Privacy Concerns And Internet Use – A Model Of Trade-Off Factors

Tamara Dinev
Department of Information Technology and Operations Management
College of Business
Florida Atlantic University
777 Glades Rd.
Boca Raton, FL 33431
e-mail: tdinev@fau.edu
TEL: (954) 762-5313
FAX: (561) 297-3686

Paul Hart
Department of Information Technology and Operations Management
College of Business
Florida Atlantic University
777 Glades Rd.
Boca Raton, FL 33431
e-mail: hart@fau.edu
TEL: (561) 297-3674
FAX: (561) 297-3686

Abstract

While privacy is a highly cherished value, few would argue with the notion that absolute privacy is unattainable. Individuals make choices based on tradeoffs in which they surrender a certain degree of privacy in exchange for benefits that are perceived to be worth the cost of information disclosure. This research focuses on the delicate balance between the perceived personal benefits and privacy costs associated with Internet use in conducting e-commerce transactions. A theoretical model was developed and empirically tested using data gathered from 369 respondents. Structural Equations Modeling (SEM) with LISREL after Exploratory and Confirmatory Factor Analyses were conducted to validate the instrument. The results suggest that privacy concerns inhibit e-commerce transactions. However, the cumulative influence of trust, personal interest, and the ability to control personal information are important factors that

can outweigh perceptions of vulnerability and privacy concerns when using the Internet. The findings are important for a number of reasons including their general support for the arguments made by researchers who have advocated the need to follow "procedural fairness" with respect to information disclosure.

Introduction

The individualistic and libertarian nature of the American society places privacy as a highly privileged value (Etzioni 1999). In the recent years, the explosive growth of information technology and Internet use to obtain information, goods and services has fueled debate and controversy about the potential threats to privacy. The increased technical capacity of information systems provides clear efficiency and qualitative benefits to firms that gather, process, and store consumer data. The use of this vast amount of data to profile customers and acquire knowledge about customer behaviors and preferences allows firms to develop, market and distribute products and services in more efficient ways, thus opening more opportunities for growth and competitive advantage. While these processes provide strategic benefits to firms, they also introduce vulnerabilities for individuals (Kling and Allen 1996) who either intentionally or unintentionally disclose information. Yet, while concerns about privacy have reportedly increased, Internet use continues to increase as well.

Information systems researchers have been concerned about privacy issues for a number of years. Prominent examples include the work of Culnan (1993), Culnan and Armstrong (1999), Mason (1986), Milberg et al. (1995), Smith (1993), and Smith (1996). There is every reason to believe that researchers would have continued to be interested in information privacy as information technology applications and use continue to increase. However, the events on

September 11th may prove to be a further important catalyst in fueling the debate among citizens of Western democracies that could generate even more research regarding this issue.

The objective of our research is to better understand the predictors of withholding or surrendering personal information when using the Internet, as well as to identify competing factors that influence the decisions to use the Internet for e-commerce activity. In this paper we report on the development and validation of a model that assesses the trade-offs in the delicate balance between the perceived personal benefits and privacy costs associated with Internet interaction. The model assessment uses Structural Equations Modeling (SEM) with LISREL. Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) were used to develop and validate the instrument which measures privacy-related antecedents to Internet use and use itself. The primary contribution of this paper is the empirical evidence demonstrating that a number of factors play a role in decisions to interact with web sites. By identifying the trade-offs that allow individuals to surrender private information, companies should gain a better understanding of how to address privacy concerns and increase the level of comfort and sense of security for those who seek to obtain information, products, and services through the Internet. And this, in turn, should lead to an increase in Internet use to support e-commerce activity (Gefen and Straub 2002).

Theoretical Framework

A number of researchers have examined the concept of privacy from a behavioral perspective (e.g., Goodwin 1991, Laufer and Wolfe 1977, Margulis 1977, Tolchinsky et al. 1981). Margulis (1977) proposed the following common-core definition consistent with various approaches: "Privacy represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability". Two themes are evident in this

definition, which are common throughout the literature: 1) the notion of individual control over disclosed personal information (Johnson 1974, Shils 1966, Westin 1967), and 2) the notion of vulnerability. Vulnerability refers to the perception of the consequences of disclosure (Fusilier and Hoyer 1980). This definition implies that privacy is a complex construct, constituting a dichotomy between the individual and others (Kelvin 1973) and between the factors that define it, namely control and vulnerability. Moreover, it is a dynamic variable that is likely to vary over time and is dependent on any given individual's experience.

Scholarly interest in privacy among MIS researchers has paralleled the development of digital network and storage technologies. The threat to privacy has been examined by researchers focusing on the role of large commercial organizations (e.g., banks, lending institutions, and credit card companies) that use these technologies to advance their own purposes (e.g., Clarke 1998, Culnan 1993, Culnan and Armstrong 1999, Jones 1991, Mason 1986, McCrohan 1989, Petty 2000, Phelps et al. 2000, Rindfleish 1997, Thomas and Mauer 1997). On the one hand, organizations gain competitive advantage by using collected transaction data (Glazer 1991). Highly sophisticated technologies like data mining and knowledge discovery require a large amount of personal data from a large number of individuals, so that new business rules and patterns can be extracted. Companies use profiling for targeted marketing, developing better products and relationships with customers, and for identifying consumer preferences. On the other hand, the increasing need for more detailed customer information increases the potential for privacy invasion. An increased perception of the latter could lead to a decrease in the size of the customer base due to customer unease in conducting online transactions. As Culnan and Armstrong (1999) state, "the challenge to organizations, then, is to balance the competing forces of the power of information with privacy in their dealings with customers" (p. 105).

At the same time, a good deal of MIS research has also focused on privacy concerns and procedures within organizations - for example, employee values and beliefs about regulatory approaches have been examined across different types of organizations (Kelvin 1973, Milberg et al. 1995, Milberg et al. 2000, Smith 1993, Stewart and Segars 2002, Stone et al. 1983, Tolchinsky et al. 1981). In an interesting investigation, Smith, Milberg, and Burke (1996) also examined the effect of regulatory approaches across different cultures. They found that a country's regulatory mechanisms for managing information privacy are affected by its cultural values and by individuals' information privacy concerns. The primarily reactive self-regulatory mechanisms of privacy governance found in the United States may in fact increase privacy concerns, thus bringing into question the long-term sustainability of the self-regulatory approach. Moreover, since Internet transactions generally involve several entities (e.g., merchant, credit card company, web provider, etc.), it is doubtful whether strict privacy policies can be self-enforced across all entities. As Milberg et al. (2000, p.50), concluded, "there is a little reason to believe that a particular firm can successfully protect privacy when its policies are at variance with those of other firms in its industry" involved in an e-commerce transaction. And "until a critical mass of agreement is reached regarding policies…self-regulation cannot be a meaningful approach to the governance of privacy" (p. 50).

Privacy research on the specific challenges posed by the Internet is beginning to emerge. Culnan (2000) and Miyazaki and Fernandez (2000) examined Internet retail disclosures and self-regulatory practices. Their findings were consistent with Milberg et al. (2000) arguments about the viability of the self-regulatory mechanisms. In addition, they found that the privacy policies and adherence to them vary across industries. Sheehan and Hoy (2000) conducted an e-mail survey to examine dimensions of privacy concerns among online users. Phelps et al. (2000)

examined privacy concerns and consumer willingness to provide personal information. Their study addressed the trade-offs consumers are willing to make when they exchange personal information for shopping benefits. However, their study focused on traditional direct marketing channels rather than the Internet.

Internet users are becoming increasingly conscious of the power of Internet technologies to monitor their behavior and to unobtrusively gather information about them. Some users might be prone to develop concerns and suspicions, sometimes unwarranted, about the "hidden" or undisclosed purposes of free software applications or websites, which claim to facilitate online browsing. This might lead to inhibiting Internet use and/or resulting in more limited use or an aversion to experimenting with new applications and/or web sites.

According to the UCLA Report (2000, 2001 and 2002), privacy concerns and the requirement to submit personal data are among the primary factors that discourage users from shopping online. According to the same study, only 1 out of 3 initiated online shopping procedures end up with actual purchase primarily due to reluctance to submit personal data. Many consumers do not register at web sites primarily because of privacy concerns and as much as 50% of consumers provide false information when asked to register at a web site or fill in surveys (Greenman 1999, BCG 1998). Therefore, it is important to better understand which factors contribute to easing individuals' privacy concerns when submitting information over the Internet.

Fair information practices are global standards for the ethical use of personal information and provide individuals with the ability to control disclosed personal information (Culnan 1993). They are based on the notion of procedural fairness (Culnan and Armstrong 1999). Fair information practices are an important factor in the "privacy calculus" the user makes in determining whether to disclose personal information through a web site. The "privacy calculus"

is an assessment made regarding whether disclosed information will be used in a way that will have negative consequences for the individual (Culnan and Armstrong 1999, Laufer and Wolfe 1977, Milne and Gordon 1993, Stone and Stone 1990). On the one hand, there are concerns about how easily accessible information disclosed could be to others or whether the information could be misused in a way that would negatively affect the individual. On the other hand, there are personal interests in obtaining information, products or services via the Internet. Firms can promote customer disclose of personal information by adopting fair information practices and announcing their information policies. Nevertheless, effectiveness of self-regulatory privacy information handling strategies are questionable. According to Culnan (2000), while 67% of the web sites post privacy disclosure, only 14% of these disclosures constitute comprehensive and fair privacy practices and policies. Similar results have been reported by Miyazaki and Fernandez (2000), with substantial differences across product categories.

Culnan and Armstrong's (1999) notion of a "privacy calculus" provides a useful theoretical framework upon which we built our model of trade-off factors in Internet usage. The above considerations suggest the following:

Hypothesis 1: There is a negative relationship between privacy concerns and Internet use.

Privacy concerns are dependent on an individual's experience and are likely to vary over the course of an individual's lifetime (Louis Harris and Associates 1991). Individuals, who experience a positive outcome (e.g., a job offer) as a result of information disclosure, perceive less privacy invasion than those who did not experience a positive outcome (Fusilier and Hoyer 1980). Thus, privacy concerns are dependent on the perception of the outcome of information disclosure. The perception of a negative outcome constitutes vulnerability, that is, an individual

is likely to suffer as a consequence of personal information disclosure. Therefore, perceptions of vulnerability are an important determinant of privacy concerns.

The primary sources of perceived vulnerability for Internet users are related to the risk of misuse or abuse of personal information mainly through three categories of privacy invasion: 1) unauthorized access to information, 2) surreptitious collection of consumer information, and 3) unwanted contact or solicitation based on secondary usage and/or consumer profiling. Unauthorized access to information can be caused by any number of factors including accidental disclosure, insider curiosity, insider subordination, unauthorized access, hacking into computer systems, security defects, scams (i.e., fraudulent web sites established for the purpose of obtaining information and money), and so on (Rindfleish 1997, O'Brien 2000). Surreptitious collection of consumer information is highly probable on the Internet due to the distributed nature of handling, storage, and availability of transaction data. A single e-commerce transaction spans several organizational information systems, from the merchant to the web site provider, as well as several geographical regions. A lack of strict privacy policies increases the risk of surreptitious collection and usage of personal information, including "identity theft" (Saunders and Zucker 1999). Lastly, vulnerability is also based on the uncontrolled use of secondary data by a third party unrelated to the initial transaction agent without the knowledge or consent of the consumer. This results in consumer profiling and subsequent unwanted contacts and solicitation (Budnitz 1998, FTC Report 1999).

The above factors contribute to perceptions of vulnerability among Internet users and influence privacy concerns. Therefore we conclude that perceptions of vulnerability have to be considered as a separate construct and are related to Internet users' privacy concerns:

Hypothesis 2: There is a positive relationship between users' perceptions of vulnerability and their privacy concerns.

Hypothesis 3: There is a negative relationship between users' perceptions of vulnerability and their Internet usage

Control over personal information allows individuals to determine the impressions others form about them (Goffman 1963). Control is possible through limiting self-disclosure (Derlega and Chaikin 1977) or by determining how information disclosed will be used (Stone and Stone 1990). In general, consumers find it unacceptable for marketers to sell information about them (Nowak and Phelps 1992). Individuals strenuously object the lack of knowledge about secondary use of their personal information (Wang and Petrison 1993). Given the anonymity and impersonal nature of interactions with a web site, it is reasonable to expect that an individual's need to control disclosed information will be a factor in decisions to make online purchases. Indeed, online consumers have expressed concerns about how information might be transferred to third parties without their consent (Milne 2000). Sheehan and Hoy (2000) found that the ability to control information collection and use by third parties are concerns among online consumers. According to Phelps et al. (2000) purchasing decisions are affected by the amount of information control consumers are given and the type of information requested. Studies have reported that 81% of the respondents believe that consumers have lost all control over how personal information about them is circulated and used (Budnitz 1998) and that 86% of consumers want to be able to control personal data (BCG 1998).

Privacy has been strongly related to the ability of individuals to control information about themselves (Westin 1967). Individuals perceive information disclosure as less privacy-invasive when, among other things, they believe that they will be able to control future use of the

information and that the information will be used to draw accurate inferences about them (Culnan and Armstrong 1999). Individuals believe their privacy is compromised when they are aware that information about them is being collected without their consent (Nowak and Phelps 1995). Using consumer data without permission is seen as an invasion of consumers' privacy and non-ethical and illegitimate behavior on the part of the company Cespedes and Smith (1993).

There is ample evidence to suggest that when control is not allowed or when future use of information is not known, individuals resist disclosure. In their study on procedural fairness and fair information practices, Culnan and Armstrong (1999) operationalized fairness in terms of procedures that provided individuals with control over disclosure and subsequent use of personal information. They found that when individuals were not informed about fair procedures they were less willing to have information used. They also found that for individuals who were informed about fair procedures, privacy concerns did not distinguish individuals who were willing from those who were unwilling to have information used. In other words, privacy concerns washed out.

Despite the findings of previous research, few companies provide information about how submitted personal information will be stored, handled, and subject to secondary use. Milne and Boza (1998) found that 38% of online sites notify customers about gathering personal information, 33% indicate the use of this information, and 26 % ask for permission to use the information (also see Culnan 2000, and Miyazaki and Fernandez 2000). Therefore, there is a disparity between consumer demand for control and disclosure by businesses regarding how personal information is used and the extent to which consumers can control information use. This disparity may be one of the reasons that motivate online users' practices of providing false information when asked to register at a web site or fill in surveys, as found by Greenman (1999)

and BCG (1998). We therefore conclude that the ability to control is an antecedent to both privacy concerns and Internet usage:

Hypothesis 4: There is a negative relationship between perceived ability to control and privacy concerns.

Hypothesis 5: There is a positive relationship between the perceived ability to control and Internet usage.

Trust is also an important element in conducting online transactions. Trust is a complex variable with many dimensions and is difficult to define (Rousseau et al. 1998, McKnight et al. 2002). The widely accepted definition is that trust is the belief that another party will act in an anticipated way. It reflects a willingness to assume risks of disclosure and to be vulnerable to another party (Mayer et al. 1995). Positive experiences with a firm over time increase customers' perceptions that the firm can be trusted (Culnan and Armstrong 1999). Building trust is important because it increases the likelihood that the customer will be involved in future relationships with the firm (Gundlach and Murphy 1993). A component in building consumer trust involves providing improved products and services, which requires greater knowledge of customer demand and preferences. Thus, paradoxically, the process of building trust also involves an increase in consumer data collection and analysis, which may constrain trust development. The potential harm can be avoided by implementing fair information practices that positively influence both trust and privacy concerns (Bies 1993).

Hart and Saunders (1997) categorized the dimensions of trust into two basic groups: the cognitive group and the emotional group. The cognitive group includes the dimensions of competency and reliability, while the emotional group constitutes the dimensions of caring and openness. Other dimensions of trust appear in the literature, however most fall within one of

these two categories. For example, the dimensions of ability, benevolence, and integrity (Lee and Turban 2001, McKnight et al. 2002) are all related to the cognitive group of trust.

In the specific context of Internet usage, the potential for e-commerce can only be realized if consumers are comfortable transacting with unfamiliar vendors and web sites (Gefen and Straub 2002). According to Hoffman et al. (1999), close to 95% of consumers have declined to provide personal information to Web sites, and 63% of these do not trust those collecting the data. Comfortability levels of consumers transacting over the Internet are associated with the anticipation of positive outcomes and with lower perceptions of vulnerability. Therefore, there is an important relationship between consumers' perceptions of vulnerability and the level of trust in the vendor.

Trust in e-commerce becomes both more important to consumers than traditional brick-and-mortar business and harder to define. Internet transactions are characterized by greater social distance (Culnan and Armstrong 1999). Therefore, cognitive development of trust becomes more important without the face-to-face opportunity to build trust related to emotional factors. When trust has been established between two parties, privacy issues are of less concern (Sweat 2000). Often web sites are relatively new or unfamiliar to users. Long-standing experience that might otherwise build trust is not necessarily present in the context of e-commerce. This reinforces the need for communicating competence and reliability to encourage more involved interaction of the Internet users. Therefore we advance the following hypotheses:

Hypothesis 6: There is a negative relationship between users' perceptions of vulnerability and their trust.

Hypothesis 7: There is a positive relationship between the perceived ability to control and trust.

Hypothesis 8: There is a positive relationship between trust and Internet usage.

An important factor in the decision to surrender personal information is the extent of personal interest in obtaining certain information, products, or services. Interest can range from the intent to obtain coupons, personalized special offers and improved buying experiences (Sweat 2000), to the need for extensive research and valuable information, or the need to obtain urgent and life-saving information about diseases and health risks/benefits. The interest in information is based on the need to obtain accurate and very specific services/information. Online support groups, discussion boards, advisory and referral services, drug information sites fall into these categories. When information is otherwise unavailable or difficult to access, individuals will be more inclined to submit highly sensitive personal information in exchange for critical information. In their study, Phelps et al. (2000) found that personal interest is an important antecedent to consumer willingness to provide personal information to direct marketers. Personal interest should be an important factor that may compete with the privacy concerns and be related to more extensive and interactive Internet use.

Hypothesis 9: There is a positive relationship between interest and Internet usage.

The factors discussed in this study, perceptions of vulnerability, privacy concerns, trust, ability to control, and interest – present a complex and dynamic psychological map of user attitudes and behaviors with respect to the Internet e-commerce. Culnan and Armstrong's (1999) application of procedural fairness to the privacy calculus conducted by individuals when determining whether to disclose personal information provides an important theoretical framework for understanding the trade-offs related to information privacy. They argue that the collection and use of personal information involves a "social contract" between the consumer and the firm, where, in addition to completing a purchasing transaction, the consumer also makes a

non-monetary exchange of personal information for benefits such as higher quality of service or better products. Customers will continue to participate in this contract as long as benefits exceed the risk. The violation of this psychological contract may result in angry and disloyal customers, which are more likely to defect (Morgan and Hunt 1994).

Our model of competing and simultaneously influencing factors (trade-offs) that affect decisions to engage in Internet transactions attempts to operationalize the notion of the privacy calculus. For users to engage in Internet e-commerce transactions, a balance between the trade-offs has to be achieved. Any misbalance between perceived vulnerability, trust, privacy concerns, perceived ability to control, and interest in which the negatively influencing factors would prevail, results in user resistance to complete the transaction. And vice versa, the more the positively influencing factors prevail, the more users will be inclined to complete transactions. Figure 1 illustrates the proposed model for the effect of the discussed constructs on the Internet level of use. Therefore we are advancing our last hypothesis:

Hypothesis 10: The competitive and simultaneous influence of the factors of Internet use included in our model results in users' decisions to conduct online transactions if positively influencing factors prevail.

Methodology, Instrument Development, and Results

The research model was empirically tested using data collected from a survey. Two pilot tests and a final survey were administered to a broad sample of individuals in the southeast of United States. The survey demographics were reported elsewhere (identifying reference). The 369 respondents[1] to the final survey comprised a sample of wide range in age, employment, education, race, with almost equal representation of gender. The respondents were a heterogeneous group that may approximate a representative sample of a larger population of

[1] Earlier reports on this study were based on a sample of 301 individuals.

Internet users. The development of the scales for the constructs considered in this study was initiated by examining prior work on similar constructs. However, the items used in each of the pilot tests and in the survey were developed by the authors using a 5-point Likert scale.

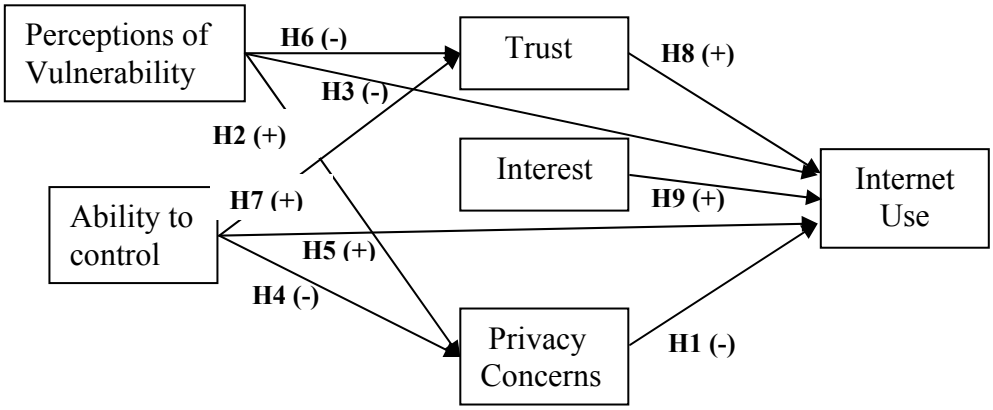

Figure 1. Model of Trade-off Factors of Internet Use

Exploratory Factor Analysis

Exploratory Factor Analysis (EFA) of the privacy construct and its antecedents – perceived vulnerability and perceived ability to control - were also reported elsewhere (identifying reference). The instruments for these constructs are shown in the Appendix. During the EFA previously reported, we identified two dimensions of privacy concerns: privacy concerns related to information finding (PCIF) and privacy concerns related to information abuse (PCIA). Our analyses demonstrated that these two privacy concerns are distinctly different. However, they display similar relationships. For the purpose of this study, we consider the PCIA construct to which we simply refer as privacy concerns or PC. Here we report the EFA phase of the other constructs while considering the privacy construct and its antecedents in their nomological net. Reliability tests using Cronbach's alpha coefficients were used to assess the internal consistency

of the scale items for each construct. In all cases, the coefficients were above .84 - much higher than the threshold level of 0.6 suggested for exploratory research. The corrected item-total correlations, which provided initial indications of reliability, were high for most of the items.

The convergent and discriminant is established through EFA by examining the correlations among all items of all constructs. Factor analysis with Varimax rotation and Kaiser normalization was utilized to make the initial assessment of the constructs' adequacy, with all items run simultaneously in EFA. All indicators loaded on the latent variables they were intended to measure, with insignificant cross-loadings of items. This ensures the face/content validity of the instrument. Furthermore, most of the factor loadings range between .7 and .9, as shown in Table 1. In addition, all inter-item correlations were examined for further verification of discriminant validity. The values of the correlations between items measuring different constructs were significantly lower than the correlations between the items measuring one and the same construct. These results suggest that both discriminant and convergent validity were established through the classical EFA approach. The items comprising the constructs' scales used in this study are shown in the Appendix.

Item	**Mean**	**Standard Deviation**	**Corr. Item-Total Corr.**	**Privacy Concerns (PC)**	**Internet Use (IU)**	**Perceptions of Vulnerability (PV)**	**Personal Interest (PI)**	**Trust (T)**	**Perceived Ability to Control (AC)**
				$\alpha = .88$	$\alpha = .84$	$\alpha = .88$	$\alpha = .86$	$\alpha = .91$	$\alpha = .89$
PC1	3.78	1.07	.66	**0.79**	0.01	0.15	-0.12	-0.12	0.09
PC2	3.86	1.10	.76	**0.79**	-0.36	0.14	-0.05	-0.13	0.08
PC3	3.82	1.03	.84	**0.87**	-0.17	0.19	-0.06	-0.09	0.05
PC4	3.68	1.08	.70	**0.79**	-0.11	0.17	-0.03	-0.17	-0.01
IU1	3.41	1.11	.68	-0.11	**0.78**	0.01	0.16	0.21	0.12
IU2	2.85	1.14	.62	-0.11	**0.64**	-0.14	0.19	0.28	0.08
IU3	3.15	1.15	.80	-0.15	**0.85**	-0.03	0.13	0.21	0.07
IU4	3.12	1.25	.64	-0.14	**0.76**	0.00	0.11	0.19	0.06
PV1	3.93	0.90	.71	0.14	-0.02	**0.81**	0.00	-0.10	0.06
PV2	3.93	0.87	.77	0.18	-0.06	**0.85**	-0.02	-0.09	0.05
PV3	4.11	0.82	.80	0.13	0.00	**0.87**	0.00	-0.15	0.07

PV4	3.91	0.88	.67	0.04	-0.02	**0.77**	-0.07	-0.11	0.10
PI1	3.47	0.97	.73	-0.07	0.20	-0.10	**0.83**	0.14	0.06
PI2	3.46	1.03	.75	-0.02	0.16	-0.06	**0.83**	0.17	0.04
PI3	3.25	1.09	.74	-0.13	0.18	-0.13	**0.80**	0.18	0.09
T1	2.99	0.90	.84	-0.15	0.27	-0.13	0.16	**0.78**	0.03
T2	3.08	0.86	.80	-0.17	0.32	-0.08	0.18	**0.70**	0.06
T3	3.04	0.67	.87	-0.13	0.25	-0.14	0.16	**0.92**	0.06
AC1	3.48	0.93	.73	0.05	0.14	-0.04	0.03	0.01	**0.81**
AC2	3.53	0.98	.84	0.05	0.06	0.04	0.10	0.11	**0.87**
AC3	3.64	0.71	.82	0.08	0.03	0.15	0.10	0.10	**0.93**

Table 1. Exploratory Factor Analysis. (The items' means, standard deviations, corrected item-total correlations, and factor loadings. Cronbach's alpha α is shown for each factor.)

Confirmatory Factor Analysis - Measurement Model

After determining a high reliability and validity of the instrument through EFA, the study proceeded with CFA Measurement model. Confirmatory Factor Analysis (CFA) is a contemporary approach that represents a significant advancement of validity assessment in comparison to EFA (Bollen 1989), and results in increased confidence in instrument validity. This study employs LISREL 8.5 as the CFA and SEM software for assessing the model validity (Joreskog and Sorbom 1993). Maximum likelihood estimations were employed for the model assessment. This step was essential to assess and finalize and bring the measurement model to satisfactory levels of validity and reliability before structural model was tested (Segars and Grover 1993). CFA was performed on the entire set of items simultaneously with each observed variable restricted to load on its a priori factor.

Unidimensionality and convergent validity. The unidimensionality and convergent validity criteria require that a set of measurement items appears to be indicators of one single underlying latent variable. Assuming the overall model fit indices are adequate, high factor loadings (above .60 as suggested by Bagozzi and Yi 1988) and high t-values of the items to their respective

constructs establish unidimensionality and convergent validity (Bollen 1989). In general, if the t-values are greater than |1.96| or |2.576|, they are considered significant at levels .05 and .01, respectively (Koufteros 1999). In addition, potential misspecifications in the measurement model can be detected by examining each item's modification indices and completely standardized expected changes in Λ_x, (i.e., potential cross loadings). Items with statistically significant cross-loadings lack unidimensionality. High modification indices suggest that the item may share a significant amount of the variance with another construct, thus the item is not unidimensional. An often considered threshold is the expected change with a value greater than .4 which usually is an indication of lack of unidimensionality. Table 2 provides the complete list of the final measurement model items and the constructs they describe, with their standardized factor loadings (λ‘s), error terms and the t-values of the factor loadings. The model diagram presented in Appendix II implies the measurement model of the six latent variables addressed in our study along with their corresponding indicators. As seen from the results, all the items exhibit high λ‘s and high statistically significant t-values (much higher than the cut-off value corresponding to statistical significance at level .01). No item with completely standardized expected change in Λ_x greater than .4 was found – in fact, the greatest value of expected change is .23. Thus, all indicators are significantly related to their specified constructs and thus provide evidence to support the convergent validity.

The average variance extracted (AVE), a measure of the amount of variance captured by a construct from each scale has recommended values of .50 or higher to provide evidence for convergent validity (Fornell and Larcker 1981). As seen from Table 3 which provides the AVE for all constructs, the lowest value is .61, with most AVE's in the range of .7 to .8.

Latent Variable	Item	Unstandardized Factor Loadings	Completely Standardized Factor Loadings	Factor Loadings Error Term	t-value	R^2

IU	IU1	.84	.77	.05	16.67	.59
	IU2	.76	.68	.05	14.15	.46
	IU3	1.00	.88	.05	20.42	.78
	IU4	.89	.72	.06	15.32	.52
PC	PC1	.78	.69	.05	14.68	.48
	PC2	.99	.84	.05	19.23	.70
	PC3	1.00	.92	.04	22.05	.84
	PC4	.87	.77	.05	16.86	.59
PI	PI1	.91	.84	.04	18.65	.70
	PI2	.94	.82	.05	18.08	.67
	PI3	1.00	.83	.05	18.31	.68
T	T1	1.00	.90	.04	21.78	.81
	T2	.90	.85	.04	19.91	.72
	T3	.79	.94	.05	23.35	.88
PV	PV1	.95	.77	.04	16.97	.60
	PV2	1.00	.85	.04	19.45	.72
	PV3	.97	.87	.04	20.30	.76
	PV4	.84	.71	.04	15.07	.51
AC	AC1	.76	.74	.04	16.26	.55
	AC2	1.00	.93	.04	22.54	.87
	AC3	.69	.89	.03	21.05	.80

Table 2. Confirmatory Factor Analysis Statistics.

Discriminant Validity. There are three techniques to determine discriminant validity (Mullen et al. 1996), which refers to the extent to which items that measure one construct are different from the items that measure another construct. The first technique is to analyze the correlations between the latent constructs. Assuming the overall model fit indices are adequate, discriminant validity is achieved if the correlations between constructs are not equal or close to 1.00. If some of the correlations are close to 1.00, the second alternative technique - the χ^2 difference test can be performed (Joreskog and Soborn 1993, Bollen 1989). In this test, a model is analyzed in which the correlation between any two constructs (ϕ_{ij}) is fixed at 1.00, thereby assuming that these constructs are identical. This constrained model's χ^2 is compared to the original model's χ^2 where the correlation between the same two constructs was estimated freely. Since the difference in degrees of freedom between the two models is 1, a difference in χ^2greater than 3.84 suggests

that the two constructs are statistically significant at level .05. The better model will be the one in which the two constructs are viewed as distinct, yet correlated factors (Segars 1997). Finally, a third, more rigorous test suggested by Fornell and Larcker (1981) can be employed. This test compares the average variance extracted (AVE) to the squared correlations between all pairs of constructs (Bagozzi and Phillips 1982). Discriminant validity is achieved if the items share more common variance with their respective constructs than any variance that construct shares with other constructs. Therefore, a construct's AVE should be higher than the squared correlation between that construct and any other construct.

We employed all three techniques in this study. Examining the freely estimated correlations (Table 3) between the constructs adequately demonstrates discriminant validity. Indeed, the highest correlation between any two constructs has a value of .60 with an error term of .04. This means that the correlation value is in the interval (.60 ± *t* (.04)), where *t* is the *t*-value. With confidence 95% the highest value of the correlation is in the interval (.60 ± 2.576 (.04)), or between .50 and .70 – again, far from 1.00. We also performed the χ^2 difference test as described above (Table 3). For each model run with a fixed ϕ_{ij} the difference in χ^2 was in the hundreds – considerably greater than the cut-off value of 3.84 (the minimum χ^2 difference was 405.26). Therefore the second and more rigorous technique provided strong evidence for discriminant validity. This conclusion is corroborated by the third technique of testing discriminant validity, i.e. the findings that the squared correlations between all latent constructs were significantly less than the corresponding AVE estimations. The highest squared correlation has a value of .36 between Internet usage and trust (IU and T), with corresponding AVEs at .61 and .81, respectively.

	IU	**PC**	**PI**	**T**	**PV**	**AC**
IU	.89					

	[.61]					
PC	-.42 (.05) **[479.94]**	.91 [.68]				
PI	.46 (.05) **[405.26]**	-.25 (.06) **[499.08]**	.87 [.69]			
T	.60 (.04) **[351.83]**	-.37 (.05) **[747.14]**	.46 (.05) **[425.05]**	.93 [.81]		
PV	-.14 (.04) **[760.55]**	.38 (.05) **[653.56]**	-.18 (.06) **[516.2]**	-.32 (.05) **[783.54]**	.92 [.69]	
AC	.20 (.06) **[675.64]**	.11 (.06) **[693.12]**	.20 (.06) **[514.38]**	.17 (.05) **[687.71]**	.15 (.06) **[686.28]**	.89 [.73]

Table 3. Latent Variable Statistics (correlations and error terms () (off-diagonal terms), composite reliabilities and average variances extracted [] (diagonal terms). On the line below each correlation, in brackets and in bold, are shown χ^2 differences between the fixed and free solution for the respective pair of constructs).

Reliability. The Squared Multiple Correlations (R^2) of the observed variables provide estimations of their reliability (Bollen 1989), the degree to which the indicators measure the construct in a consistent manner and are free from random error. High R^2 (close to 1.0 and not less than .5) indicate that the items share substantial variance and therefore provide evidence of acceptable reliability. Table 2 lists the R^2 of all the items in this study and the R^2 for most of them are high.

Another measure of the internal consistency is composite reliability. It is reported that, compared to Cronbach's alpha which provides a lower bound estimate of the internal consistency, the composite reliability is a more rigorous estimate for the reliability (Chin and Gopal 1995). A composite reliability greater than .5 would indicate that the variance captured by the measures is greater than the one captured by the errors (Bagozzi 1980). The recommended values for establishing strong reliability are above .80 (Koufteros 1999). The AVE estimates provide a complimentary measure to the composite reliability (Fornell and Larcker 1981). Composite reliability as well as AVE of the constructs in this study are given in Table 3. The

lowest composite reliability is .87 whereas the rest are in the range of .9. All the estimates of AVEs are above .6. The high values of both estimations provide further evidence of reliability of the scales.

Model Fit. In the most general terms, CFA generates multiple indices and metrics to assess the model fit. That is, the extent to which the observed covariance matrix (the covariances between the item measures as collected from data) "fits" the "model" matrix (the set of covariances generated through maximum likelihood estimation as a result of the specified model) (Stewart and Segars 2002). The most common fit indices are shown in Table 4 along with the referenced literature. In Table 4 the values in column labeled Model 2 correspond to the fit indices of the measurement model. The CFA model resulted in a converged, proper solution with a low χ^2 per degree of freedom and a reasonable fit. Besides the adequate model fit, it is worth noting that no significant error correlation terms were found that, if allowed to be estimated, would yield a better fit model. Collectively, the data from the model fit indices, factor loadings, and squared multiple correlations suggest that the indicators account for a large portion of the variance of the corresponding latent construct and therefore provide support for the validity of the measures. Only after the measurement model was finalized did we test the hypothesized model by employing the LISREL structural model.

Structural Equation Models (SEM)

The covariance structure model, as defined by the terminology of Joreskog and Sorbom (1993), consists of two parts: the measurement model (sometimes referred as CFA stage), and the structural model (also known as SEM stage). While the measurement model's purpose is to assess the measurement properties of the observed variables with respect to their underlying (hypothesized) latent variables, the structural model specifies the causal relationships among the

constructs. It is employed to indicate direct and indirect causal effects and the amount of unexplained variance (Anderson and Gerbing 1982).

Our structural model tests the relationships of the following mediating variables: trust, privacy concerns, and interest. Perceived ability to control and perceived vulnerability are the antecedents to these mediating variables. In SEM terms, the exogenous variables are perceived vulnerability (PV) and perceived ability to control (AC), and the endogenous variables are privacy concerns (PC), trust (T), personal interest (PI), and Internet use (IU).

The first structural model (Model 1) tested the hypothesized relationships. Only the structural parameter estimates which represent the hypothesized relationships were allowed to be evaluated and the others were held fixed. While the model fit indices presented a good model fit for Model 1, further analysis of the data based on the modification indices revealed additional relationships that were not hypothesized but were statistically significant. Based on these newly discovered relationships, a second model, Model 2, was further tested.

In Model 2 (shown in Figure 2) all structural parameter estimates were allowed to be evaluated, including those not hypothesized. There is an empirical and exploratory justification to consider a model that deviates from the hypotheses of the study. In seeking a model that best fits the data and comparing it to the hypothesized model, further validation of the hypothesized model is achieved through exploring the differences of the model fit indices between the two models. Thus a model that is different from the hypothesized model may be found and provide a better fit with the data (Stewart and Segars 2002). In Model 2, we allowed for all structural parameter estimates to be evaluated, however some were not statistically significant (low t-values). In the interest of parsimony, the final Model 2 was estimated with these structural paths deleted from the model (Byrne 1998).

The results of fitting both structural models to the data indicate that both models have a good fit and that the difference between the χ^2 of both models is slight (Table 4). The dependence of χ^2 on the sample size and degrees of freedom is widely understood (Bentler and Bonett 1980). χ^2 has been recognized as an inappropriate test for large sample sizes and must be interpreted with caution. Other measures of fit, including χ^2 per degree of freedom, which need to be considered in the model fit assessment are also shown in Table 4.

Both Model 1 and Model 2 resulted in an acceptably low χ^2 per degree of freedom ratio. All other indices introduced to assess model fit were in the acceptable range and above the recommended values. The results of the structural model estimation indicate a good fit of the data with the models, with Model 2 exhibiting slightly higher fit indices. As seen in Table 4, χ^2 for Model 1 is 315.25, with 179 degrees of freedom. χ^2 for Model 2 is 291.6, with 174 degrees of freedom. For the five degrees of freedom difference, a χ^2 greater than 19.2 would mean that the models have statistically significant χ^2 difference at level .05.

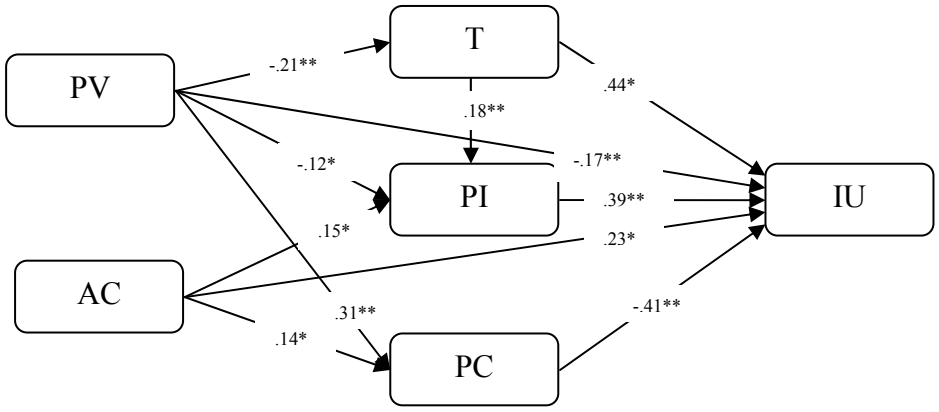

Figure 2. Structural Equation Model 2. * = p<.05; ** = p<.01.

Goodness of Fit Measures	Good Model Fit Recommended	Model 1 Values	Model 2 Values

	Ranges		
Chi-Square (d.f.)	Low, but is dependent on sample size	315.25 (179) p<.001	291.6 (174) p<.001
Normed Chi-Square/degree of freedom	< 2.0	1.76	1.67
NFI - Normed Fit Index	>.90	.94	.94
NNFI – Non-Normed Fit Index	>.90	.97	.97
CFI - Comparative Fit Index	>.90	.97	.98
IFI - Incremental Fit Index	>.90	.97	.98
RFI - Relative Fit Index	>.80	.93	.93
GFI - Goodness of Fit Index	≈.90	.92	.93
AGFI - Adjusted Goodness of Fit Index	>.8	.90	.91
PGFI - Parsimony Goodness of Fit Index	>.5	.72	.70
RMR – standardized Root Mean Square Residual	<.05	.05	.041
RMSEA-Root Mean Square Error of Approximation	<.08	.046	.042

Table 4: Goodness of Fit Assessments for Model 1 and Model 2.

Discussion And Limitations

Along with the improved fit indices, the findings indicate that this study's data fit the expanded Model 2 better than the hypothesized Model 1. These new results need to be verified by further research and additional evaluation to ensure they do not capitalize on chance. The findings reported in the previous section suggest qualified support for most of the hypothesized relationships. The overall Goodness of Fit Index for the second order model was very good at .93. This also suggests that the causality of the constructs tested in the structural model is adequate and establishes the nomological validity of the model. (The standardized path coefficients in the following discussion are taken from Model 2 as given in Figure 2.)

The first hypothesis focused on the relationships between privacy concerns and Internet use. The relatively large path coefficient (-.41 at level .01) indicates the significant role privacy concerns play with respect to e-commerce Internet use and thus supports the hypothesis.

The second hypothesis addressed the positive relationship between privacy concerns and perceived vulnerability. The strong relationship between the two constructs (.31 at level .01) confirms previous findings as well as our hypothesis that perceived vulnerability significantly contributes to greater privacy concerns.

The third hypothesis stated that there would also be a direct negative relationship between perceived vulnerability and Internet use. Indeed, the data suggested support for this relationship in the hypothesized direction (-.17 at level .01). This suggests that individuals who perceive vulnerability in submitting personal information over the Internet will refrain from engaging in e-commerce transaction.

The fourth hypothesis focused on the relationship between perceived ability to control and privacy concerns. The path coefficient of .14 (at level .05) indicates that there is a statistically significant relationship between the perceived ability to control and privacy concerns. However, the results indicate that the relationship is not in the hypothesized direction[2]. The data suggest that greater control over information is related to greater privacy concerns. This surprising result warrants further investigation. Moreover, while the direct effect of this relationship is positive, the indirect effect is -.09 (i.e., the composite relationships of all indirect paths from perceived control to privacy concerns following the procedures for assessing structural models (Bollen 1989)), in the hypothesized direction and statistically significant at level .01. Thus the total effect indicated cancellation of the direct and indirect effects and yielded a non-statistically significant value of .05 (the relationships' indirect and total effects which were in the same directions as the direct effects are not reported elsewhere in this paper but are available from the authors).

[2] In an earlier report of this study we indicated a relationship in the hypothesized direction. However, more comprehensive and meticulous examination of the data as well as the direct, indirect, and total effects of this particular relationship revealed a relationship in the reverse direction from the hypothesized.

Because control of transactions is embedded in the definition of privacy, this finding has to be addressed with great caution and cannot be ignored because of the strong model validity and fit.

One possible explanation for this result is that our measures for controlling information may have captured need for control rather than existing perceived ability to control information. Arguably, a greater need for control could reflect greater privacy concerns and thus a positive relationship between the two constructs. On the other hand, a greater sense of having the ability to control information measures would reduce privacy concerns and thus reflect a negative relationship. Future research should consider this distinction.

The fifth hypothesis, which focused on the relationship between perceived ability to control and Internet use, was supported (.23 at level .01) in the hypothesized direction. The data show that perceived control over personal information is positively related to Internet use. This finding suggests that ability to control information is a more important antecedent to Internet use compared to privacy concerns, which was the focus of the fourth hypothesis.

The sixth, seventh and eight hypotheses addressed relationships involving trust. The sixth hypothesis focused on the relationship between perceived vulnerability and trust. The data supported this hypothesis (-.21 at level .01). The seventh hypothesis focused on the relationship between perceived ability to control and trust. However, the data did not support this relationship. The path coefficient of .09 was not statistically significant (non-significant path coefficients are not shown in the results provided in Figure 2.) On the other hand, the indirect effect between perceived control and trust was significant. The coefficients for indirect effects (.14 at level .01) and for total effect (.23 at level .01) provide support for the strength of these indirect relationships. The lack of a direct relationship and the presence of an indirect relationship may point to the mixed role of the perceived ability to control information and

warrants further attention. The eighth hypothesis focused on the relationship between trust and Internet use. This hypothesis was supported with a positive path coefficient of .44 (at level .01), which was the strongest relationship in our model and is consistent with previous research that emphasizes the important role that trust plays in successful e-commerce transactions.

The ninth hypothesis predicted a positive relationship between interest in obtaining information, products, or services and Internet use. The data supported this relationship (.39 at level .01). Greater interest is related to greater Internet use. It should be noted that the interest construct measures a particular aspect of the personal interest, that is, to what extent personal interest outweighs to the user's intent to suppress his or her privacy concerns. Therefore, this finding suggests that Internet vendors should focus on providing goods and services of high personal interest to the customer in order to develop e-commerce.

The final hypothesis focused on the overall relationships among the various antecedents to Internet use. In particular, this hypothesis addressed the possible trade-offs between privacy concerns and other factors that might mitigate these concerns. To interpret the results of the structural equation model with respect to this hypothesis, two arguments need to be advanced about the relative strengths of the different relationships in the model. First, the magnitudes of the path regression coefficients are indicators of the relative strength of the relationship between any two given constructs in the model (Bollen 1989, Byrne 1998). Second, the completely standardized path coefficients are well suited for comparing the relative contributions to the explained variance (Bagozzi 1980). Therefore, the comparison of the relationships is theoretically and empirically justified and can illuminate the concept of the trade-off dynamics involving user interaction with websites.

The largest path coefficient in magnitude, shown in Model 2 (Figure 2), is between trust and Internet use (.44). This suggests that trust plays a central and important role in the decision to submit personal data to an Internet vendor. These results lend support to the argument that certain researchers, such as Culnan and Armstrong (1999), have made, that organizations requesting information from individuals must create a willingness to disclose information. Since there is a risk in disclosure, efforts to build trust ought to mitigate risk and encourage individuals to disclose information. The same prescription applies to organizations that hope to engage individuals in e-commerce or support more conventional distribution channels.

The findings further suggest that the three factors of trust, privacy concerns, and personal interest are similar in magnitude in their respective relationships with Internet use, with trust being the strongest. This suggests that personal interest alone is not a sufficient predictor of Internet use. That is, if trust and ability to control information are not factors in the "privacy calculus", successful completion of e-commerce transactions requiring personal data submission will not occur. Perceived vulnerability and privacy concerns may override user intentions, motivated by interest only, to conduct transactions over a web site. In sum, it is not sufficient for vendors to target only users' interests (i.e., through user-friendly and attractive web sites, lucrative marketing incentives, quality products and services, etc.) to influence them to disclose necessary personal information required to conduct e-commerce transactions. Online vendors need to focus on building trust in their consumers, mainly through employing fair information practices (Culnan and Armstrong 1999).

The combined path coefficients between privacy concerns and Internet use (-.41) and between perceived vulnerability and Internet use (-.17) constitute a significant negative influence in the decision to disclose personal information. On the other hand, the combination of the

relationships between trust and Internet use (.44), personal interest and Internet use (.39), and ability to control and Internet use (.23) offsets the negative concerns and positively influences user willingness to disclose personal information. Thus, the data supported hypothesis ten, which focused on the competitive and simultaneous influence of Internet use antecedents.

Three more relationships proved statistically significant in our expanded model (Model 2) that were not hypothesized and considered in the theoretical section. First, there is a significant positive relationship between trust and personal interest (.18 at level .01). A second relationship was also positive, namely between perceived ability to control and personal interest (.15 at level .05). And, there was a statistically significant relationship between personal interest and perceived vulnerability (-.12 at level .05). The centrality of personal interest in this combination suggests that personal interest does not merely influence Internet use. Rather than competing with the trust, ability to control information, and perceived vulnerability in the decision to use the Internet, personal interest influences other antecedents. It complements trust and ability to control information and it mitigates perceived vulnerability. Thus, personal interest is involved in a complex nomological network.

The theoretical roots of these relationships can be found in social cognitive theory. Bandura (1977) links trust and an individual's experience of heightened interest and motivation to engage in interaction with a trusted party. Consistent with this theory, as well as with the concept of intrinsic interest and motivation for certain behaviors, entities who are trusted because they are consistent and competent are more likely to be considered as objects of emulation, leadership and interaction (Higgins and Sorrentino 1990, Markus and Katayama 1991). Social and personality psychologists have identified the major factors that affect social behavior in the so called the BUCET framework of motives: belonging, understanding, controlling, enhancing self,

and trusting others (Bandura 2001, Fiske et al. 2001). Both control and trust are factors in the BUCET framework, which explains the relationships observed in our model.

In the context of IS research, to the best of our knowledge these relationships have not been addressed. It is, however, rational to expect the principle of social cognitive theory to apply to the trust-control-interest relationship in the realm of information systems and consumer-vendor interaction. Indeed, if one trusts a web vendor, the level of one's interest and motivation to interact with that vendor and benefit from what is offered on the web site may be enhanced. If one is confident that he or she has control over the information he or she submits to the vendor, the level of interest in engaging with the vendor and benefiting from the interaction would be expected to rise. Similar arguments can be made with respect to the negative relationship between perceived vulnerability and the personal interest. This area deserves further attention in future research.

An important limitation of our study is that we neither distinguished nor incorporated need as a motivation distinct from interest that may influence Internet use. The items measuring interest are more related to trade-off calculations than to intrinsic motivation. Motivation related to need may be based on the lack of alternative sources for goods, services or information. Motivation based on interest may be more closely associated with an interaction between preference and convenience, or similar constructs, which are distinct from need. Future investigations ought to account for this lapse.

Finally, attention needs to be given to the measures used for the constructs of trust and ability to control in privacy research. As pointed out in the theoretical framework, trust is a multidimensional construct and many nuances have not been captured in the items used in our study. Our measures of trust were related to reliability and competence because they were more

cognitive than other measures such caring and openness, which are more affective. The influence of previous experience on trust development (Miyazaki and Fernandez 2000, Ackerman et al. 1999) has also not been addressed in our study. Perhaps there are other dimensions of trust that are also related to Internet use and have not been captured by our unidimensional approach to trust. Since trust appears to play such a central role, we need a greater understanding of the dimensions of trust that are salient to privacy concerns and Internet.

As with most empirical studies, the sample size and spectrum of respondents is a limitation. Even though we made a concerted effort to include a range of different individuals representing different social groups of Internet users, the sample is limited to a certain geographical region of USA. A statistically random sample would have increased confidence in our results.

References

Ackerman, M. S., L. F. Cranor, J. Reagle. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proc. of the First ACM Conference on E-commerce, EC'99*.

Anderson, J. C., S. W. Gerbing. 1982. Some methods for respecifying measurement models to obtain unidimensional construct measurement. *J. of Marketing Res.* **19**(1) 453-460.

Bagozzi, R. P. 1980. *Causal modeling in marketing*. Wiley, New York.

Bagozzi, R. P., L. W. Phillips. 1982. Representing and testing organization theories: A holistic construal *Admin. Sci. Quart.* **27**(3) 459-489.

Bagozzi, R. P., Y. Yi. 1988. On the evaluation of structural equation models, *J. of Acad. Marketing Sci.* **16**(1) 74-94.

Bandura, A. 1977. *Social Learning Theory.* Prentice-Hall, Englewood Cliffs, N.J.

Bandura, A. 2001. Social cognitive theory: An agentic perspective. *Ann. Rev. of Psychology* **52** 1-26.

BCG, Boston Consulting Group 1998. Shop.org/BCG Survey of Online Customers, www.bcg.com

Bentler, P. M., D. G. Bonett. 1980. Significance tests and goodness of fit in the analysis of covariance structures. *Psych. Bull.* **88**(3) 588-606.

Bies, R. J. 1993. Privacy and procedural justice in organizations, *Social Justice Res.* **6**(1)69-86.

Bollen, K. A. 1989. *Structural Equations with Latent Variables*. Wiley, New York, N.Y.

Budnitz, M. E. 1998. Privacy protection for consumer transactions in electronic commerce: Why self-regulation is inadequate *South Carolina Law Rev.* **49** 847-886.

Byrne, B. M. 1998. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*, Lawrence Erlbaum, N.J.

Cespedes, F. V., H. J. Smith. 1993. Database marketing: new rules for policy and practice. *Sloan Management Rev.* **34** 7-22.

Chin, W., A. Gopal. 1995. Adoption intention in GSS: Importance of beliefs, *Data Base Adv.* **26** 42-64.

Clarke, R.A. Information Technology And Dataveillance. 1998. *Comm. of the ACM* **31** 498-512.

Culnan, M. J. 1993. "How did they my name?" An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quart.* **17**(3) 341-363.

Culnan, M. J. 2000. Protecting privacy online: Is self-regulation working? *J. of Public Policy & Marketing* **19** 20-29.

Culnan, M. J., P. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Sci.* **10(**1) 104.

Derlega, V. J., A. L. Chaikin. 1977. Privacy and self-disclosure in social relationships. *J. of Social Issues* **33** 102.

Etzioni, A. 1999. *The Limits of Privacy,* New York, Basic Books.

Fiske, D., Schacter, S. , Zahn-Waxler, C. (Eds). 2001. *Ann. Rev. of Psychology* **52** 1.

Fornell, C., D. F. Larker. 1981. Evaluating structural equation models with unobservable measurement error *J. of Marketing Res.* **18** 39-50.

FTC. 1999. Self-Regulation and Privacy Online. *Report to Congress*

Fusilier, M. R., W. D. Hoyer. 1980. Variables affecting perceptions of invasion of privacy in a personnel selection situation, *J. of Applied Psychology* **65** 623-626.

Gefen, D., D. W. Straub. 2002. Managing user trust in B2C e-services. *eService J.* **2** 1.

Glazer, R. 1991. Marketing in an information-intensive environment: Strategic implications of knowledge as an asset, *J. of Marketing* **55** 1-20.

Gofmann, E. 1963. *Stigma: Notes on Management of Spoiled Identity*. Englewood Cliffs, N.J., Prentice Hall.

Goodwin, C. 1991. Privacy: Recognition of a consumer right. *J. of Public Policy & Marketing* **10** 149.

Greenman, C. 1999. On the Net, curiosity has a price: Registration. *New York Times,* December 23, 1999.

Gundlach, G.T., P.E. Murphy. 1993. Ethical and legal foundations of relational marketing exchanges. *J. of Marketing* **57**(4) 35-46.

Hart, P., C. Saunders. 1997. Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization Sci.* **8**(1) 23.

Higgins. E., R. Sorrentino (Eds.). 1990. *Handbook of Motivation and Cognition: Foundations of Social Behavior* (Vol. 2, pp. 53-92). New York: Guilford.

Hoffman, D.L., T.P. Novak, M.A. Peralta. 1999. Building consumer trust online. *Comm.ACM* **42**(4) 80-85.

Johnson, C., 1974, Privacy as personal control. In *Man-Environment Interactions: Evaluations and applications,* Washigton, D.C.: Environmental Design Research.

Jones, M. G. 1991. Privacy: A significant marketing issue for the 1990s. *J. of Public Policy and Marketing* **10** 133.

Joreskog, K. , D. Sorbom. 1993. *LISREL VIII. Scientific Software*, Chicago, IL.

Kelvin, P. 1973. A social-psychological examination of privacy *British J. of Social Clinical Psychology* **12** 248-261.

Kling, R., J. P. Allen. 1996. How the marriage of management and computing intensifies the struggle for personal privacy, in Lyon, D. and Zureik E. (Eds.) *Computers, Surveillance and Privacy*, Minneapolis: The University of Minnesota Press, 104-131.

Koufteros, X. A. 1999. Testing a model of full production: a paradigm for manufacturing research using structural equation modeling. *J. of Operations Management* **17** 467-488.

Laufer, R.S., M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *J. of Social Issues* **33** 22-42.

Lee M., E. Turban. 2001. Trust in b-to-c electronic commerce: a proposed research model and its application. *International J. of Electronic Commerce* **6** 75-91.

Louis Harris and Associates, Inc. and A. Westin. Dimensions of privacy: A national opinion research survey of attitudes toward privacy, Galrland Publishing, Inc., New York, NY 1981.

Markus, H., S. Katayama. 1991. Culture and the self: Implications for cognition, emotion, and motivation. *Psych. Rev.* **98** 224-253.

Margulis, S. T. 1977. Conceptions of privacy: current status and next steps. *J. of Social Issues* **33** 5-10.

Mason, R.O. 1986 Four ethical issues of the information age *MIS Quart.* **10**(1) 4-12.

Mayer, R., J. Davis, F.Schoorman. 1995. An integrative model of organizational trust. *Acad. of Management Rev.* **20**

McCrohan, K. F. 1989. Information technology, privacy, and the public good. *J. of Public Policy and Marketing* **8** 265-278.

McKnight, D. H., V. Choudhury, C. Kacmar, 2002. Developing and validating trust measures for e-commerce: An integrative topology. *Inform. Systems Res.* **13** 334-359.

Milberg, S. J., S. J., Burke, H. J. Smith, E.A. Kallman. 1995. Values, personal information privacy, and regulatory approaches. *Comm. of the ACM* **38** 65-74.

Milberg, S.J., H. J. Smith, S. J. Burke. 2000. Information privacy: Corporate management and national regulation. *Organization Sci.* **11** 35-37.

Milne, G. R. 2000. Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *J. of Public Policy & Marketing* **19** 1.

Milne, G. R., M. Boza. 1998. *A Business Perspective on Database Marketing and Consumer Privacy Practices*, (Cambridge, MA: Marketing Science Institute).

Milne, G. R., M. E. Gordon. 1993. Direct mail privacy-efficiency trade-offs within an implied social contract. Framework *J. of Public Policy and Marketing* **12**(2) 206.

Miyazaki, A.D., A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. *J. of Public Policy & Marketing* **19** 54-63.

Morgan, R. M., S.D.Hunt. 1994. The commitment-trust theory of relationship marketing. *J. of Marketing*, **58** 20-39.

Mullen, M. R., G. R. Milne, N. Didow. 1996. Determining cross-cultural metric equivalence in survey research: a statistical test, *Advances in International Marketing*, **8** 145-157.

Nowak, G. J., Phelps, J. 1992. Understanding privacy concerns: An assessment of consumers' information related knowledge and beliefs. *J. of Direct Marketing* **6** 28-39.

Nowak, G. J., Phelps, J. 1995. Direct marketing and the use of individual-level consumer information: Determining how and when privacy matters. *J. of Direct Marketing* **9** 46-60.

O'Brien, T. 2000. Aided by Internet, identity theft soars, *The New York Times,* April 3.

Petty, R. D. 2000. Marketing without consent: Consumer choice and costs, privacy, and public policy. *J. of Public Policy & Marketing* **19** 42-57.

Phelps, J., Nowak, G. J., Ferrell, E. 2000. Privacy concerns and consumer willingness to provide personal information. *J. of Public Marketing* **19** 27-44.

Rindfleish, T. C.1997. Privacy, information technology, and health care. *Comm. of the ACM* **40** 92-100.

Rousseau, D., Sitkin, R. Burt, R., Camerer, C., 1998. Not so different after all: a Cross-discipline view of trust. *Acad. of Management Rev.* **23** 393.

Saunders, K., Zucker, B. 1999. Counteracting identity theft in the information age: identity theft and assumption deterrence Act. *Cornell J. of Law and Public Policy* **8(**3).

Segars, A. H. 1997. Assessing the unidimensionality of measurement scales: A paradigm and illustration within the context of information systems research. *Omega* **25** 107.

Segars, A. H., V. Grover. 1993. Re-examining perceived ease of use and usefulness: A Confirmatory Factor Analysis. *MIS Quart.* **17** (4) 517-529.

Sheehan, K., M. Hoy. 2000. Dimensions of privacy concern among online consumers. *J. of Public Policy & Marketing,* 19, 62-75.

Shils, E.1966. Privacy: its constitution and vicissitudes. *Law and Contemporary Problems* **31** 281.

Smith, H. J. 1993. Privacy policies and practices: Inside the organizational maze. *Comm. of the ACM* **36** 105-122.

Smith, H. J., S. J. Milberg, S.J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* 167-196.

Stewart, K.A., A.H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Inform. Systems Res.* **13(**1) 36-49.

Stone, E. F., H. G. Gueutal, D. B. Gardner, S. McClure. 1983. A field experiment comparing information-privacy value, beliefs, and attitudes across several types of organizations. *J. of Applied Psychology* **68** 459-468.

Stone, E. F., D. L. Stone. 1990. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms in K.M. Rowland and G.R. Ferris (Eds.), *Research in Personnel and Human Resources Management*, **8**, Greenwich, CT: JAI Press, 349-411.

Sweat, J. 2000. Privacy paradox: Customers want control – and coupons, *Informationweek* April, **781**, 52.

Thomas, R. E., V. G. Mauer. 1997. Database marketing practice: Protecting consumer privacy. *J. of Public Policy and Marketing* **16** 147-155.

Tolchinsky, P. D, M. McCuddy, J. Adams, D. C. Ganster, R. Woodman, H. L. Fromkin. 1981. Employee perceptions of invasion of privacy: A field simulation experiment. *J. of Applied Psychology* **66** 308-313.

UCLA Internet Report, 2000, 2001, 2002, Surveying the digital future, www.ccp.uc

Wang, P., L. Petrison. 1993. Direct marketing activities and personal privacy. *J. of Direct Marketing* **7** 7.

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

Appendix I: Items and Scales

Latent Variable	**Item**	**5 point Lickert Scale Range** (midpoint is always Neutral)
Perceived Ability to Control (AC)	Rate the extent to which you agree with the following statements: **AC1:** I would only submit accurate and personal information at a website if the site allowed me to control the information I volunteer. **AC2:** I would only provide accurate and personal information at a website if the site allowed me to control the information they can use **AC3:** Being able to control the personal information I provide to a website is important to me.	Strongly disagree – Strongly agree
Perceptions of Vulnerability (PV)	What do you believe is the risk for regular Internet users due to the possibility that: **PV1:** Records of transactions could be sold to third parties **PV2:** Personal information submitted could be misused **PV3:** Personal information could be made available to unknown individuals or companies without my knowledge **PV4:** Personal information could be made available to government agencies.	Very low risk – Very high risk
Trust (T)	Rate the extent to which you agree with the following statements: **T1:** Internet websites are safe environments to exchange information with others. **T2:** Internet websites are reliable environments to conduct business transactions. **T3:** Internet websites handle personal information submitted by users in a competent fashion.	Strongly disagree – Strongly agree
Privacy Concerns (PC)	Indicate the extent to which you are concerned about the following: **PC1:** I am concerned that the information I submit on the Internet could be misused. **PC2:** I am concerned that a person can find private information about me on the Internet **PC3:** I am concerned about submitting information on the Internet, because of what others might do with it. **PC4:** I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.	Not at all concerned - Very concerned
Personal Interest (PI)	Rate the extent to which you agree with the following statements: **PI1:** I find that personal interest in the information I want to obtain from the Internet overrides my concerns of possible risk or vulnerability I may have regarding my privacy. **PI2:** The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns. **PI3:** In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.	Strongly disagree – Strongly agree

Internet Usage (IU)	To what extent are you using the Internet to do the following activities: **IU1:** Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information). **IU2:** Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites). **IU3:** Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software). **IU4:** Retrieve highly personal and password protected financial information (e.g., using websites that allow me to access my bank account or my credit card account).	Not at all – Very much

Appendix II: CFA Measurement model. Notation and symbolic, according to Joreskog and Soborn (1993).