Information Systems Research
Vol. 17, No. 1, March 2006, pp. 61–80
ISSN 1047-7047 | EISSN 1526-5536 | 06 | 1701 | 0061

informs

DOI 10.1287/isre.1060.0080
© 2006 INFORMS

An Extended Privacy Calculus Model for E-Commerce Transactions

Tamara Dinev, Paul Hart
Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, Florida 33431 {tdinev@fau.edu, hart@fau.edu}

While privacy is a highly cherished value, few would argue with the notion that absolute privacy is unattainable. Individuals make choices in which they surrender a certain degree of privacy in exchange for outcomes that are perceived to be worth the risk of information disclosure. This research attempts to better understand the delicate balance between privacy risk beliefs and confidence and enticement beliefs that influence the intention to provide personal information necessary to conduct transactions on the Internet. A theoretical model that incorporated contrary factors representing elements of a *privacy calculus* was tested using data gathered from 369 respondents. Structural equations modeling (SEM) using LISREL validated the instrument and the proposed model. The results suggest that although Internet privacy concerns inhibit e-commerce transactions, the cumulative influence of Internet trust and personal Internet interest are important factors that can outweigh privacy risk perceptions in the decision to disclose personal information when an individual uses the Internet. These findings provide empirical support for an extended privacy calculus model.

Key words: privacy calculus; trust; risk; e-commerce; LISREL
History: Cynthia Beath, Senior Editor; Laurie Kirsch, Associate Editor. This paper was received on August 18, 2003, and was with the authors $15\frac{1}{2}$ months for 4 revisions.

Introduction

The fact that privacy is a widely coveted and highly privileged value in American society reflects the importance of individualism in the country's philosophical foundations (Etzioni 1999). In recent years, the explosive growth of Internet use to obtain information, goods, and services has fueled debate and controversy about potential threats to privacy. While contemporary information systems provide clear efficiencies that allow firms to gather, process, and store consumer data, providing important marketing-related competitive opportunities, they also introduce risks for individuals who disclose personal information to retailers. Most polls reveal that consumers strongly value privacy (Westin 2001, UCLA 2000–2004). Yet, while privacy concerns are reported to be a major factor inhibiting e-commerce, sales over the Internet continue to increase. Economists and practitioners who refer to this paradox argue that consumers' actual behaviors may be different from their revealed privacy preferences. Either their behavior reflects lower privacy concerns than polls and research would suggest (Ackerman et al. 1999, Sweat 2000), or other factors mitigate privacy concerns.

The objective of our research is to address this paradox by attempting to better understand the predictors of a user withholding or surrendering personal information when using the Internet. In the following section, we develop a theoretical model that includes important antecedents related to the disclosure of personal information in the context of online transactions. The subsequent section describes data collection procedures, survey instrument validation, and model testing using structural equations modeling (SEM) with LISREL. In the last section, we discuss the contributions of this paper, which include empirical support for demonstrating that a number of factors are related to the intention to disclose personal information when using the Internet to conduct transactions. Identification of these antecedents should help Web retailers better address the challenge of supporting the confidence of those who seek to obtain information, products, and services. In turn, this should lead to an increase in e-commerce (Gefen et al. 2003).

Theoretical Framework

Over the last half of the past century, social scientists spent a considerable amount of effort in trying to understand the predictors of individuals' behavior. Numerous studies focusing on behavior related to information technology were based on the theory of reasoned action (TRA) (Ajzen and Fishbein 1980) and its later revision, the theory of planned behavior (TPB) (Ajzen 1988), that established a parsimonious framework for investigating behavioral intention and performance. From the earliest examples of this research (Davis 1989, Davis et al. 1989) to one of the more recent (Venkatesh et al. 2003), MIS researchers have tried to advance theoretical specification by testing numerous predictors of behavioral intention.

Our investigation follows the direction of this literature by specifying a model that focuses on two of the primary components of the TRA and TPB models, namely beliefs and behavioral intention, an approach that others have taken (e.g., McKnight et al. 2002). Specifically, we are interested in the beliefs that influence the behavioral intention to disclose the personal information necessary to successfully complete a transaction on the Internet.

Concurrently, our study attempts to gain a better understanding of the role that contrary beliefs play in an individual's intention to disclose personal information. Most empirical models have attempted to test the relative strength of noncontrary factors (e.g., shopping convenience, ecology concerns, customer relations, and product value) as predictors of e-commerce success (e.g., Torkzadeh and Dhillon 2002). However, we assume that the salient beliefs that influence the intention to disclose the personal information, which is required to successfully complete Internet transactions can be contrary, and that together the beliefs comprise a set of elements in a *calculus*, or decision process, in which the Internet user engages. The influence of one belief might override another to the extent that the resulting probability favors one behavioral intention over another. However, the strength of the overriding belief's influence does not eliminate the role or the importance of the contrary belief. In the theoretical model that we describe, contrary factors are included because it is possible for individuals to have strong beliefs about each one simultaneously.

The notion of a calculus as a cumulative antecedent to information disclosure in general has been addressed by a number of scholars in the past. Laufer and Wolfe (1977) argued that a *calculus of behavior*, accounting for situational constraints such as institutional norms of appropriate behavior, anticipated benefits, and unpredictable consequences (involving the presence of "computerized data banks [sic]," p. 37), is an important predictor of when and whether individuals would disclose personal information. They further argued that a crucial element of the calculus of behavior is that individuals are "often unable to predict the nature of that which has to be managed" (Laufer and Wolfe 1977, p. 37), which implicitly suggests the importance of personal beliefs in swaying behavioral intention.

Following Laufer and Wolfe (1977), Culnan and Armstrong (1999) argued that, in the more specific context of purchasing products and services, individual decision processes prior to the disclosure of personal information necessary to complete a transaction involve a privacy calculus. Specifically, when consumers are informed about the vendor's information practices and perceive the business as fair to them, they are more willing to consent to personal information disclosure. The research model we test herein can be viewed as an extension of Culnan and Armstrong's *privacy calculus*, in that we account for an individual's willingness to provide personal information with respect to Internet transactions specifically, rather than with respect to transactions with retailers in general.

Internet users' behavioral intentions should be consistent with expectancy theory, which holds that individuals will behave in ways that maximize positive outcomes and minimize negative outcomes (van Eerde and Thierry 1996, Vroom 1964). A comprehensive assessment of the *costs* and *benefits* related to information disclosure in a range of settings was addressed by Stone and Stone (1990). In focusing on consumer and retailer relationships in particular, Culnan and Bies (2003) argued that individuals will disclose personal information if they perceive that the overall benefits of disclosure are at least balanced by, if not greater than, the assessed risk of disclosure. Thus, they equated a cost-benefit analysis with the privacy calculus. They further argued that "a positive

net outcome should mean that people are more likely to accept the loss of privacy that accompanies *any* disclosure of personal information as long as an acceptable level of risk accompanies the benefits" (Culnan and Bies 2003, p. 327). The research undertaken here should shed light on the paradox that, while the disclosure of personal information is a major inhibitor of business-to-consumer (B2C) e-commerce, the latter nonetheless continues to increase. In the next section of this paper we provide the theoretical justification for our proposed model.

Behavioral Intention

The dependent variable representing behavioral intention in our model is the willingness to provide personal information to transact on the Internet. Personal information refers to the type of information necessary to conduct an online transaction. This includes credit card numbers and identifiers and any other information that might be required to purchase goods, information, or services or to register at websites, such as home addresses and other contact information, and possibly customer or product preferences. This construct differs from similar constructs used in prior research in two important ways. First, it refers not to only to the intention to transact on the Internet (e.g., Gefen et al. 2003, Jarvenpaa et al. 2000, Pavlou 2003, Pavlou and Geffen 2004), but also the willingness to provide personal information as a condition for transacting (McKnight et al. 2002). This construct is consistent with the attempt to better understand the relationship between the information-related antecedents specified in the theoretical model and the behavioral intention to conduct online transactions. Second, this construct refers to intended use of the Internet in general rather than specific websites in particular, which is an operationalization of intention to transact used in a number of other e-commerce studies (e.g., Gefen et al. 2003, Jarvenpaa et al. 2000, Pavlou 2003, Pavlou and Gefen 2004). Again, this is consistent with the focus of our study that seeks to better understand the influence of beliefs on willingness to disclose information in an online environment, rather than perceptions related to particular features of certain websites or particular website vendors and their influence on transaction intentions.

Following Culnan and Bies's (2003) admonition, the belief antecedents we describe focus on costs and benefits, or as we call these polarities, *risk beliefs* and *confidence and enticement beliefs*. Figure 1 shows the proposed hypotheses and Table 1 indicates the constructs and their definitions.

Risk Beliefs

Risk has been defined as "the possibility of loss" (Yates and Stone 1992, p. 4) and is "an inherently subjective construct" (Yates and Stone 1992, p. 5; Chiles and McMackin 1996). Perception of risk can be related to the uncertainty caused by the possibility of the seller's opportunistic behavior that can result in loss for the consumer (Ganesan 1994). In the context of conventional transactions, there is a certain amount of risk involved for the consumer who, for example, may be uncertain about the quality or the durability of a product purchased. Familiarity with brands and

Figure 1 Hypothesized Relationships of the Extended Privacy Calculus Model

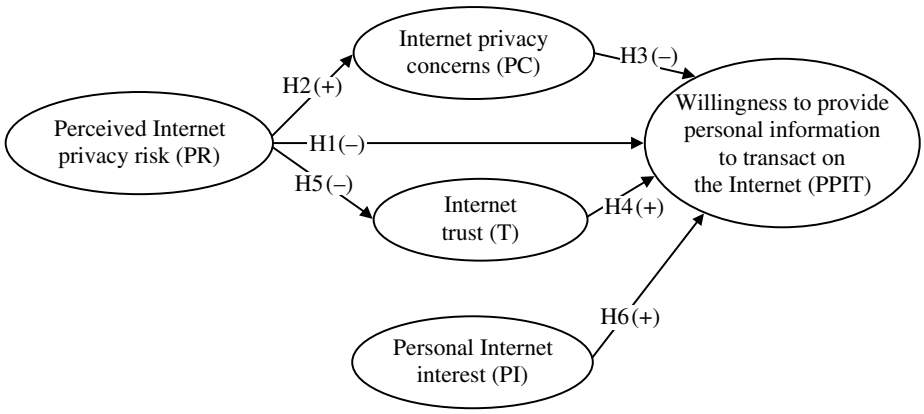


Table 1 Constructs in the Extended Privacy Calculus Model

Construct category	Construct	Acronym	Definition
Willingness to act	Willingness to provide personal information to transact on the Internet	PPIT	Willingness to provide personal information required to complete transactions on the Internet.
Risk beliefs	Perceived Internet privacy risk	PR	Perceived risk of opportunistic behavior related to the disclosure of personal information submitted by Internet users *in general*.
	Internet privacy concerns	PC	Concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent *in particular*.
Confidence and enticement beliefs	Internet trust	T	Trust beliefs reflecting confidence that personal information submitted to Internet websites will be handled competently, reliably, and safely.
	Personal Internet interest	PI	Personal interest or cognitive attraction to Internet content overriding privacy concerns.

assurances from salespeople mitigate the perception of risk in these conventional contexts. However, the more information technology has come to be used to facilitate transactions, the greater is the privacy risk associated with the requirement for personal information disclosure. There are few assurances in place to mitigate the perception of privacy risk that is based on the possibility of another's opportunistic acquisition and use of this personal information. However, Milne and Culnan (2004) reported that Internet users find privacy notices to be an important assurance, particularly when dealing with unfamiliar vendors.

A number of e-commerce studies tested models that included risk as an antecedent to intentions to conduct transactions. However, none of these studies accounted for the possible loss of personal information in their assessments of perceived risk; risk was measured either in more general terms or emphasized the possibility of economic loss rather than privacy loss. For example, Jarvenpaa et al. (2000) assessed risk perceptions in terms of the potential for economic loss in their study of specific bookstore and travel websites, and found negative relationships between perceived risk and willingness to buy from both types, but more so for the travel websites. In a related cross-cultural study, using the same measures but assessing only risk related to specific bookstore websites, Jarvenpaa et al. (1999) found a consistent negative relationship between perceived risk and willingness to buy among respondents in Australia and Israel. Using similar risk measures, Pavlou (2003) also found a negative relationship, although his research design incorporated specific respondent-selected websites. In another study, Pavlou and Gefen (2004) assessed risk in terms of economic loss in the context of a community of sellers in an online auction, and again found a negative relationship with intention to transact. These studies differ from more recent investigations, such as McKnight et al. (2002) and Malhotra et al. (2004), in which risk was assessed as the perceived uncertainty related to the disclosure of personal information online. The strength of the relationships in the McKnight et al. (2002), -0.28, and Malhotra et al. (2004), -0.63, studies compared to those in investigations mentioned above, for example Pavlou (2003), -0.11, or Pavlou and Gefen (2004), -0.20, suggest that perceived privacy risk might be a more influential factor than economic risk in dissuading individuals from conducting e-commerce transactions.

In our attempt to assess privacy risk, we account for the perceived risk of opportunistic behavior related to obtaining personal information submitted by Internet users. Sources of opportunistic behavior include selling to, or sharing information with, parties not involved in immediate transactions, such as third-party marketing firms, financial institutions (Budnitz 1998, FTC 1999) or government agencies (Preston 2004, Wald 2004). Privacy risk could also include the misuse of personal information, such as insider disclosure or unauthorized access and theft (O'Brien 2000, Rindfleisch 1997). A recent study by the Pew Internet & American Life Project examined Internet users' fears. The top ranking revealed that 84% of over 1,000 Internet users surveyed were concerned that businesses and people they did not know were getting personal information about them and their families (Fox 2000). The perception that third parties could use personal information in unintended ways or that

information might not be securely protected reflects the possibility that individuals might suffer the consequences of opportunistic behavior with respect to personal information submitted over the Internet. This perception of uncertainty in the Internet environment makes individuals hesitant to disclose personal information necessary to conduct e-commerce transactions. The behavioral intention not to provide information when perceptions of risk are high is consistent with expectancy theory's explanation that individuals are motivated to minimize negative outcomes.

Hypothesis 1. *A higher level of perceived Internet privacy risk is related to a lower level of willingness to provide personal information to transact on the Internet*.

Perceptions of risk concerning Internet websites should be directly related to privacy concerns. Both are risk beliefs, although the latter reflects an internalization of the possibility of loss. The former reflects a belief that amounts to an assessment of Internet websites in general. The latter is an assessment about what happens to the personal information that the user discloses on the Internet. Perceived risk and privacy concerns are closely related, but distinct, factors.

Privacy concerns are based on the Internet's technical capabilities and how companies can advance their own strategic purposes using IT investments. The growth of Internet use and recent heightened awareness about privacy issues have paralleled the evolution of scholarly interest in privacy concerns. Although researchers from social science and business disciplines have studied this issue—including researchers from psychology (Altman 1975, Laufer and Wolfe 1977), human resources (Stone and Stone 1990, Tolchinsky et al. 1981), sociology (Etzioni 1999), law (Rosen 2000), political science (Westin 1967), and marketing (Goodwin 1991)—interest among MIS researchers has been more recent and followed the growth of investments in IT (Culnan 1993, 2000; Culnan and Armstrong 1999; Culnan and Bies 2003; Malhotra et al. 2004; Mason 1986; Smith 1993; Smith et al. 1996; Stewart and Segars 2002). These investments over time have allowed companies to better gather, store, and analyze consumer information. In more recent years, the growth of the number of Internet users has broadened the extent of data collection. Increasingly sophisticated technologies such as data mining, which require a large amount of data from which consumer patterns can be extracted, have improved the capability of companies to profile and target specific individuals. While these advances have made it possible for firms to identify consumer preferences, develop better products, and improve customer relations (Glazer 1991, Kling and Allen 1996), those advances have also increased concern among consumers about access to their personal information and how it is used. Individuals are concerned that, without their knowledge, their personal information is available to an invisible network of information seekers.

As Culnan and Armstrong (1999) have noted, "in an absolute sense, individuals surrender a measure of privacy whenever they disclose personal information" (p. 109). Disclosing personal information over the Internet can increase privacy concerns because the technology introduces greater uncertainty about who has access to the information and how it is used. Privacy concerns are beliefs about who has access to information that is disclosed when using the Internet and how it is used. The greater the uncertainty about the access and use, the greater the privacy concerns. Individuals who perceive the Internet as an environment in which there is a risk of other parties' opportunistic behaviors should also have concerns about who has access to the personal information they themselves disclose.

Hypothesis 2. *A higher level of perceived Internet privacy risk is related to a higher level of Internet privacy concerns*.

Privacy concerns, in turn, should be related to the willingness to provide personal information to transact on the Internet. Findings described in a series of UCLA (2000–2004) reports bear this out, indicating that privacy concerns and the requirement to submit personal information are among the primary factors that discourage users from shopping online. Researchers found that only one out of three attempts to conduct online transactions was successfully completed; the failures were primarily due to the user's reluctance to submit personal information. Privacy concerns are the single most frequently cited reason by non-Internet users for declining to use the Internet (Westin 2001).

At the same time, it is not clear that companies are doing much to mitigate consumers' privacy concerns. Culnan and Armstrong (1999) found support for the notion that consumers would be more willing to disclose information if they knew who would have access to it and how it would be used. However, recent investigations of Internet site policy disclosures have shown that privacy policies and adherence to them vary across industries (Culnan 2000, Miyazaki and Fernandez 2000). These findings are consistent with research in other settings that question the viability of self-regulatory mechanisms governing the disclosure of privacy policies (Milberg et al. 1995, 2000).

The behavioral intention not to provide information when perceptions of privacy concerns are high is again consistent with expectancy theory's explanation that individuals are motivated to minimize negative outcomes.

Hypothesis 3. *A higher level of Internet privacy concerns is related to a lower level of willingness to provide personal information to transact on the Internet*.

Confidence and Enticement Beliefs

Confidence and enticement beliefs are related to the willingness to disclose personal information over the Internet. They do not necessarily eliminate risk beliefs, but they can override their influence on behavioral intention.

Trust is a confidence belief that can positively influence willingness to disclose personal information. Trust is a multidimensional construct (Gefen 2000, Gefen et al. 2003, Mayer et al. 1995, McKnight et al. 2002, Rousseau et al. 1998) and has been defined in numerous ways. Recent studies on e-commerce have incorporated trust in empirical models and have defined it as a set of specific beliefs about another party that positively influence an individual's intention to conduct online transactions. These beliefs embody the expectation that another party will not engage in opportunistic behavior. For example, Jarvenpaa et al. (2000) used a set of beliefs including the expectations that an online vendor would keep the best interests of the consumer and its promises to them in mind. They found that these beliefs were positively related to attitudes about the online vendor, which in turn influenced a willingness to make online purchases. Pavlou and Gefen (2004) found a direct positive relationship between a set of trust beliefs about a seller's reliability, honesty, and trustworthiness, and transaction intentions in using an auction website. Gefen et al. (2003) found a direct positive relationship between a set of trust beliefs (including a vendor's honesty, caring for customers, and predictability), and an individual's intention to disclose information to complete an online transaction. The variance in the specific trust beliefs used in these studies and others (Gefen 2000) is considerable. McKnight et al. (2002) advocate the use of the three factors of perceived trustworthiness proposed by Mayer et al. (1995), namely competence (or ability), benevolence, and integrity. They argued that most beliefs used in prior research cluster around these three factors. Furthermore, they found support for three distinct antecedents to trusting behavioral intentions (i.e., personal disposition to trust, institution-based trust, and trusting beliefs), with each containing dimensions of competence, benevolence, and integrity. Whereas the degree of specificity in the McKnight et al. (2002) model represents a significant contribution to clarifying the complexity of trust beliefs and intentions, their model makes it difficult to incorporate that model into our model, in which trust is only one of a number of proposed constructs.

In our model, we incorporate one of the antecedent constructs following McKnight et al. (2002), namely trusting beliefs. Trust is defined as a set of three beliefs that reflect confidence that personal information submitted to Internet websites will not be used opportunistically. These beliefs include competence, reliability, and safety. As we have noted earlier, the focus of our investigation is on Internet websites in general, rather than on beliefs in specific online vendors. Competence refers to the ability of the trustee to have the necessary expertise to perform the behavior expected by the trustor. It has been used frequently in a range of investigations from trust in managers (Gabarro 1987, McLain and Hackman 1999) to suppliers and vendors (Anderson and Narus 1990, Mishra 1996, Hart and Saunders 1998). Reliability clusters with integrity (which also included honesty and sincerity) in the McKnight et al. (2002) analysis. Reliability, the consistency between words and actions

(McGregor 1967), has been used in a number of studies, including investigations of trust between consumers and salespeople (Swan et al. 1988). Safety refers to the belief that information provided to the trustee will be kept safe or held in confidence. Some researchers have equated this belief with carefulness (Blakeney 1986, Gabarro 1987). Our assessment of trust did not include a benevolence belief; that may be a limitation of our work. However, to the extent that benevolence refers to beliefs about the trustee not acting opportunistically or manipulatively (McKnight et al. 2002, p. 338), we would argue that the belief that the trustee would hold information in confidence (i.e., safely) is at least related to benevolence.

Beliefs that Internet websites are reliable and safe environments in which to disclose information and that information will be handled in a competent fashion should increase the willingness of users to provide personal information. Our assessment of trust is a relatively complex construct because we measure not only the set of trust beliefs, but also the user's beliefs in the context of exchanging information and conducting business on the Internet. Higher trust should influence users to disclose personal information, reflecting a behavioral intention with anticipated positive outcomes.

Hypothesis 4. *A higher level of Internet trust is related to a higher level of willingness to provide personal information to transact on the Internet.*

The precise relationship between risk and trust has been discussed at length and is not as straightforward as one might expect. For example, Mayer et al. (1995) have made the following observation indicating the complexity of the relationship between these two constructs:

> There is no risk taken in the *willingness* to be vulnerable (i.e., to trust), but risk is inherent in the *behavioral manifestation* of the willingness to be vulnerable. One does not need to risk anything in order to trust; however, one must take a risk in order to engage in trusting action. The fundamental difference between trust and trusting behaviors is between a "willingness" to assume risk and actually "assuming" risk. Trust is the willingness to assume risk; behavioral trust is the *assuming* of risk. (Mayer et al. 1995, p. 724)

Notwithstanding this valuable insight, most research assumes that the need to form a trusting belief is based on the presence of some level of risk (Jarvenpaa et al. 2000, Tan and Thoen 2001). Researchers have also assessed the subjective interpretation of these realities (i.e., perceived beliefs) given the inherent difficulty in obtaining objective information (Pavlou 2003).

A lower level of perceived privacy risk should be related to a higher level of trust in the other party's competence, reliability, and safekeeping of personal information. Empirical evidence from prior e-commerce research supports the expectation of a negative relationship between these constructs (Jarvenpaa et al. 1999, 2000; Pavlou 2003).

Hypothesis 5. *A lower level of perceived Internet privacy risk is related to a higher level of Internet trust.*

Finally, personal interest is a belief that reflects a level of enticement to transact. Interest is an intrinsic motivation, a cognitive state or belief related to the self-fulfilling satisfaction derived from performing the activity, as distinct from an extrinsic motivation reflecting the force of behavior caused by an extrinsic outcome (Brief and Aldag 1977). The locus of causality in the former is internal, whereas in the latter it is external. Personal interest is an intrinsic motivation that can positively influence the willingness to disclose personal information necessary to complete online transactions.

Overall, there has been a longer and greater effort in studying extrinsic motivation related to technology acceptance. For example, numerous studies have consistently found that the usefulness of information technology is an important antecedent to intended IT use (e.g., Davis et al. 1989, Taylor and Todd 1995, Venkatesh and Davis 2000). The inclusion of intrinsic motivation (which has been captured as computer playfulness or perceived enjoyment) as a factor in technology acceptance models (TAM) has been considerably more recent (e.g., Teo et al. 1999; Venkatesh 1999, 2000). Interestingly, in two separate studies van der Heijden (2002, 2004) found perceived enjoyment to be a stronger predictor than perceived usefulness of particular websites.

Although intrinsic motivation has frequently been captured by computer playfulness and perceived enjoyment, these are not the only conceivable constructs that might reflect intrinsic motivation. We

would argue that personal interest is another. Following Webster and Martocchio (1992), who defined computer playfulness as "the degree of cognitive spontaneity in microcomputer interactions" (p. 204), we would define Internet personal interest as the degree of cognitive attraction to Internet interactions. Personal interest is an appropriate intrinsic motivation in this investigation because the Internet provides access to an incredibly wide range of information, goods, and services that might not otherwise be available or conveniently available to users. The Internet is an environment in which a wide range of subjects and products can be found to match a particular user's interest, so personal interest is a salient construct in a model that attempts to explain behavioral intention with respect to intended Internet use. This is consistent with the study's intention to better understand the relative strengths of contrary factors that influence the willingness to provide personal information to transact on the Internet.

Hypothesis 6. *A higher level of personal Internet interest is related to a higher level of willingness to provide personal information to transact on the Internet.*

Research Methodology and Results

Scale Development and Survey Administration

The research model was empirically tested using data collected with a survey that included items for the constructs specified in the model. We constructed the initial set of items by analyzing the literature and reflecting on the proposed theoretical model. Privacy concerns (PC) items were based on the instruments developed by Smith et al. (1996) and further refined by Culnan and Armstrong (1999). Internet trust (T) items were based on Cheung and Lee (2001) and Lee and Turban (2001). The items for personal interest (PI) and willingness to provide personal information to transact on the Internet (PPIT) were developed by the authors, who based them on theoretical definitions described above. The PI items were constructed to ensure that we captured significant rather than fleeting or merely transitory interest. We incorporated "overriding" or "greater than" terms to assess comparisons with contrary beliefs. This measurement approach was necessitated because our model focused on Internet use in general, rather than on specific websites; the latter would have allowed us to assess the need or desire for the products, services, or information offered by that website.

Two pilot tests were administered to undergraduate and graduate business students in a southeastern university. The changes made following the first pilot study were so substantial that a second pilot test was necessary. The sample size of each pilot test was 70. Following the second pilot study, several items were dropped and word changes were made, but no additional items were added. The final version of the items is provided in the appendix. All the items used a five-point Likert scale. The final survey was administered to a broad sample of individuals in the southeastern United States, including undergraduate and graduate students of a large university, employees of four public schools, one large and one small high-tech company, one banking institution, and three small retail and service businesses, a direct mailing to one neighborhood. Participation was voluntary and the respondents who chose to participate returned a completed survey in designated collection boxes. The response rate was 40% as measured by the ratio of the number of the completed surveys returned to the number of the surveys initially distributed. The final survey respondent profile (sample size 369) is given in Table 2. The demographic distribution reveals a diverse sample, comprising a wide range of age, employment, education, and race, with equal representation of genders.

Structural Equation Modeling—Measurement Model

Exploratory factor analysis (EFA) of the Internet privacy concerns and perceived Internet privacy risk (PR) constructs were reported in Dinev and Hart (2004). In that article, two dimensions of Internet privacy concerns were identified: privacy concerns of information finding (PCIF) and privacy concerns of information abuse (PCIA). Our analyses demonstrated that PCIF and PCIA are two distinct constructs, but that they display similar relationships with other constructs in a nomological net. For the purpose of this study, we used the PCIA construct, which we simply refer to here as PC. The Cronbach's α (Table 3) for all constructs were at or

Table 2 Descriptive Statistics of Survey Respondents ($N = 369$)

Race		Gender		Education	
White	193 (52.3%)	Male	172 (46.6%)	High school	11 (3.0%)
Black	64 (17.3%)	Female	197 (53.4%)	Associate degree	58 (15.7%)
Hispanic	65 (17.6%)			University student	192 (52.0%)
Asian	31 (8.4%)	Occupation		4-year college degree	67 (18.2%)
Native American	1 (0.3%)	Clerical	29 (7.9%)	Graduate degree	41 (11.1%)
Other	5 (1.4%)	Managerial	38 (10.3%)		
Undisclosed	10 (2.7%)	Professional	84 (22.8%)	Income	
		Homemaker	10 (2.7%)	<$20,000	79 (21.4%)
Age		Student	148 (40.1%)	$20,001–$40,000	113 (30.6%)
<20 years	13 (3.5%)	Other	44 (11.9%)	$40,001–$60,000	65 (17.6%)
21–30 years	245 (66.4%)	Undisclosed	1 (0.3%)	$61,001–$100,000	70 (19.0%)
31–40 years	73 (19.8%)			>$100,000	33 (8.9%)
41–50 years	28 (7.6%)				
>50 years	10 (2.7%)				

above 0.84, and the corrected item–total correlations were high for most of the items, indicating internal consistency of each construct's items.

The research model was tested through structural equation modeling (SEM) with LISREL. We used the two-step approach, as recommended by Anderson and Gerbing (1988) and Segars and Grover (1993) to first assess the quality of our measures through the measurement model (sometimes referred as the CFA stage), and then test the hypotheses through the structural model (also known as SEM stage; Joreskog and Sorbom 1993). The CFA stage was performed on the entire set of items simultaneously with each observed variable restricted to load on its a priori factor. Maximum likelihood estimations were employed for the model assessment. All the necessary steps in the measurement model validation and reliability assessments were conducted following Byrne (1998) and Gefen et al. (2000).

Unidimensionality and Convergent Validity. Table 3 provides the psychometric properties of the items. All the items exhibit high-factor loading λ's

Table 3 Confirmatory Factor Analysis Statistics

		Completely standardized latent construct loadings and error terms								
Latent variable	Item	PPIT $\alpha = 0.84$	PR $\alpha = 0.88$	PC $\alpha = 0.88$	T $\alpha = 0.91$	PI $\alpha = 0.86$	t-value	R^2	Construct reliability	AVE
PPIT	PPIT1	0.77 (0.05)					16.60	0.59	0.89	0.62
	PPIT2	0.68 (0.05)					14.12	0.46		
	PPIT3	0.89 (0.05)					20.51	0.79		
	PPIT4	0.72 (0.06)					15.32	0.52		
PR	PR1		0.77 (0.04)				16.98	0.60	0.92	0.69
	PR2		0.85 (0.04)				19.47	0.72		
	PR3		0.87 (0.04)				20.27	0.76		
	PR4		0.71 (0.04)				15.05	0.51		
PC	PC1			0.69 (0.05)			14.65	0.48	0.91	0.68
	PC2			0.84 (0.05)			19.14	0.70		
	PC3			0.92 (0.04)			22.09	0.84		
	PC4			0.77 (0.05)			16.93	0.59		
T	T1				0.90 (0.04)		21.81	0.81	0.93	0.81
	T2				0.85 (0.04)		19.91	0.72		
	T3				0.94 (0.03)		23.31	0.88		
PI	PI1					0.84 (0.04)	18.62	0.70	0.87	0.69
	PI2					0.82 (0.05)	18.12	0.67		
	PI3					0.83 (0.05)	18.27	0.68		

(most above 0.70) and high statistically significant *t*-values reflecting unidimensionality and convergent validity (Bollen 1989). In addition, the average variance extracted (AVE) for each construct is much higher than the recommended minimum value of 0.50 (Fornell and Larcker 1981). All items are significantly related to their specified constructs; the data support the convergent validity of the CFA model.

Discriminant Validity. Discriminant validity was assessed by testing whether the correlations between pairs of construct items (Table 4) were significantly different from unity (Anderson and Gerbing 1988). Three techniques were used (Joreskog and Soborn 1993, Bollen 1989, Mullen et al. 1996). First, we observed that the highest correlation between any two constructs had a value of 0.60 with an error term of 0.04, which is far from 1.00. Second, the χ^2 differences between the fixed and the free solutions for each pair of constructs were in the hundreds, much larger than the cut-off value of 3.84. Third, the squared correlations between all latent constructs (Table 4) were significantly less than the corresponding AVE. All the criteria adequately demonstrated discriminant validity of the model.

Reliability. The squared multiple correlations (R^2) of the items are listed in Table 3. Most of them are higher than 0.5, providing evidence of their reliability. Construct (composite) reliability and AVE, which are additional measures of internal consistency, were estimated and are shown in Table 3. The construct reliability indicates the percent variance in a measurement captured by the trait variance (Bagozzi 1980). Compared with the Cronbach's alpha, which provides a lower bound estimate of the internal consistency, the construct reliability is a more rigorous estimate for the reliability (Chin and Gopal 1995). The recommended values for establishing a tolerable reliability are above 0.70 (Werts et al. 1974, Gefen et al. 2000) and for strong reliability—above 0.80 (Koufteros 1999). The lowest composite reliability for our model is 0.87 and all estimates of AVEs are above 0.6, which provide further evidence of the scales reliability (Bagozzi 1980, Fornell and Larcker 1981, Koufteros 1999).

Model Fit. Only after the measurement model was finalized did we test the hypothesized model by employing the LISREL structural model. The fit indices reported in Table 5 show a converged, proper solution with a low χ^2 per degree of freedom and a reasonable fit. In addition to the adequate model fit, it is worth noting that no significant correlation error terms were found that, if allowed to be estimated, would yield a better fit model. Collectively, the model fit indices, factor loadings, squared multiple correlations, and composite reliability 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.

Structural Equation Modeling—Structural Model

The results of fitting the structural model to the data indicate that the model has a good fit with a relatively low χ^2 (Table 5). The dependence of χ^2 on the sample size and degrees of freedom is widely understood (Bentler and Bonett 1980) and must be interpreted with caution. All other measures of fit (Table 5), including χ^2 per degree of freedom, were in the acceptable range and above the minimum recommended values. The completely standardized path coefficients of the structural model provide evidence for the hypothesized relationships and are shown on Figure 2. All the relationships of the tested model are statistically significant at level 0.01, which provides support for the hypotheses of the study.

Table 4 Latent Variable Statistics

	Mean	Std. dev.	PPIT	PR	PC	T	PI
PPIT	3.13	0.96	0.62				
PR	3.97	0.74	−0.14 (0.06)	0.69			
PC	3.79	0.91	−0.42 (0.05)	0.38 (0.05)	0.68		
T	3.05	0.75	0.60 (0.04)	−0.32 (0.05)	−0.37 (0.05)	0.81	
PI	3.39	0.91	0.46 (0.05)	−0.18 (0.06)	−0.25 (0.06)	0.46 (0.05)	0.69

Note. The correlations and error terms ( ) are shown in the off-diagonal terms. The diagonal terms indicate the AVE for each construct.

Table 5 Goodness of Fit Assessments for the Measurement and Structural Model

Goodness of fit measures	χ^2 (d.f.)	χ^2/d.f.	NFI	CFI	IFI	RFI	GFI	AGFI	RMR	RMSEA
Good model fit ranges	Non-sign.	<2.00	>0.90	>0.90	>0.90	>0.90	≈0.90	>0.80	<0.055	<0.080
CFA model	211.43 (125)	1.69	0.95	0.98	0.98	0.94	0.94	0.92	0.044	0.042
SEM model	230.42 (129)	1.79	0.94	0.97	0.97	0.93	0.94	0.91	0.054	0.046

The mediation effect of privacy concerns was also tested using alternative models and by examining the strength of the relationships between perceived risk, privacy concerns, and willingness to provide personal information (Joreskog and Sorbom 1993, Bollen 1989). To test whether perceived risk significantly affects the dependent variable in the absence of the mediator, the first alternative model excluded the privacy concerns. This model resulted in a coefficient between perceived risk and the dependent variable of -0.22 at level $p < 0.01$. In our original model, all the relationships were statistically significant at level $p < 0.01$ (0.33 for PR-PC, -0.38 for PC-PPIT, and -0.15 for PR-PPIT). Thus, the relationship between perceived risk and the dependent variable attenuated when privacy concerns were incorporated in the model, establishing support for partial mediation. To test for full mediation, another alternative model was run, in which the path from privacy risk to the dependent variable was constrained to zero. The χ^2 difference between this model and the original hypothesized model was 6.10 for $\Delta df = 1$, which means that the p-value of the difference is <0.05. Thus, the data do not support full mediation.

Discussion

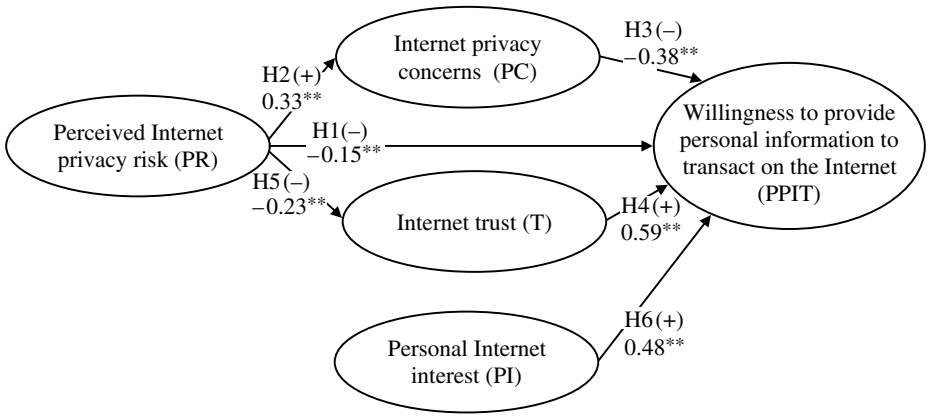
Empirical Results

The primary goal of this paper was to develop and empirically test an extended model of the privacy calculus in which a set of contrary beliefs was hypothesized to affect individuals' willingness to provide personal information to complete transactions on the Internet. The analyses indicated that all the constructs' psychometric properties exceeded the established criteria for instrument reliability, and convergent and discriminant validity (Tables 3–5). The model's *goodness of fit* indices demonstrated its nomological validity suggesting that there are causal relationships among the factors in the model we tested (Table 5). The results supported each of the hypotheses (Table 6).

Limitations

There are a number of considerations that should be taken into account prior to generalizing from these results. First, as is the case with many studies, common methods bias was a threat we had to address (Podsakoff et al. 2003, Straub et al. 2004). We eliminated this threat by ensuring anonymity to

Figure 2 SEM Completely Standardized Path Coefficients



*$p < 0.05$; **$p < 0.01$.

Table 6 A Summary of the Model's Hypotheses and Results

Hypothesis number	Hypothesized relationships	Results
1	A higher level of perceived Internet privacy risk is related to a lower level of willingness to provide personal information to transact on the Internet.	Supported
2	A higher level of perceived Internet privacy risk is related to a higher level of Internet privacy concerns.	Supported
3	A higher level of Internet privacy concerns is related to a lower level of willingness to provide personal information to transact on the Internet.	Supported
4	A higher level of Internet trust is related to a higher level of willingness to provide personal information to transact on the Internet.	Supported
5	A lower level of perceived Internet privacy risk is related to a higher level of Internet trust.	Supported
6	A higher level of personal Internet interest is related to a higher level of willingness to provide personal information to transact on the Internet.	Supported

the respondents, assuring them that there were no right or wrong answers, and requesting that they answer each question as honestly as possible. The latter procedures are known to reduce the likelihood of bias caused by social desirability or respondent acquiescence (Podsakoff et al. 2003). Also, following Podsakoff et al. (2003), we determined the common method variance using Harman's single-factor test by simultaneously loading all items in factor analysis using Varimax rotation. All indicators showed high factor loadings and low cross-loadings. Each principal component explained almost an equal amount of the 76% total variance, ranging from 13.4% to 16.6%. This indicates that our data do not suffer from common method bias.

Further remedies for common method bias include obtaining measures of the predictors and the criterion variable from different sources or temporal, proximal, psychological, or methodological separation of measurement. Despite the beneficial effects, however, these remedies may also contaminate the measurement with intervening factors (Podsakoff et al. 2003). When appropriate to the focus of a study, we would encourage scholars to use research designs in which data are collected in short interviews during which individuals could demonstrate how they use the Internet. For example, if individuals report privacy concerns, it would be useful to understand whether and how they attempt to reduce risk by manipulating Web settings. While it might be difficult to observe individuals at their own computers, demonstrated knowledge of how to manipulate browser settings and users' explanations of their choices would extend the method of data collection and reinforce findings that would otherwise be based on surveys alone.

Another consideration related to generalizing from the results provided here focuses on user willingness to disclose personal information to Internet websites *in general*. Other studies investigating behavioral intentions related to Internet transactions have developed research designs focusing on websites of specific vendors (e.g., Jarvenpaa et al. 1999, 2000; McKnight et al. 2002; Pavlou and Gefen 2004; van der Heijden 2004). In doing so, these studies, either by implication or by incorporating constructs such as vendor reputation (McKnight et al. 2002) or familiarity with vendors (Gefen 2000), account for the influence of specific parties in addition to the influence of the Internet environment. By focusing on the e-commerce

websites in general, our research design eliminated the explicit influence of particular online vendors and thus emphasized the role of the artifact. We would argue that user perceptions related to the online environment in general as well as to specific vendors in particular are both important for better understanding user behavior related to e-commerce. While we would intuitively expect that familiarity and reputation would override perceived privacy risk and privacy concerns and be positively related to willingness to disclose information, additional research is needed to substantiate this expectation. It may be that even with familiarity and reputation, residual risk perceptions and privacy concerns linger because of the Internet environment alone. By focusing on websites in general rather than specific websites, the findings reported here provide evidence in support of the argument that even when users report perceived risk and have privacy concerns about personal information disclosed in an online environment, other perceptions and beliefs are important factors that can override these concerns.

Careful attention should also be given to the measures that we have used for the constructs in our model. In particular, we note that the items we used for personal interest required respondents to indicate whether personal interest overrode other concerns. We used these measures because we needed to capture higher levels of personal interest rather than passing interest, given the focus of our study on Internet use in general. However, researchers should attempt to confirm these results using other measures or other research strategies. For example, more straightforward personal interest measures could be used in research designs that focus on specific websites, which would capture interest in the particular offerings of that online vendor. Results based on these efforts would provide more support for broadly generalizing the influence of personal interest than we can offer here, given the nature of our research design.

As with most empirical studies, the sample size and spectrum of respondents presents some limitations to generalization. Even though we made a concerted effort to include a range of individuals representing different demographic groups of Internet users, the sample was limited to a specific area in the southeastern United States, which limits generalizability to this region of the country. A statistically random sample of the U.S. population would have increased the generalizability of our results.

Contributions

The factors examined in the model comprise a set of beliefs in a calculus or decision process in which competing beliefs are weighed and where the strength of one may override the influence of another. The results for the individuals who responded to our survey show that all of the antecedent beliefs were directly related to the dependent variable. Overall, the three factors most strongly related to the willingness to provide personal information were Internet privacy concerns, Internet trust, and personal Internet interest. This reinforced our claim that the antecedent beliefs were indeed competing.

The pattern of these results provides insight into the complex process that leads to the decision to provide personal information over the Internet. A high level of behavioral intention must be preceded by higher levels of confidence and enticement beliefs than the levels of general and specific privacy risk beliefs. Higher levels of privacy risk beliefs would suggest user resistance to personal information disclosure.

While prior studies (e.g., Jarvenpaa et al. 1999, 2000; Pavlou 2003; Pavlou and Gefen 2004) incorporated trust and risk as predictors of willingness to make e-commerce purchases, the model we tested incorporated these predictors and specified willingness to provide personal information over the Internet as the dependent variable. Very few studies have linked these variables to information sharing, much less incorporated privacy concerns as a predictor of behavioral intention. Our results concerning the centrality of trust in influencing the willingness to provide personal information to transact on the Internet corroborate the results of two notable exceptions (McKnight et al. 2002, Malhotra et al. 2004). However, in comparing the results of these investigations with those reported here, the strength of the relationship between trust and willingness to provide information in this study was considerably greater. (McKnight et al. 2002 reported a coefficient of 0.30 and

Malhotra et al. 2004 reported 0.23, and the coefficient in this study was 0.59.) Also, other investigations that have incorporated risk as a predictor of e-commerce transactions have specified risk in terms of economic uncertainty (e.g., Jarvenpaa et al. 1999, 2000; Pavlou 2003; Pavlou and Gefen 2004). In our investigation, as well as those of McKnight et al. (2002) and Malhotra et al. (2004), risk was specified as privacy uncertainty. This is an important distinction that researchers interested in information sharing on the Internet will want to emulate.

Incorporating the personal Internet interest factor in the model represents an incremental contribution that helps to explain willingness to provide information. Personal interest enriches the privacy calculus model and should be included in future models that seek to explain transaction intentions.

Implications for Research

The framework of a calculus is useful for studying beliefs that are antecedent to behavioral intentions following the theoretical framework provided in TRA, TPB, and TAM. The notion of a calculus reinforces the perspective that antecedents influencing behavioral intention can be contrary, and that their relative influence needs to be accounted for in attempting to understand planned behavior and technology acceptance. While the inclusion of contrary factors in the privacy calculus is intuitively appealing, it is also theoretically useful because it assumes that deterministic outcomes, either utopian or anti-utopian (Kling 1996, Iacono and Kling 1996), are not likely. The explanation for an Internet user's willingness to disclose personal information over the Internet is more complex than a deterministic perspective suggests.

Theoretical models based on the notion of a calculus can advance our understanding of how individuals use information technology by providing a framework for specifying different sets of beliefs that match particular functionalities of a given technology (Orlikowski and Iacono 2001). The belief factors examined in this investigation are related to the functionality of the Internet that (a) provide a wide range of information, products, and service-related offerings to users, and (b) allow for the collection of personal information as a necessary condition for user transaction completion. The functionality of (a) offers benefits to Internet users by providing offerings that match personal interest, whereas the functionality of (b) is the source of costs related to privacy risk and concerns.

The model we tested and the results reported are consistent with expectancy theory, which broadly holds that individuals are motivated to maximize positive outcomes (i.e., benefits) and minimize negative ones (i.e., risks). This theoretical framework provides a useful basis for further investigations. Expectancy is the subjective probability that an action will lead to a certain outcome (Vroom 1964). Subjective probability is influenced by a number of factors, including an individual's emotional orientation to the outcome (Van Eerde and Thierry 1996). Future investigations focusing on the personal information disclosure outcome in an online environment should account for variance in emotional orientation. Prior experience in disclosing personal information in conventional or online settings and the positive or negative consequence of this action will influence one's emotional orientation toward future willingness to disclose personal information. Moreover, as individuals acquire more experience over time, emotional orientation toward the outcome can change. Researchers might also find Petronio's (1991, 2002) information boundary theory a useful perspective for explaining how past experience informs decisions to disclose or withhold information. In sum, an important direction for future research is to account for the dynamic nature of emotional orientations as a factor in the privacy calculus for personal information disclosed in online environments.

Other areas for future exploration involve cognitive antecedents to expected outcomes, which might be viewed as an extension of expectancy theory. Are individuals with greater technical knowledge about information technology in general, or the Internet in particular, more or less willing to disclose personal information online? Are "heavy" consumers of news and information-oriented programs and articles more or less willing to do so? In a related study, we reported that Internet literacy (i.e., the ability to use Internet applications to accomplish practical tasks) was negatively related to privacy concerns, whereas social awareness (i.e., interest in following social and

political developments, including regulations of high-tech industries, through various media) was positively related to privacy concerns (Dinev and Hart 2006).

Research focusing on how to manage privacy risk and encourage trust to offset privacy concerns related to Internet use is another area in which important contributions could be made. Recently, Milne and Culnan (2004) found that reading privacy notices on websites is one way that individuals manage privacy risk. Reading the notices was particularly important when individuals did not have prior experience with a firm. They also found that perceived comprehensibility of the notice was an important predictor of whether it was read and whether it contributed to encouraging trust: "Notices that are perceived by consumers to be obfuscated or excessively legalistic can contribute to skepticism" (Milne and Culnan 2004, p. 24).

What other ways do individuals attempt to manage privacy risk? Does adjusting the settings on a Web browser diminish privacy risk and concern? Does installing security tools (e.g., firewalls) have a similar effect? To what extent are an individual's subjective norms, following the theory of reasoned action (Ajzen and Fishbein 1980), related to an awareness of these protective measures, the tendency to follow them, and their overall influence on the behavioral intention to provide personal information over the Internet?

Other directions for future effort focus on the personal interest factor. The strength of the relationship we found between personal interest and willingness to provide personal information to transact on the Internet reflects the influence of enticement within an electronic gallery in which wide ranges of information, products, and services are available. Future research should attempt to refine the personal interest factor and measure other beliefs related to enticement in the context of Internet use. Certain types of personal interest, which we defined as cognitive attraction, might have greater influence in overriding privacy risk and concerns than others. For example, interest that is based on needs related to health, work, education, or family may have a greater overriding influence compared with interest based on lifestyle or entertainment.

Another enticement factor that deserves investigation is convenience that the Internet provides relative to alternative sources of information, products, or services (Torkzadeh and Dhillon 2002) and the possibility that convenience will override perceptions of privacy risk and concerns. This factor has multiple dimensions. In the context of e-commerce, geographic proximity to conventional stores is one aspect of an alternative source factor. However, the extent of proximity is also important, as is evident in comparing the case of an Internet user in a rural area with a user in a metropolis—but even for the latter, proximity can be an overriding influence. There might also be an interaction between proximity and the type of product sought (e.g., uncommon or rare products). A user might decide that the need for a highly desired uncommon product that is not in close proximity overrides privacy risk and concerns. However, Maslow's (1954) hierarchy of needs would suggest that privacy would rank below other needs. Satisfying privacy needs would be required for individuals to be attentive to higher needs. Thus, unless privacy risks and concerns are addressed, we would speculate that individuals would not be inclined to disclose personal information necessary to make online purchases. Maslow's hierarchy may be a useful framework for further investigating the relative importance of privacy in online environments.

In addition, there is a temporal dimension to the convenience factor. Search engines on the Internet and various indexing protocols embedded in websites can substantially reduce the amount of time spent locating desired information, products, and services. Rice et al. (2001, p. 33) have written an extensive review of the literature on accessing and browsing information. They note that greater perceived and actual accessibility leads to greater likelihood of use, and that this "in turn tends to increase perceived accessibility, leading to more use (Culnan 1983) and to reported increases in effectiveness (Rice and Shook 1988)." Greater use and skill in using the Internet may be related to an increase in perceived access to the things that the Internet provides and increased effectiveness in obtaining them. The enticement to reduce search time and the capability to retrieve information and obtain goods and services from websites which

might otherwise be onerous could override perceived privacy risks and concerns.

These time and geographic (space) dimensions of convenience are examples of the time-space distanciation, or the separation of time and space, that Giddens (1990, 1991) argued characterized "high modernity." In traditional societies, time and space were linked through place. The requirement of physical presence in a specific place to obtain information, products, and services is substantially alleviated by the Internet. While certain benefits associated with time-space distanciation may be evident, the challenge for MIS researchers is to more fully understand the consequences. An important direction for future research is to investigate the extent to which the benefits of distanciation through Internet use override or diminish privacy risks and concerns.

It has been 19 years since the first article on privacy was published in an MIS journal (Mason 1986). Since that time, significant advances in digital storage and networking technologies have paralleled aggressive corporate initiatives in collecting and analyzing personal information about current and prospective customers. While interest in privacy by MIS scholars is evident, we would argue that the amount of attention given does not match its social importance. Considerably greater effort needs to be made in understanding privacy concerns and how they affect individuals' interactions with other entities when using information technology, particularly the Internet.

Implications for Practice

Our study provides insight into the argument made by practitioners and economists about the privacy paradox (see, e.g., Ackerman et al. 1999, Sweat 2000), namely that consumer behavior contradicts consumer preference. Why do privacy concerns rank high in opinion polls while consumers appear to exhibit contradictory behavior by continuing to submit personal information "as if they didn't care?" The results of this investigation show that perceived privacy risk and privacy concerns are two factors, among a set of at least four factors, related to the willingness to provide personal information to conduct transactions on the Internet. Behavioral intention with regard to information disclosure is the result of a combination of factors that do not eliminate perceived privacy risk and privacy concerns even when there is a decision in favor of information disclosure.

These results would suggest that practitioners and economists should not assume that personal information disclosure reflects a lack of concern with respect to privacy. Although further research is required to better understand how individuals might be persuaded to overcome privacy concerns and allow other factors to override these concerns, the findings presented here lend support to the notion that website providers ought to be vigilant in seeking ways to build user confidence and minimize user privacy risks. In particular, the strong relationship between perceived Internet trust and willingness to provide personal information suggests that trust is an important condition for completing online transactions. Therefore, Internet vendors and other website sponsors ought to proactively work to sustain and ensure trust.

Conclusion

Over time, we can expect that information technology will be increasingly used to collect personal information with consequences that are potentially both beneficial and harmful to individuals. At the same time, the debate over individuals' rights and policies that has been initiated in attempts to benefit society as a whole, and the pivotal importance of privacy in this debate will also continue to increase (Etzioni 1999). As both of these processes evolve, it is important to develop a better understanding of how individuals develop privacy concerns and what consequences these perceptions have in influencing interactions with other individuals, groups, agencies, and vendors. The privacy calculus model is useful for both researchers and practitioners because it is a framework that accounts for contrary factors and thereby better represents the complicated nature of the issues that are before us.

Acknowledgments

The authors are very grateful to Cynthia Beath, Senior Editor, for her encouragement and direction in helping them develop this manuscript. They are also grateful to the associate editor and three anonymous reviewers for their constructive advice, and to Michael Mullen and Xenophon Koufteros at Florida Atlantic University for their assistance on methodological and statistical issues.

Appendix. Items and Scales

Latent variable	Item	Scale
Willingness to provide personal information to transact on the Internet (PPIT)	To what extent are you willing to use the Internet to do the following activities? PPIT 1: 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) PPIT 2: 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) PPIT 3: Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software) PPIT 4: 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
Perceived Internet privacy risk (PR)	What do you believe is the risk for regular Internet users due to the possibility that PR1: Records of transactions could be sold to third parties? PR2: Personal information submitted could be misused? PR3: Personal information could be made available to unknown individuals or companies without your knowledge? PR4: Personal information could be made available to government agencies?	Very low risk–Very high risk
Internet 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
Internet trust (T)	Rate the extent to which you agree with the following statements: T1: Internet websites are safe environments in which to exchange information with others. T2: Internet websites are reliable environments in which to conduct business transactions. T3: Internet websites handle personal information submitted by users in a competent fashion.	Strongly disagree–Strongly agree
Personal Internet interest (PI)	Rate the extent to which you agree with the following statements: PI1: I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that 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

References

Ackerman, M. S., L. F. Cranor, J. Reagle. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proc. 1st ACM Conf. E-commerce, EC'99*, Denver, CO.

Ajzen, I. 1988. *Attitudes, Personality, and Behavior*. Dorsey Press, Chicago, IL.

Ajzen, I., M. Fishbein. 1980. *Understanding Attitudes and Predicting Social Behavior*. Prentice-Hall, Englewood Cliffs, NJ.

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Brookes, Monterey, CA.

Anderson, J. C., S. W. Gerbing. 1998. Structural equation modeling in practice: A review and recommended two-step approach. *Psych. Bull.* **103**(3) 411–423.

Anderson, J. C., J. A. Narus. 1990. A model of distributor firm and manufacturer firm working partnerships. *J. Marketing* **54**(1) 42–58.

Bagozzi, R. P. 1980. *Causal Models in Marketing*. Wiley, New York.

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.

Blakeney, R. N. 1986. A transactional view of the role of trust in organizational communication. *Trans. Anal. J.* **16**(1) 95–98.

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

Brief, A. P., R. J. Aldag. 1977. The intrinsic-extrinsic dichotomy: Toward conceptual clarity. *Acad. Management* **2**(3) 496–500.

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. 1998. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*. Lawrence Erlbaum Association, Mahwah, NJ.

Cheung, C., M. Lee. 2001. Trust in Internet shopping: Instrument development and validation through classical and modern approaches. *J. Global Inf. Management* **9**(3) 23–35.

Chiles, T. H., J. F. McMackin. 1996. Integrating variable risk preferences, trust, and transaction cost economics. *Acad. Management Rev.* **21**(1) 73–99.

Chin, W. W., A., Gopal. 1995. Adoption intention in GSS: Relative importance of beliefs. *DATA BASE* **26**(2, 3) 42–64.

Culnan, M. J. 1993. "How did they know 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. Public Policy Marketing* **19** 20–29.

Culnan, M. J., P. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organ. Sci.* **10**(1) 104–115.

Culnan, M. J., R. J. Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *J. Soc. Issues* **59**(2) 323–342.

Davis, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quart.* **13**(3) 319–340.

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

Dinev, T., P. Hart. 2004. Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behav. Inform. Tech.* **23**(6) 413–422.

Dinev, T., P. Hart. 2006. Internet privacy concerns and social awareness as determinants of intention to transact. *Internat. J. Electronic Commerce*. Forthcoming.

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

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

Fox, S. 2000. *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. The Pew Internet & American Life Project. Accessed on April 18, 2005. http://www.pewinternet.org.

Federal Trade Commission (FTC). 1999. Self-regulation and privacy online. Report to Congress. http://www.ftc.gov/os/1999/07/privacy99.pdf.

Gabarro, J. 1987. *The Dynamics of Taking Charge*. Harvard Business School Press, Boston, MA.

Ganesan, S. 1994. Determinants of long-term orientation in buyer-seller relationships. *J. Marketing* **58** 1–19.

Gefen, D. 2000. Electronic commerce: The role of familiarity and trust. *Omega* **28**(5) 725–737.

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

Gefen, D., D. W. Straub, M. C. Boudreau. 2000. Structural equation modeling and regression: Guidelines for research practice. *Comm. AIS* **4**(Article 7) 1–80.

Giddens, A. 1990. *The Consequences of Modernity*. Polity Press, Cambridge, U.K.

Giddens, A. 1991. *Modernity and Self-Identity*. Polity Press, Cambridge, U.K.

Glazer, R. 1991. Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. *J. Marketing* **55**(4) 1–20.

Goodwin, C. 1991. Privacy: Recognition of a consumer right. *J. Public Policy Marketing* **10**(1) 149–166.

Hart, P., C. Saunders. 1998. Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organ. Sci.* **8**(1) 23–42.

Iacono, S., R. Kling. 1996. Computerization movements and tales of technological utopianism. R. Kling, ed. *Computerization and Controversy*. Academic Press, San Diego, CA, 85–105.

Igbaria, M., J. Iivari, H. Maragahh. 1995. Why do individuals use computer technology? A Finnish case study. *Inform. Management* **29**(5) 227–238.

Jarvenpaa, S. L., N. Tractinsky, M. Vitale. 2000. Consumer trust in an Internet store. *Inform. Tech. Management* **1** 45–71.

Jarvenpaa, S. L., N. Tractinsky, L. Saarinen, M. Vitale. 1999. Consumer trust in an Internet store: A cross-cultural validation. *J. Comput.-Mediated Comm.* **5**(2) 44–71.

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

Kling, R. 1996. Hopes and horrors: Technological utopianism and anti-utopianism in narratives of computerization. R. Kling, ed. *Computerization and Controversy*. Academic Press, San Diego, CA, 40–58.

Kling, R., J. P. Allen. 1996. How the marriage of management and computing intensifies the struggle for personal privacy. D. Lyon, E. Zureik, eds. *Computers, Surveillance and Privacy*. University of Minnesota Press, Minneapolis, MN, 104–131.

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

Laufer, R. S., M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *J. Soc. Issues* **33**(3) 22–42.

Lee, M., E. Turban. 2001. Trust in b-to-c electronic commerce: A proposed research model and its application. *Internat. J. Electronic Commerce* **6**(1) 75–91.

Malhotra, N. K., S. S. Kim, J. Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inform. Systems Res.* **15**(4) 336–355.

Maslow, A. H. 1954. *Motivation and Personality*. Harper and Row, New York.

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

Mayer, R., J. H. Davis, F. D. Schoorman. 1995. An integrative model of organizational trust. *Acad. Management Rev.* **20**(3) 709–734.

McGregor, D. 1967. *The Professional Manager*. McGraw-Hill, New York.

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

McLain, D. L., Z. K. Hackman. 1999. Trust, risk, and decision-making in organizational change. *Public Admin. Quart.* **23**(2) 152–176.

Milberg, S. J., H. J. Smith, S. J. Burke. 2000. Information privacy: Corporate management and national regulation. *Organ. Sci.* **11**(1) 35–37.

Milberg, S. J., S. J. Burke, H. J. Smith, E. A. Kallman. 1995. Values, personal information privacy, and regulatory approaches. *Comm. ACM* **38**(12) 65–74.

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

Mishra, A. K. 1996. Organizational responses to crisis: The centrality of trust. R. M. Kramer, T. R. Tyler, eds. *Trust in Organizations: Frontiers of Theory and Research*. Sage, Thousand Oaks, CA, 261–287.

Miyazaki, A. D., A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. *J. Public Policy Marketing* **19**(1) 54–63.

Mullen, M. R., G. R. Milne, N. Didow. 1996. Determining cross-cultural metric equivalence in survey research: A statistical test. *Adv. Internat. Marketing* **8** 145–157.

O'Brien, T. 2000. Officials worried over a sharp rise in identity theft. *New York Times* (April 3) 1.

Orlikowski, W., S. Iacono. 2001. Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Inform. Systems Res.* **12**(2) 121–134.

Pavlou, P. A. 2003. Consumer acceptance of electronic commerce—Integrating trust and risk, with the technology acceptance model. *Internat. J. Electronic Commerce* **7**(3) 69–103.

Pavlou, P. A., D. Gefen. 2004. Building effective online marketplaces with institution-based trust. *Inform. Systems Res.* **15**(1) 37–59.

Petronio, S. 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Comm. Theory* **1** 311–335.

Petronio, S. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press, Albany, NY.

Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, N. P. Podsakoff. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psych.* **88**(5) 879–903.

Preston, J. 2004. Judge strikes down section of patriot act allowing secret subpoenas of Internet data. *New York Times* (September 30) 26.

Rice, R. E. 2001. *Accessing and Browsing Information and Communication*. The MIT Press, Cambridge, MA.

Rice, R. E., D. E. Shook. 1988. Access to, usage of, and outcomes from an electronic messaging system. *ACM Trans. Office Inform. Systems* **6**(3) 255–276.

Rice, R. E., M. McCreadie, S. L. Chang. 2001. *Accessing the Browsing—Information and Communication.* MIT Press, Cambridge, MA.

Rindfleish, T. C. 1997. Privacy, information technology, and health care. *Comm. ACM* **40**(8) 92–100.

Rosen, J. 2000. *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York.

Rousseau, D., R. Sitkin, R. Burt, C. Camerer. 1998. Not so different after all: A cross-discipline view of trust. *Acad. Management Rev.* **23**(3) 393–404.

Segars, A. H., V. Grover. 1993. Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quart.* **17**(4) 517–529.

Smith, H. J. 1993. Privacy policies and practices: Inside the organizational maze. *Comm. ACM* **36**(12) 105–122.

Smith, H. J., S. J. Milberg, S. J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* **20**(2) 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., D. L. Stone. 1990. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. K. M. Rowland, G. R. Ferris, eds. *Research in Personnel and Human Resources Management*, Vol. 8. JAI Press, Greenwich, CT, 349–411.

Straub, D., M.-C. Boudreau, D. Gefen. 2004. Validation guidelines for IS positivist research. *Comm. AIS* **13**(Article 24) 380–427.

Swan, J., I. Trawick, D. Rink, J. Roberts. 1988. Measuring dimensions of purchaser trust of industrial salespeople. *J. Personal Selling Sales Management* **8** 1–9.

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

Tan, Y., W. Thoen. 2001. Toward a generic model of trust for electronic commerce. *Internat. J. Electronic Commerce* **5**(2) 61–71.

Taylor, S., P. A. Todd. 1995. Understanding information technology usage: A test of competing models. *Inform. Systems Res.* **6**(2) 144–176.

Teo, T. S. J., V. K. G. Lim, R. Y. C. Lai. 1999. Intrinsic and extrinsic motivation in Internet usage. *Omega* **27**(1) 25–37.

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. Appl. Psych.* **66**(3) 308–313.

Torkzadeh, G., G. Dhillon. 2002. Measuring factors that influence the success of Internet commerce. *Inform. Systems Res.* **13**(2) 187–204.

University of California, Los Angeles (UCLA). 2000, 2001, 2002, 2003, 2004. Internet report: Surveying the digital future. http://ccp.ucla.edu/pages/internet-report.asp.

van der Heijden, H. 2002. Factors influencing the usage of websites: The case of a generic portal in The Netherlands. *Inform. Management* **40**(6) 541–549.

van der Heijden, H. 2004. User acceptance of hedonic information systems. *MIS Quart.* **28**(4) 695–704.

van Eerde, W., H. Thierry. 1996. Vroom's expectancy models and work-related criteria: A meta-analysis. *J. Appl. Psych.* **81**(5) 575–586.

Venkatesh, V. 1999. Creation of favorable user perceptions: Exploring the role of intrinsic motivation. *MIS Quart.* **23**(2) 239–260.

Venkatesh, V. 2000. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Inform. Systems Res.* **11**(4) 342–365.

Venkatesh, V., F. D. Davis. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Sci.* **46** 186–204.

Venkatesh, V., M. G. Morris, G. B. Davis, F. D. Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS Quart.* **27**(3) 425–478.

Vroom, V. H. 1964. *Work and Motivation*. Wiley, New York.

Wald, M. L. 2004. Threats and responses: The airlines; U.S. wants all air traveler files for security test. *New York Times* (September 22) 1.

Webster, J., J. J. Martocchio. 1992. Microcomputer playfulness: Development of a measure with workplace implication. *MIS Quart.* **16**(2) 201–226.

Werts, C. E., R. L. Linn, K. G. Jöreskog. 1974. Intraclass reliability estimates: Testing structural assumptions. *Educ. Psych. Measurement* **34** 25–33.

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

Westin, A. F. 2001. Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Hearing on "Opinion surveys: What consumers have to say about information privacy." (May 8). http://energycommerce.house.gov/107/hearings/05082001Hearing209/Westin309.htm.

Yates, J. F., E. R. Stone. 1992. Risk appraisal. J. F. Yates, ed. *Risk-Taking Behavior*. John Wiley, Chichester, U.K., 49–85.

Copyright 2006, by INFORMS, all rights reserved. Copyright of Information Systems Research is the property of INFORMS: Institute for Operations Research and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.