reputation (Hendrix 1999). A meta-analysis by Saeed et al. (2003) showed that vendor characteristics such as size and reputation have an impact on online consumer behavior through vendor trust and the perceived usefulness of the vendor. Based on the present literature review, a relationship between a website’s reputation and users’ privacy concerns has been encapsulated in the following hypothesis.

**Hypothesis 2:** The perception of a website’s reputation is negatively related to users’ perceived privacy concern.

Meanwhile, Zucker (1986) proposed that the trust placed in an institution depends either on company-specific attributes (e.g., certification as an accountant) or on an intermediary mechanism (e.g., the use of escrow accounts). Such trust has a formal marketable structure similar to that of institutions and third-party guarantors that sell certificates guaranteeing integrity, ability, and intention. Such certifications are deliberately designed and used to build trust in the bearer’s ability and behavior, through external guarantors such as universities and state regulators.

For example, the Korean government issues an e-privacy certificate to Internet sites as supporting evidence of a vendor’s respect for personal privacy. In the United States, online seal programs, such as TRUSTe, the Online Privacy Alliance, and the Council of Better Business Bureaus, Inc. (BBBOnline), are designed to build consumers’ trust and confidence in the Internet. The certificates are typically conferred on the Internet sites by the government, institutions or the mass media. The conferred Internet sites display the certificate so that visitors will recognize that their privacy protection is dependable. Miyazaki and Krishnamurthy’s (2002) study indicated that participation in seal programs reduces consumers’ privacy concerns, although it has no influence on the actual online privacy practices of companies. The presence of seal logos was found to increase personal information disclosure among online shopping consumers who are highly risk-averse with respect to privacy security, but no effect was found for those who are less risk-averse. Kimerly and McCord (2002) found that third-party assurance seals had no influence on consumers’ trust of a specific e-retailer, with the exception of the use of one particular seal, TRUSTe. Accordingly, a relationship between third-party approval of a Web site and users’ perceived privacy concern was hypothesized as follows.

**Hypothesis 3:** The perception of third-party certificates in a Web site is negatively related to users’ perception of privacy concern.

Consumers’ willingness to disclose their personal information and their attitudes towards marketers’ use of that information are determined to be the sole factor affecting their willingness to disclose personal information.

**Hypothesis 4:** There is a negative relation between users’ privacy concerns about a Website and the intention to disclose personal information on the website.

### RESEARCH METHODS

To test the proposed model, an online survey was conducted. A Website was created for the Web survey and five thousand of e-mails requesting participation were sent to Internet users in Korea. E-mailing list was purchased from a research company. There were 395 online participants over a two-week period. After eliminating responses with insincere answers and excessive amounts of missing data, 323 responses were analyzed to test the proposed model. Sixty-eight percent of the respondents were male, almost all in their 20s or 30s.

### Measurements

The respondents were first asked to identify a Website they had recently visited. They were then asked to answer a series of questions about that Website. Questionnaire items were developed based on the literature review. Most of the items related to the three antecedents (i.e., perceived ease of using the Website, perceived reputation of the Web site, and third-party certificates in the Website) were conceptually based on Cheskin Research and Studio Archetype/Sapient (1999) and Luo (2002). The perceived convenience of using the Website was defined as the development of a trust based on convenience, usefulness, familiarity, and cultural similarity. The perceived reputation of the Website was based on brand name and experience. The perception of third party certificates was measured in relation to certificates, marks, and symbols authenticated by a third-party guarantor. Items for measuring privacy concerns and willingness to disclose personal information were adapted from Culnan (1993) and Cranor, Reagle, and Ackerman (1999) to fit the Internet context. Privacy concerns were measured in relation to uneasiness about unauthorized (internal and external) secondary use of personal information and improper access by third parties to the data. Willingness to disclose personal information was measured by asking respondents about the extent to which they were willing to disclose their personal information to the website.

The data were examined to assess the validity and reliability of the scales. First, exploratory factor analysis was conducted with a Varimax rotation to examine whether all items fell into the five conceptual categories, as expected. The five categories were extracted as expected, and no item failed to fall into these categories. The factor loadings were greater than .60, which is considered to be sufficient (Bagozzi and Yi 1988). As a measure of reliability, the internal consistencies of the variables were calculated. Internal consistency is an expression of the stability of individual measurement items across replication from the same source of information (Straub 1989). The Cronbach alphas of the constructs ranged from 0.83 to 0.95, which is considered to be an acceptable level of reliability (Hair, Anderson, and Tatham 1998; Straub 1989). The correlation matrix of the entire data set indicates that each item showed a higher correlation with items reflecting the same construct than with items reflecting other constructs, in accordance with the MTMM (Multitrait-Multimethod) principle (Bagozzi 1991).

Finally, a confirmatory factor analysis (CFA) was run using LISREL 8. The CFA indicated that several items had shared residual variance, which means that they needed to be dropped to achieve unidimensionality and good fit indexes in LISREL.
resulting CFA showed that all remaining items loaded significantly and highly on their assigned constructs and that LISREL reliability coefficients and extracted variances of constructs were acceptable. The CFA also showed that the overall models’ fit indices were good, except for $\chi^2$, which is typical for a large sample: $RMSR=.05$, $GFI=.93$, $AGFI=.90$, $NFI=.93$ and $\chi^2_{109}=213.23 (p=.00)$ (Kelloway 1998).

Hypothesis testing

The hypotheses were analyzed using LISREL 8; the results are presented in Figure 1. There was good model fit ($\chi^2_{112}=227.35 (p=.00)$, $GFI=.92$, $AGFI=.90$, $NFI=.93$, $RMSR=.062$), except for $\chi^2$, which is typical for a large sample. In addition to the overall fit of the model, four relationships were proposed. In Hypothesis 1, a negative relationship was proposed between consumers’ perceived convenience of using a Website and their privacy concerns about the Web site. The data showed a significant negative relationship ($\gamma = -.44$, $p<.01$) as proposed. However, Hypothesis 2 was not supported ($\gamma = .02$, $p>.10$). In other words, the relationship between the perceived brand reputation of a Website and an individual’s privacy concerns about that Website was not significant. Hypothesis 3 proposed a negative relationship between third-party certificates and privacy concerns, and was supported ($\gamma = -.14$, $p<.05$). The data supported Hypothesis 4, which proposed a negative relationship between users’ privacy concerns and their willingness to disclose personal information ($\beta = -.15$, $p<.01$).

DISCUSSION

This research makes two primary contributions to the field of Internet marketing. Most previous studies incorporated constructs of value and trust separately and used sub-dimensions such as ease of navigation, usefulness, web security, brand, technology, and clarity of interface interchangeably to determine whether these are related to the willingness to disclose personal information. However, the present study tried to reclassify three categories of antecedent simultaneously in relation to benefits and trust. The present study proposed a model incorporating antecedents, privacy concern, and intent to disclose personal information. This study is one of the first attempts to examine empirically a model that embraces antecedents that are associated with Internet users’ privacy concerns and their willingness to cooperate Internet sites for direct marketing. Most studies incorporated those factors separately as determinants of trust in or perceived value of the Internet, or attitudes towards direct marketing, or examined causal relationships between trustworthiness and attitude towards disclosure. Thus, the present study embodies a more comprehensive approach.

All proposed path relationships were significant, with one exception: between perceived brand reputation of a Website and privacy concerns about the Website. This implies that Internet users tend to feel more secure and safe at Websites that they perceive as more comfortable, convenient, and easy to use, and where they can recognize reliable third-party certificates or logos. Accordingly, a business may be wise to maximize the user-friendliness of its Website by making it more consistent with potential visitors’ value and preferences. The business may consider acquiring authentic third-party certification by establishing concrete privacy-related policies and practices. By doing so, the business could gather high-quality data regarding current and potential consumers, which may increase its profitability.

However, the reputation of a Website will not directly allay the privacy concerns of consumers. This may be because the experience of most online shoppers has not yet accumulated to the extent that it supports a good reputation for Websites. Meanwhile, consumers who are less concerned about their privacy at a Website are more willing to share their personal information for marketing purposes. Considering that marketers need quality data for individualized marketing strategies, individuals who are willing to share their personal information are a valuable source of quality data. Consumers who are willing to provide accurate and current data in comparison with those who are forced to or deceived into disclosing their personal information may provide more reliable data. According to our findings, Websites that collect, store, and exchange consumer data are likely to improve their data quality and quantity if they establish the trust of their Website visitors by developing visitor-friendly Websites and obtain and display privacy-related certificates and logos conferred by credible third-party organizations.

Our proposed model and its empirical testing could provide valuable information to policy makers who intend to boost e-commerce. The model suggests that governments should consider establishing comprehensive and clear-cut policies regarding consumer privacy issues in e-businesses and direct marketing. Under such policies, a certificate could be conferred to compliant e-businesses. In this way, consumers would become less reluctant to make business transactions on the Internet, thereby assisting the expansion of e-business.

Like other studies, this study has a number of limitations. First, most of the respondents were regular Internet users. Thus, the findings may not be applicable to those who are unfamiliar with it. However, this may not be a significant concern because Internet businesses are also mostly interested in understanding the attitudes and behaviors of consumers who already are regular Internet users. The second limitation is also related to the sample. Most of the respondents were students or office workers. Considering a growing number of housewives are active Internet users, a portion of the population could be considered as under-represented, and the findings may not be generalizable to other populations.

The present study raises other questions that call for future research. Future studies should measure actual disclosure rather than merely stated willingness to disclose personal data. Considering the variety of Websites, privacy concerns and behaviors could be compared among various categories of Websites with different characteristics. For example, the Website of a non-profit organization may not be perceived to be as much of a threat to privacy as a commercial website.

REFERENCES


Cheskin Research and Studio Archetype/Sapient (1999),
concern: understanding Net users’ attitudes about online
privacy,” AT&T Labs Research Technical Report 15
(September).
exploratory investigation of consumer attitude toward
concerns, procedural fairness and impersonal trust: an
Das, S., R. Echambadi, M. McCardle, and M. Luckett (2003),
“The effect of interpersonal trust, need for cognition, and
social loneliness on shopping, information seeking and
Ernst and Young (1999), The second annual Ernst and Young
Internet shopping study.
Fishbein, M. and I. Ajzen (1975), Belief, attitude, intention, and
behavior: An introduction to theory and research, Reading,
MA: Addison-Wesley.
in online shopping: an integrated model.”, MIS Quarterly,
27(1), 51-90.
Advertising Age survey finds privacy and security concerns
are blocking the growth of e-commerce,” Advertising Age,
71, 113.
online-shopping,” Journal of Business Ethics, 39, 43-50.
personal data: consumers’ awareness and concerns,” The
Multivariate data analysis with readings, 5th edition.
Hendrix, P. E. (1999), “Build it, and they will come,” Marketing
Management, 8, 31–35.
Javis, S. (2000), Companies tell all about consumer privacy.
Marketing News, 34, 3.
concerns cost eCommerce $15 Billion,” Forrester Research.
Kelloway, E. K. (1998), Using LISREL for structural equation
Kimery, K. and M. McCord (2002), “Third-party assurances:
mapping the road to trust in e-retailing,” Journal of
Information Technology Theory and Application, 4, 63–82.
Management,” 51(10), 34-40.
Liang, T. and H. Lai (2002), “Effects of store design on
consumer purchases: an empirical study of online
Taiwanese perceptions concerning privacy, trust, and
behavioral intentions in electronic commerce,” Journal of
Global Information Management, 12(1), 18-40.
Luo, X. (2002), “Trust production and privacy concerns on the
Internet: a framework based on the relationship marketing
and social exchange theory,” Industrial Marketing
Management, 31, 111–118.