Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact

Tamara Dinev and Paul Hart

ABSTRACT: This study focuses on antecedents to Internet privacy concerns and the behavioral intention to conduct on-line transactions. Perceptions of privacy are socially constructed through communication and transactions with social entities over a networked environment, a process that involves a certain level of technical skill and literacy. The research model specifies that social awareness and Internet literacy are related to both Internet privacy and intention to transact. Survey data collected from 422 respondents were analyzed using structural equation modeling (SEM) with LISREL and provided support for the hypothesized relationships. Social awareness was positively related and Internet literacy was negatively related to Internet privacy concerns. Moreover, Internet privacy concerns were negatively related and Internet literacy positively related to intention to transact on-line. This research explores the two alternative antecedents to Internet privacy concerns and intention to engage in e-commerce activity and contributes to our understanding of Internet privacy and its importance in the global information environment. The construct of social awareness can be broadened to develop a much-needed construct of awareness in MIS research related to the voluntary usage of information technology. A segmentation of Internet users with respect to privacy concerns is also proposed.

KEY WORDS AND PHRASES: Intention to transact on-line, Internet literacy, Internet privacy, social awareness.

The explosive growth of information technology and of the capacity to store and process copious amounts of personal information has paralleled the increased use of the Internet. Customer data are a major marketing asset through which businesses can improve customer service and build competitive advantage. The need to gather personal data, however, poses a threat to customer privacy and may affect the further growth of Internet usage [16, 17].

A substantial body of recent research shows that trust is a very important factor influencing Internet users' purchasing intentions and behavior [38, 45, 66, 70]. Privacy is another important factor whose nature and impact need to be fully understood and adequately studied. Privacy is a highly cherished value [19, 25, 27, 78]. It is the reason most frequently cited for why individuals do not use the Internet [25, 26, 74, 75, 76, 79] or for why they once shopped on-line but are now reluctant to do so [72]. Various polls have reported that approximately 80 percent of Americans view information collected about them was extremely important, but believe they have lost control over how their personal information is collected and used by companies [25, 31]. Web buyer confidence in on-line credit card security has been steadily declining, with more consumers questioning the safety of submitting credit card data on-line and wondering whether buying on-line is worth the risk [36].

Concerns about privacy are an important factor in Internet use. Privacy is a social concept, and protecting one's privacy in the Internet environment and

International Journal of Electronic Commerce / Winter 2005–6, Vol. 10, No. 2, pp. 7–29.

1086-4415/2006 $9.50 + 0.00.

on Internet-connected computers requires technical skills and an understanding of how data and information flows are processed in a network environment. Thus, an individual's Internet privacy concerns result from two processes: (1) interaction with information technology (the Internet in this case), which requires a set of skills and a level of technical literacy, and (2) a social process of communication and transaction with sometimes anonymous or little-known social entities (companies or individuals) in the networked environment. The study explores two factors salient to Internet privacy concerns: Internet literacy and social awareness. It reports on the confirmatory factor analysis (CFA) validation of the social awareness and Internet literacy instruments, while integrating previously developed instruments for Internet privacy concerns and intention to use the Internet for the purposes of e-commerce. A model is then proposed and tested through structural equation modeling (SEM) related to the above-mentioned constructs. The study's findings about the psychological antecedents of privacy concerns and Internet use can help IS managers and e-commerce marketers develop strategies that will broaden their Internet user base and facilitate the interaction and usage of Internet Web sites and applications, thus opening opportunities for growth and competitive advantage.

The dependent variable of the model is intention to use the Internet for purposes of e-commerce, or, in short, intention to transact. Following Pavlou, intention to transact is operationalized by restricting it to the consumer's intent to engage in an electronic exchange with a B2C on-line business that involves the disclosure of personal information [52, 53]. Note, by the way, that much of the information merchants demand is very often not necessary for completing the transaction, but just desirable for their marketing purposes.

Theoretical Considerations and Propositions

Internet Privacy Concerns

A wide range of scholars in different fields have researched privacy as a psychological construct and sociological issue [21, 37, 42]. Every theoretical perspective involving privacy accounts for its complexity, given its multidimensional, elastic, contextually dependent, and dynamic nature, and the dichotomy between the individual and others [1, 35, 37, 43]. Much research in this area involves employees' perceptions of privacy values and beliefs [35, 46, 47, 59, 61]. Given the difficulty of defining privacy as a psychological construct, many sociologists define it as the "right to be left alone" [78]. MIS researchers have tailored the definition toward the informational aspect of privacy rather than its physical, spatial, and behavioral aspects, and refer to privacy as the right to control the collection and use of information about oneself [11, 44, 50]. In addition, privacy is usually regarded as a right. However, the notion of a right is also multidimensional. A right may be an ethical, social, or legal concept. Thus, it is difficult to find a generally accepted definition that may be operationalizable across studies conducted by researchers in different disciplines (e.g., psychology and law).

Interest in privacy by MIS researchers has been triggered by the explosive development and use of digital, storage, and Internet technologies [11, 14, 15, 16, 32, 44, 57]. Some researchers have focused their interest on concerns related to information privacy and an anticipation of possible loss of privacy [11, 14, 16, 46, 61]. Among other things, researchers have found that on-line purchasing intent is most influenced by security and privacy concerns [56, 66]. Internet users are becoming conscious of the power of Internet technologies to monitor their activities and gather information about them with or without their knowledge and consent [13]. They are also learning that a great many Web pages offer deceptive content [22]. As reported by Carroll, only 6 percent of U.S. consumers had a high level of trust in how Web sites handle and protect personal data [9]. In a study of the "trade-off" factors that influence Internet use, Dinev and Hart found that privacy concerns affect user decisions to conduct e-commerce transactions over the Internet [17].

The present study defines Internet privacy concerns as concerns about possible loss of privacy as a result of a voluntary or surreptitious information disclosure to a B2C Web commerce site. Based on the considerations outlined above, the model includes the negative relationship between Internet privacy concerns and intention to transact:

> *Hypothesis 1: Internet privacy concerns have a negative effect on intention to transact.*

Internet Literacy

Internet users often face challenges that may affect successful on-line interaction. Challenges a typical on-line user may encounter include establishing an on-line connection, orienting oneself efficiently on a Web page, dealing with deceptions [22], completing an Internet e-commerce transaction, submitting personal information, quickly and efficiently searching the Internet, dealing with offensive content retrieved by accident, dealing with spam e-mail or spy applications, setting the browser's privacy and security options, and identifying spoof e-mail or Web sites. All these processes require substantial skill and knowledge in order to protect one's computer, one's privacy, and information one would rather not disclose, or permit to be further disclosed by the company one is dealing with.

Internet literacy is closely related to computer literacy, which is now of great importance in everyday life [40, 48, 80]. The Internet is an infrastructure whose exploitation depends on computer use. Users' computer skills, attitudes, and beliefs are related to their use of the Internet. Because the Internet environment is so complex, Internet literacy is a more complex construct than computer technical literacy and includes the network-related factors mentioned above. Following the standard dictionary definition of computer literacy as "the ability to use a computer and its software to accomplish practical tasks," Internet literacy is defined in this paper as the ability to use an Internet-connected computer and Internet applications to accomplish practical tasks. Note that competency and literacy, as constructs,

are distinctly different from the construct of computer or Internet self-efficacy. The latter measures the level of confidence and belief that an individual can perform a certain task. The literature relates lower levels of self-efficacy to technology avoidance and anxiety. On the other hand, competence and literacy scales focus on either independently measured or self-assessed *ability* to do a specific task.

Privacy-invasive Internet technologies and applications present several challenges even to technically competent users. Computers are networked and thus are vulnerable to attacks, viruses, and intrusions perpetrated by malicious Internet users and facilitated by the ignorance and behavior of other Internet users. In addition, Internet users are regularly exposed to bogus and spoof e-mails or Web sites [39], spam e-mails, and unsolicited contacts through Internet communication channels. There is a constant need to be vigilant over the potential of hacker activity and possibility of viruses, and worms that attack Internet-connected computers and cost immense frustration, not to mention privacy and material losses [3]. Security alerts and system vulnerabilities are periodically announced, and users are often urged to update and install security fixes and patches [30]. Some Web sites and some Internet-related applications impose ActiveX controls and scripts that have free rein within the user's device. These may change browser preferences that most users do not understand, let alone know how to manage. Other Web sites and free software applications, without the user's knowledge and consent, install surreptitious software (so-called spyware) that monitors the user's on-line activities and provides click-stream data to a specific server [63, 71]. Users who find themselves in situations of this kind that are beyond their control tend to feel that their privacy has been invaded. This may substantially elevate their emotional state associated with Internet use, generating aggravation and hopelessness, and eventually lead to less Internet usage.

Software packages and applications are available that provide protection against these intrusions, but users need to know how to install them and take advantage of the benefits they offer [34]. Moreover, such software is often incomplete and inadequate. Further difficulty is presented by the need to constantly keep up with the issuance of patches and newer versions of the protective software, as well as operating systems, utilities, and key applications. For many people, this may spiral into a perception that they are facing a challenge that is insurmountable without advanced Internet and networking knowledge. The less Internet literacy users have, the more concerned they will be about privacy, because they will feel incompetent to protect their computers and to control intrusive technologies gathering personal data. Based on this observation, Spiekermann, Grossklags, and Berendt argued that privacy technologies need to enable even moderately computer-literate on-line users to protect themselves by allowing only a degree of disclosure they are comfortable with [62]. The above considerations suggest the following:

Hypothesis 2: Internet literacy has a negative effect on Internet privacy concerns.

Hypothesis 3: Internet literacy has a positive effect on intention to transact.

Social Awareness

Many challenges arise in relation to e-commerce. Some are technical in nature (e.g., achieving a secure and reliable environment), some are regulatory (e.g., legal frameworks and standardizations), and some are social. Among the social issues, trust, privacy, security, governance, censorship, and restrictions have been identified as having the highest priority [7, 51]. For example, MIS research on trust has undoubtedly shown that it is one of the most important factors in the acceptance of e-commerce [38, 45, 66, 70]. Public interest and involvement in these social issues drives policy changes intended to address the concerns of citizens and Internet users [72]. Passive involvement and raised interest in social issues are defined in the literature as social awareness. Social awareness is one of the key components of consciousness-raising, social action being the other [5, 23]. Social awareness is about appreciating the needs, impetus, and historical specificity of social events and processes. Speaking up against social injustice, creating awareness of how people affect the environment, promoting racial tolerance and respect, and making consumer decisions based on a company's ethics are different aspects of the social-awareness construct. People with high social awareness will tend to understand how a democracy works and exhibit interest in their country's political system [20, 28]. Awareness of issues and how they affect the individual, community, and society is a precursor to social movements and policy generation [5, 64, 67]. The effectiveness of social institutions depends on whether they engage their members or clients and encourage them to develop a social awareness that will eventually drive social change. Previous research has linked social awareness to individuals' attitudes and cognitive development [54, 55, 73]. Following Greene and Kamimura, who define social awareness as "naming the problem, speaking out, consciousness raising, and researching" [23, p. 3], in this paper, social awareness is defined as citizens' behavior with respect to following and being interested in and knowledgeable about community and government policies and initiatives, including those related to technology and the Internet.

People place a high value on privacy as an expression of personal dignity [12, 37]. Privacy is honored as an important individual right [19, 41, 68, 69, 78, 79]. For example, according to one poll in the United States, 79 percent of the public believe that "if the Framers of the Declaration of Independence were rewriting that document today, they would add privacy to the trinity of life, liberty, and pursuit of happiness" [76].

Because of their interest in social issues and policies, Internet users with high social awareness will closely follow Internet privacy issues, the possible consequences of a loss of privacy due to accidental, malicious, or intentional leakage of personal information, and the development of privacy policies. News items and highly publicized cases will heighten their acquaintance with possible breaches of privacy and security, and the risk of identity theft. Therefore, one may posit, with respect to privacy concerns, that Internet users who are more socially aware will tend to know more about the privacy debate, privacy policies, privacy risks associated with the Internet, and the legal implications of privacy invasions and identity theft. These users will have a stronger awareness of the importance of privacy in social life. The greater one's

social awareness, the more importance one will place on privacy as a societal value. One will also presumably be more concerned about privacy. Thus,

> *Hypothesis 4: Social awareness has a positive effect on Internet privacy concerns.*

The model presented in this paper is illustrated in Figure 1.

Research Method

The research hypotheses were tested empirically using data collected from a survey, using Dinev and Hart's instrument for measuring privacy concerns for information abuse, and intention to transact [17, 18] (items are shown in the Appendix). The scales for the new constructs in the theoretical model proposed in this study, Internet literacy and social awareness, were developed by examining prior work on similar constructs and adapting the existing measures. The computer literacy instrument developed by Gutek, Winter, and Eriksson was the basis for measuring Internet literacy [24]. However, the instrument could not be applied directly and needed substantial modification because it measures computer literacy by means of questions on programming experience that do not apply to Internet users.

Similarly, since the existing social-awareness instrument was developed to measure the attitudes of college students on cultural-diversity social issues, such as ethnicity, race, gender, and sexual orientation [23], it could not be readily applied to the study. Nonetheless, it provided important guidance and a base to build on. The instrument was substantially modified by deleting, rewording, and adding items. Consistent with current best practices in scale development, a wider net of candidate items was cast for the present model [10, 29, 60]. Based on additional extensive search of the Internet and the academic, professional, and popular literature, a list of 10 items was drafted.

The responses were statistically processed with exploratory factor analysis (EFA), followed by confirmatory factor analysis (CFA). SEM with LISREL was then applied to empirically test the hypothesized relationships. EFA is the standard and classic technique for initially establishing the validity and reliability of a measurement. CFA is a significantly more advanced technique for validity assessment than EFA [6, 49] and yields greater confidence in an instrument's validity and unidimensionality [2, 58, 77]. Additionally, EFA cannot detect and estimate the degree of correlation among items. The more reliable, robust, and flexible methodology of CFA along with SEM represents an increasingly popular approach for more rigorous assessment of theorized models.

This study employed LISREL 8.5 as the CFA and SEM software for assessing the model's validity [33]. An alternative research technique popular in MIS studies is SEM with partial least squares (PLS). However PLS is regarded as a soft-modeling approach, the rule of thumb being that if the model can be proved with LISREL, then LISREL is the better approach [6]. PLS makes use of least squares methods, which do not necessarily require stringent assump-

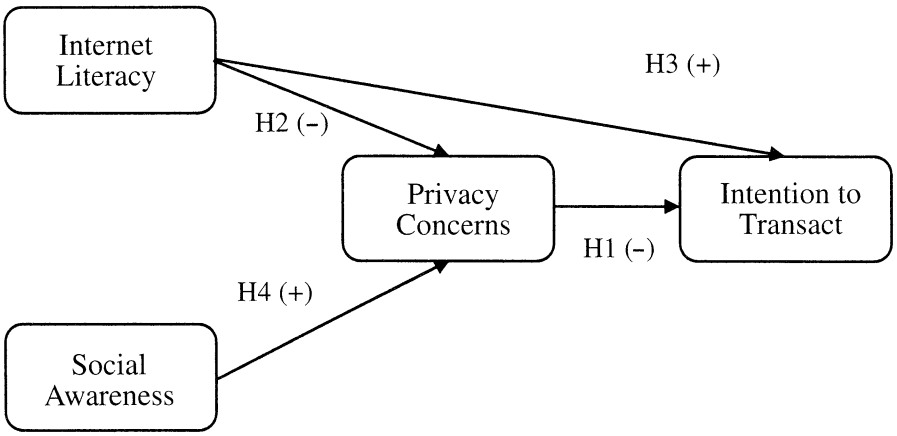

Figure 1. Proposed Theoretical Model

tions about the distribution of variables, residuals, and parameters. Thus PLS is especially useful for analyzing large, complex path models where LISREL often fails to converge within reasonable time limits. It is also quite useful for analyzing models based on small data sets where the sample covariance matrix is not positively definite.

Model Test

This paper reports on the EFA and CFA of Internet literacy and social-awareness instruments and on the SEM results of the relationships with respect to privacy concerns and intention to transact.

The instrument development for the constructs used in this study consisted of two pilot tests and several stages of survey administration during the years 2002–2004. The first pilot test was conducted with a sample of 100 respondents in the southeastern United States, including MIS students from a large university and retail and service-business employees. The EFA, reliability testing, and careful examination of the correlations required substantial changes to the instruments. Items had to be added, deleted, and modified, and this warranted the need for a second pilot survey. The latter was conducted with a sample of 70 undergraduate students at a large southeastern university. Following the same appropriate tests for data, minor wording changes were made, three items were dropped because of poor validity, and no additional items were suggested. The final instrument met the EFA validity and reliability criteria and was consistent at satisfactory levels. All items used were based on a 5-point Likert scale (*see Table 1*).

The final version of the survey was administered to a broad sample of respondents in the southeastern United States, including residents of two neighborhoods, teachers from two middle and two high schools, students and faculty from one large university, and employees from a large department store, five high-tech companies, one bank, one voluntary organization, and small service-

Construct	Item symbol	Item
Internet literacy (IL)		Rate the extent to which you are able to do the following tasks:
	IL1	Identify and delete a program which you consider intrusive (spyware) and which was installed through the Internet without your knowledge and permission.
	IL2	Manage virus attacks by using antivirus software.
	IL3	Communicate through instant messaging or discussion boards.
	IL4	Download files/audio/video/executables from the Internet.
Social awareness (SA)		To what extent do you agree with the following?
	SA1	I am interested in reading political commentaries or watching them on TV.
	SA2	I closely follow developments in my community.
	SA3	I enjoy discussing important social issues with others.
	SA4	I watch news and other television programs/channels that address current issues.
	SA5	I closely follow government regulation of high-tech businesses.
	SA6	I read at least one newspaper every day or watch news on TV.

Table 1. Internet Literacy and Social Awareness Items.

oriented businesses. The subjects were asked to fill in the survey and drop it in a conveniently located collection box. The average response rate was 55 percent, which reflects the completely voluntary participation. Many of the people who were given surveys and asked to fill in the questionnaire did not return a completed survey.

Results

Demographics and Exploratory Factor Analysis

The demographic profile of the 422 respondents who submitted usable surveys is shown in Table 2. The internal consistency and reliability of the scale items for each construct were established through the Cronbach's alpha coefficients (*see Table 3*), which were much higher than the threshold level of 0.66 suggested for exploratory research [49]. The corrected item-total correlations, which provide initial indications of reliability, were also high for all of the items. EFA with varimax rotation and Kaiser normalization were utilized for the initial assessment of the constructs' convergent and discriminant validity

Gender		Race		Age		Occupation		Income	
male:	49	White:	58	< 30:	59	technology:	12	< $60,000:	63
female:	51	Black:	16	< 30:	41	finance:	11		
		Hispanic:	15			retail:	10	$61,000-$100,000:	20
		Asian:	7			education:	15	> $100,000:	16
						government:	14		

Table 2. Demographic Profile of Respondents (*N* = 422).

Note: Numbers are percentages. Remaining percentages to 100 are either undisclosed or "other."

adequacy, with all items run simultaneously in EFA (*see Table 3*). All indicators loaded on the latent variables they were intended to measure, with insignificant cross-loadings of items. Furthermore, most of the factor loadings ranged between 0.7 and 0.88, as shown in the table. This confirms the face/content and factorial validity of the instrument. 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 items measuring one and the same construct. These results suggest that both discriminant and convergent validity were established through the classical EFA approach.

Structural Equation Modeling

The covariance structure model has two parts: the measurement model (sometimes referred as the CFA stage), and the structural model (also known as the SEM stage) [33]. The CFA stage was performed on the entire set of items simultaneously, with each observed variable restricted to load on its a priori factor. All the necessary steps in the validation and reliability assessment of the measurement model were conducted following Byrne [8] and Stewart and Segars [65]. The results of the most commonly used fit indices are shown in Table 4.

The analysis resulted in a converged, proper solution with a low χ^2 per degree of freedom and a good fit as indicated by all the listed fit indices. Collectively, the data from the model's fit indices, factor loadings, *t*-values, and squared multiple correlations suggest that the indicators account for a large portion of the variance of the corresponding latent construct and therefore support the validity of the measures (*see Table 5*) [6]. Discriminant validity is supported if the correlations between constructs are not equal or close to 1.00 within the 95 percent confidence intervals [4]. This clearly is the case for the model, because the highest value of the correlations is far from 1.00, lying in the interval (0.42 ± 1.96 [0.05]) or between 0.32 and 0.52. After the measurement model was finalized, the hypothesized model was tested by employing the LISREL structural model.

Item	Mean	Standard deviation	Corrected item-total correlation	Internet literacy	Social awareness	PCIA	Intention to transact
				$\alpha = 0.87$	$\alpha = 0.87$	$\alpha = 0.89$	$\alpha = 0.84$
IL1	4.38	0.72	0.61	0.70	0.20	0.03	0.21
IL2	3.93	1.07	0.72	0.85	0.10	-0.11	0.28
IL3	3.62	1.19	0.64	0.76	0.15	0.03	0.21
IL4	4.05	1.01	0.80	0.88	0.09	-0.03	0.19
SA1	3.55	1.05	0.67	0.01	0.78	0.08	0.12
SA2	3.43	0.93	0.68	0.05	0.78	0.07	0.08
SA3	3.66	0.95	0.60	0.12	0.70	-0.01	0.07
SA4	3.84	0.91	0.77	0.16	0.84	0.04	0.06
SA5	3.33	0.96	0.62	0.31	0.75	-0.05	0.02
SA6	3.24	0.98	0.66	0.18	0.74	0.06	-0.03
PC1	3.78	0.67	0.67	-0.03	0.05	0.78	-0.07
PC2	3.84	0.77	0.77	-0.07	0.00	0.80	-0.05
PC3	3.86	0.86	0.86	-0.05	0.11	0.86	-0.01
PC4	3.73	0.78	0.78	-0.01	0.06	0.77	-0.05
IU1	3.41	1.11	0.68	-0.11	0.16	0.01	0.78
IU2	2.85	1.14	0.62	-0.11	0.19	-0.14	0.64
IU3	3.15	1.15	0.80	-0.15	0.13	-0.03	0.85
IU4	3.12	1.25	0.64	-0.14	0.11	0.00	0.76

Table 3. Exploratory Factor Analysis of All Items Run Simultaneously.

Note: Shown are the items' means, standard deviations, corrected item-total correlations, and factor loadings. Cronbach's α is shown for each factor.

Goodness of fit measures	Good model fit ranges	CFA model values	SEM model values
Chi-square (*d.f.*)	Nonsignificant	320.83 (129) $p < 0.001$	321.91 (130) $p < 0.001$
Normed chi-square/degrees of freedom	< 2.0	2.48	2.48
NFI (normed fit Index)	> 0.90	0.92	0.92
CFI (comparative fit index)	> 0.90	0.95	0.95
IFI (incremental fit index)	> 0.90	0.95	0.95
RFI (relative fit index)	> 0.80	0.91	0.91
GFI (goodness of fit index)	≈ 0.90	0.92	0.92
AGFI (adjusted goodness of fit index)	> 0.8	0.90	0.90
PGFI (parsimony goodness of fit index)	> 0.5	0.70	0.70
RMR (standardized root mean square residual)	< 0.05	0.055	0.057
RMSEA (root mean square error of approximation)	< 0.8	0.058	0.058

Table 4. Goodness of Fit CFA and SEM Model Assessments.

Hypothesis Testing

The structural model's SEM stage specifies the direct and indirect causal relationships among the constructs and the amount of unexplained variance [2]. As stated in the hypotheses, the structural model tests the relationships between Internet privacy concerns (PC), Internet literacy, social awareness, and intention to transact on-line (i.e., e-commerce transactions). In SEM terms, the exogenous variables are privacy concerns, Internet literacy, and the social awareness, and the endogenous variable is the intention to transact. The structural model shows the completely standardized parameter estimates between all latent variables (*see Figure 2*). The results strongly supported all the hypotheses of the study, and the regression coefficients are all statistically significant at level 0.01.

Discussion and Limitations

The purpose of this research was to better understand whether social awareness and Internet literacy are related to Internet privacy concerns and how all three of these antecedents are related to use of the Internet for e-commerce purposes. The findings reported in the preceding section strongly support the relationships described in the hypotheses. As shown in Figure 2, all of the relationships indicated in the hypotheses are statistically significant at level 0.01. The negative relationship between privacy concerns and intention to transact (–0.39) support H1, thus confirming previous findings [16, 17, 18]. As hypothesized in H2, Internet literacy proves to be negatively related to privacy concerns (–0.17). Indeed, savvy and literate Internet users are more likely to be able to deal with privacy-invasive technologies, customize their browsers or Internet applications, eliminate surreptitious software programs running

Latent variable	Item symbol	Unstandardized factor loadings	Completely standardized factor loadings	Factor loadings error term	*t*-value	R^2
Privacy concerns (PC)	PC1	0.75	0.70	0.05	15.83	0.50
	PC2	0.92	0.83	0.05	20.14	0.69
	PC3	0.94	0.93	0.04	24.01	0.86
	PC4	0.80	0.76	0.05	17.70	0.57
Intention to transact (IU)	IU1	0.85	0.77	0.05	17.89	0.59
	IU2	0.79	0.69	0.05	15.49	0.50
	IU3	1.03	0.92	0.05	22.95	0.84
	IU4	0.88	0.71	0.06	15.96	0.50
Internet literacy (IL)	IL1	0.84	0.78	0.05	18.28	0.60
	IL2	0.80	0.67	0.05	15.05	0.46
	IL3	0.88	0.89	0.04	22.40	0.80
	IL4	0.95	0.84	0.05	20.56	0.71
Social awareness (SA)	SA1	0.79	0.75	0.05	17.10	0.56
	SA2	0.68	0.73	0.04	16.56	0.53
	SA3	0.64	0.66	0.04	14.53	0.44
	SA4	0.76	0.84	0.04	20.44	0.71
	SA5	0.64	0.65	0.05	14.31	0.43
	SA6	0.84	0.72	0.05	16.71	0.51

Table 5. Confirmatory Factor Analysis of All Constructs.

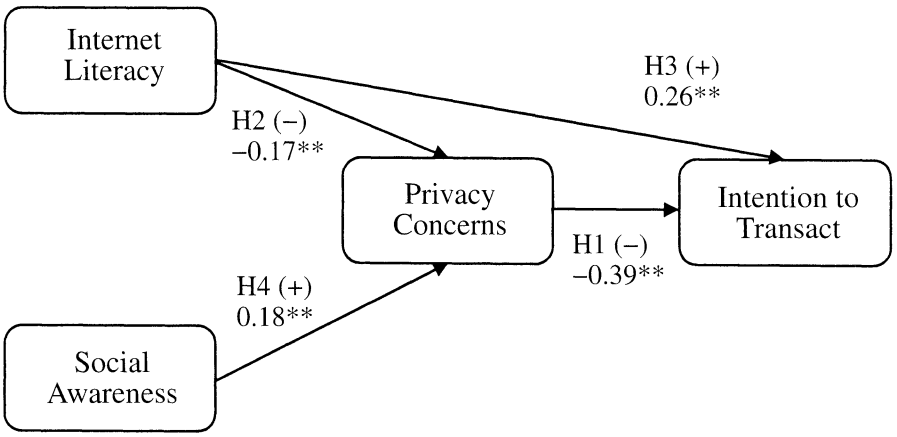

Figure 2. Structural Equation Model with Parameter Estimates

Notes: The numbers represent the completely standardized parameter estimates of the structural equation model; ** $p < 0.1$.

on background, and keep up with the latest antivirus, antispam applications. Such users feel they have more control over their computers, and as a result their privacy concerns are significantly lower. Individuals with high Internet literacy will also have higher intention to use the Internet, as confirmed by the findings related to H3 (0.26).

There is, however, another, "intuitively felt" aspect of the relationship between Internet literacy and privacy concerns. One might argue that a more technically literate Internet user would be more able to grasp the seriousness, the core vulnerabilities, and the insecurities of the Internet and the networked information systems, and therefore have stronger privacy concerns. While the direction of such a relationship is the opposite of the one supported in this study, the complexity of these relationships, both positive and negative, needs to be recognized and further investigated. Both aspects should be addressed in future research, and a more complete model will be necessary to answer how and under exactly what circumstances the negative aspect of the relationship will override the positive one to result in a totally negative regression coefficient, as shown in the results in Figure 1.

Social awareness was positively related to privacy concerns (0.18), supporting H4. Thus, individuals who are aware of the social and political processes tend to exhibit more privacy concerns with respect to Internet use. This is an important finding that has both theoretical and empirical significance. Social awareness has not been researched as a construct in the MIS literature, nor has its relationship to privacy concerns been investigated. With the increased integration of on-line communications and the Internet into everyday life, their social role increases as well. Thus, users' attitudes, their antecedents, and their consequences are important factors that need to be studied in order to understand the social impact of information technologies, and of the Internet in particular.

Several important implications arise from this study. First, as a theoretical and empirical contribution, the study identifies and validates two relatively new antecedents of Internet privacy concerns: Internet literacy and social awareness. The proposed structural model was tested with strong empirical data that confirmed the measurement properties of the new constructs and provided strong support for the proposed hypotheses.

This study is an empirical contribution to the literature on the role of privacy in on-line environments and the importance of privacy for Internet use [16, 17, 18]. With a large and diverse sample, taken over several periods for two years, the negative relationship between privacy concerns and intention to transact, as stated in H1, is again one of the strongest (–.39). Thus, along with trust [38, 45, 66, 70], privacy concerns prove to be a strong factor that may influence e-commerce use.

So far as is known, this study is the first to introduce the concept of awareness in the IS literature. Awareness is an integral part of the study of voluntary behavior in psychology and the social sciences (e.g., sexual awareness, situational awareness, the role of awareness in disease prevention, in crime prevention, child or spouse abuse, social injustices, minority groups movements, election processes, etc.). Historically, the development of MIS research has revolved around technology adoption in organizations where adoption is mandatory. With the penetration of personal computers, the Internet, and Internet technologies in everyday life, the issue of the voluntary use of technology, and accepting and managing its consequences, reveals the need once again to study the technology-adoption process. The key factors in voluntary use are awareness, raised consciousness, and knowledge about a certain technology and its personal and social benefits and risks. The decision to use a Web site for e-commerce is a type of voluntary technology acceptance [52, 53]. This study is limited to social awareness and how it affects and forms privacy concerns when a user is asked to submit personal information on-line. While social awareness does not directly affect intention to transact, the implications of the study's introduction of awareness can be seen in other types of IT research. For example, adopting technologies that control spyware, computer viruses, and scams, and avoiding falling victim to spoofing Web sites, are all related to raising one's awareness of existing problems and the need to find adequate solutions. The contribution of this study is its development and introduction of the concept of social awareness in relation to Internet privacy concerns. The instrument for social awareness developed in the study is general and can be adapted easily to any specific type of awareness appropriate for an IT study.

This is the first study to empirically validate the relationship between Internet literacy and privacy concerns, and social awareness and Internet privacy concerns. From the discovery point of view, the study broadens our understanding of the concept of information privacy and examines alternatives antecedents to Internet privacy concerns. In the information age and global economy, it is of the utmost importance to understand the role of these factors in user decisions to take advantage of all benefits the Internet offers.

From the managerial perspective, the study clearly establishes that Internet literacy is related to privacy concerns. Considering the previous studies show-

ing that privacy concerns are related to Internet use, this study concludes that low Internet literacy, inability to manage security risks and privacy invasions, may impede Internet usage even more through higher privacy concerns. Thus the IT industry needs to develop software technologies that are more user friendly to manage security and privacy threats. It needs to give users the ability to control and adjust the levels of intrusion and the amount of personal information submitted to a comfortable level of interactivity.

Higher social awareness among Internet users will help build more effective information management and information policies that employ fair information practices [14, 15, 16]. Since policy changes and organizational information practices are usually reactive to consumer or employee pressure [46, 47, 59], they will change in an easier and more effective way when citizens are more aware of the benefits, difficulties, pitfalls, or risks involved. Social awareness will play an important role in shaping public attitudes toward government surveillance. The latter has intensified in most countries in response to the threat of terrorism and criminal behavior. However, the other side of surveillance and monitoring the Internet activities is the loss of privacy and personal intrusion by overzealous agencies. Through raised awareness and consequent active engagement, the public will facilitate government surveillance policies and practices to develop a healthy degree of protection and security.

Although the two constructs introduced here have a continuous nature, the study can help in identifying segments of Internet users with respect to their privacy concerns and their Internet literacy and social awareness (*see Table 6*). For example, users with high social awareness and low Internet literacy tend to be the ones with the highest privacy concerns. These users may constitute a very broad group of adults who represent the intellectual core of society but are not able (or willing) to keep up with demanding technologies in order to protect themselves from privacy invasions while using the Internet. Among these users may be teachers, journalists, writers, economists, lawyers, doctors, and social workers. Intellectual leaders in the "soft sciences" not only have great influence on policies and regulations, but also are among the most attractive target groups for e-commerce businesses from the marketing perspective. At this point it is not clear how their Internet use would be affected if their very intense privacy concerns are not addressed and mitigated by other factors. There may be a tolerance threshold at which these users would estimate that it is not worth the risk of shopping on-line or of providing personal information given the abundance of security, virus, and spoof threats. This argument seems to find support in the Forrester research findings about eroding confidence in credit card security [36].

On the opposite end of the spectrum of Internet users, there is another distinct group, users with high technical (Internet) literacy and low social awareness. Believing they can handle intrusions by building and using strong protections, these users would tend not to rely on society to solve privacy problems through policies and regulations. Besides, they don't follow policies and issues on the social scene. These users constitute the group of technically savvy Internet users often referred to as "computer geeks." There may be a more complex, nonlinear relationship between Internet literacy and privacy

	Low Internet literacy	High Internet literacy
Low social awareness	Unknown	Lowest privacy concerns Computer and technology geeks
High social awareness	Highest privacy concerns Soft-science intellectuals	Industrial visionaries and technology creators High concern for privacy of individuals in society; low privacy concern for themselves

Table 6. Segmentation of Internet Users by Privacy Concerns.

concerns for members of this segment. Better able to protect their privacy, these individuals may exhibit a U-type of relationship, initially negative (until they discover a suitable protection) and then positive. They are not very worried about their privacy being compromised and consequently would be among the most frequent e-commerce and Internet users engaging in the most diverse spectrum of Internet applications. Among these users one can identify younger generations of engineers and software technicians with some kind of education or experience in networks and computers.

A further segment comprises technically competent, well-informed Internet users who keep on the cutting edge of Internet technology. They know how to protect their computers and their privacy and use many measures to do so. They may even participate in creating the technologies. They are also politically and socially engaged and have high social awareness. Individuals from this group, because of their high social awareness, would indeed have high privacy concerns, probably more from empathy for other citizens, and would recognize the importance of privacy and security as social issues. At the same time, however, these individuals, because of their high Internet literacy and their ability to take the necessary preventive measures, would exhibit lower privacy concerns and concerns about being intruded on-line. Thus, they are likely to be savvy and diversified Internet users who are always watchful and alert for unpleasant surprises. The segmentation of Internet users with respect to the factors considered in this study has important implications for marketers, IT managers, Web designers, and policymakers.

Although its results confirm the hypothesized relationships, the study has some limitations. It considered only two antecedents of privacy concerns, but the literature recognizes several other antecedents, such as ability to control information and perceptions of vulnerability. The study confirms the statistical significance of the relationships but does not test them within the nomological network of the other antecedents, so the relative importance of each of the various antecedents cannot be estimated. Another weakness of the model is the lack of salient factors like trust and perceived risk of Internet use and, in particular, of intention to transact with a B2C e-commerce site. The model is simplistic in this respect, but the authors intend to incorporate the important factors of trust, risk, technology acceptance model (TAM) construct, and privacy into a more complex model with more factors and antecedents.

As with most empirical studies, the sample size and spectrum of respondents are a limitation. Although a concerted effort was made to include a range of respondents representing different social groups of Internet users, the sample was limited to a single geographical region of the United States. A statistically random sample would have increased confidence in the results or would have produced different results. Furthermore, in light of the globalization of information and e-commerce, it is of the utmost importance to shift the focus of the study from American society and explore the relationships in other cultures. Surprises can be expected, for many societies are not as individualistic as the American (e.g., many Asian cultures), and some place much greater emphasis on data protection than does the United States (in particular, European nations and some former British colonies). Any study of information privacy is accordingly culturally relative. The researchers plan to extend the study to European countries in order to explore how cultural differences affect the relationships.

REFERENCES

1. Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*. Monterey, CA: Brookes, 1975.
2. Anderson, J.C., and Gerbing, S.W. Structural equation modeling in practice: a review and recommended two-step approach. *Psychological Bulletin, 103*, 3 (1988), 411–423.
3. Arthur, C. Hackers, shopfronts and worms: How fraud on the Internet costs customers £100,000 a day. *Independent*, November 11, 2003.
4. Bagozzi, R.P. Structural equation models in marketing research. In W.D. Neil (ed.), *First Annual Advanced Research Techniques Forum.* Chicago: American Marketing Association, 1991, pp. 335–379.
5. Bickford, D.M., and Reynolds, N. Activism and service-learning: Reframing volunteerism as acts of dissent. *Critical Approaches to Teaching Literature, Language, Composition and Culture, 8*, 2 (2002), 229–252.
6. Bollen, K. *Structural Equations with Latent Variables*. New York: Wiley, 1989.
7. Burn, J., and Loch, K. The societal impact of the World Wide Web—Key challenges for the 21st century. *Information Resources Management Journal, 14*, 4 (2001), 4–14.
8. Byrne, B. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*. Hillsdale, NJ: Lawrence Erlbaum, 1998.
9. Carroll, B. Price of privacy: Selling consumer databases in bankruptcy. *Journal of Interactive Marketing, 16*, 3 (2002), 47–58.
10. Clark, L.A., and Watson, D. Constructing validity: Basic issues in objective scale development. *Psychological Assessment, 7*, 3 (1995), 309–319.
11. Clarke, R.A. Information technology and dataveillance. *Communications of the ACM, 31*, 5 (1998), 498–512.
12. Cohen, J.E. Examined lives: Informational privacy and the subject as object. *Stanford Law Review, 52*, 1 (2000), 1373–1437.

13. Cranor, L.; Reagle, J.; and Ackerman, M. Beyond concern: Understanding Net users' attitudes about online privacy. In I. Vogelsang and B.M. Compaine (eds.), *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*. Cambridge, MA: MIT Press, 2000, pp. 47–70.
14. Culnan, M.J. "How did they get my name?" An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*, 3 (1993), 341–363.
15. Culnan M.J. Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing, 9*, 2 (1995), 10–19.
16. Culnan, M.J., and Armstrong, P.K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organizational Science, 10*, 1 (1999), 104–115.
17. Dinev, T., and Hart, P. Privacy concerns and Internet use—A model of trade-off factors. In *Best Paper Proceedings of Annual Academy of Management Meeting.* Briarcliff Manor, NY: Academy of Management, 2003, pp. 131–137.
18. Dinev, T., and Hart, P. Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behavior and Information Technology, 23*, 6 (2004), 413–423.
19. Etzioni, A. *The Limits of Privacy*. New York: Basic Books, 1999.
20. Giroux, H.A. Citizenship, public philosophy, and the struggle for democracy. *Educational Theory, 37*, 1 (1987), 103–120.
21. Goodwin, C. Privacy: Recognition of a consumer right. *Journal of Public Policy and Marketing, 10*, 1 (1991), 149–166.
22. Grazioli, S., and Jarvenpaa, S. Consumer and business deception on the Internet: Content analysis of documentary evidence. *International Journal of Electronic Commerce, 7*, 4 (summer 2003), 93–118.
23. Greene, S.P., and Kamimura, M. Ties that bind: Enhanced social awareness development through interactions with diverse peers. Paper presented at the annual meeting of the Association for the Study of Higher Education, Portland, OR, 2003, pp. 213–228.
24. Gutek, B.A.; Winter, S.J.; and Eriksson, I.V. Measuring computer literacy in the context of work: Development and initial validation. *Transactions in International Information Systems: Systems Analysis and Development Theory and Practice, 2*, 1 (2000), 53–72.
25. Harris Interactive. The Harris poll—Privacy (2001, 2002). Available at www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=113/.
26. Harris Interactive. Most people are privacy pragmatists who, while concerned about privacy, will sometimes trade it off for other benefits. March 19, 2003. Available at www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=597/.
27. Harvey, C. Optimism outduels pessimism—Breakthroughs in medicine, technology are forecast; but the auto is still here. *Wall Street Journal*, September 16, 1999, A10.
28. Hepburn, M.A. What is our youth thinking? Social-political attitudes of the 1980s. *Social Education, 49*, 4 (1985), 671–677.
29. Hinkin, T.R. A brief tutorial on the development of measures for use in survey questionnaires. *Organizational Research Methods, 1*, 1 (1998), 104–121.

30. Hulme, G.V. Microsoft releases of security updates. *Information Week*, April 19, 2004, 34–36.
31. IBM Multi-national consumer privacy survey, 1999. Available at www.asc.upenn.edu/usr/ogandy/ibm_privacy_survey_oct991.pdf.
32. Jones, M.G. Privacy: A significant marketing issue for the 1990s. *Journal of Public Policy and Marketing, 10*, 1 (1991), 133–148.
33. Joreskog, K., and Sorbom, D. *LISREL 7 User's Reference Guide*. Chicago: Scientific Software, 1989.
34. Juang, W.; Lei, C.; and Liaw, H. Privacy and anonymity protection with blind threshold signatures. *International Journal of Electronic Commerce, 7*, 2 (winter 2002/3), 143–157.
35. Kelvin, P. A social-psychological examination of privacy. *British Journal of Social Clinical Psychology, 12*, 3 (1973), 248–261.
36. Kelley, C.; Delhagen, K.; and Yuen, E.H. Online credit card security confidence erodes. Forrester Research, July 25, 2003. Available at www.forrester.com/ER/Research/Brief/0,1317,17220,FF.html.
37. Laufer, R.S., and Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*, 3 (1977), 22–42.
38. Lee, M., and Turban, E. A trust model for consumer Internet shopping. *International Journal of Electronic Commerce, 6*, 1 (fall 2001), 75–91.
39. Levi, A., and Koc, C. Risks in email security. *Communications of the ACM, 44*, 8 (2001), 112–113.
40. Luehrmann, A. Computer literacy—What should it be? *Mathematics Teacher, 74*, 1 (1981), 9–15.
41. Lyon, D. *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK: Open University Press, 2001.
42. Margulis, S.T. Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*, 1 (1977), 5–10.
43. Margulis, S.T. Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*, 2 (2003), 243–261.
44. Mason, R.O. Four ethical issues of the information age. *MIS Quarterly, 10*, 1 (1986) 4–12.
45. McKnight, D.H., and Chervany, N.L. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*, 2 (winter 2001/2), 35–59.
46. Milberg, S.J.; Burke, S.J.; Smith, H.J.; and Kallman, E.A. Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*, 12 (1995), 65–74.
47. Milberg, S.J.; Smith, H.J.; and Burke, S.J. Information privacy: Corporate management and national regulation. *Organization Science, 11*, 1 (2000), 35–57.
48. Myers, J.P. The new generation of computer literacy. *ACM SIGCSE Bulletin, 21*, 1 (1989), 177–181.
49. Nunnally, J. *Psychometric Theory*. New York: McGraw-Hill, 1978.
50. O'Neil, D. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*, 1 (2001), 17–31.
51. Papazafeiropoulou, A., and Pouloudi, A. Social issues in electronic

commerce: Implications for policy makers. *Information Resources Management Journal, 14*, 4 (2001), 24–32.
52. Pavlou, P.A. What drives electronic commerce? A theory of planned behavior perspective. In *Best Paper Proceedings of Annual Academy of Management Meeting, Denver.* Briarcliff Manor, NY: Academy of Management, 2002, pp. 213–219.
53. Pavlou, P.A. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*, 3 (spring 2003), 101–134.
54. Perry, W. *Forms of Intellectual and Ethical Development in the College Years: A Scheme*. New York: Holt, Rinehart & Winston, 1970.
55. Piaget, J. *The Equilibrium of Cognitive Structures: The Central Problem of Intellectual Development*. Chicago: University of Chicago Press, 1975/1985.
56. Ranganathan, C., and Ganapathy, S. Key dimensions of business-to-user Web sites. *Information and Management, 39*, 3 (2002), 457–465.
57. Rindfleish, T.C. Privacy, information technology, and health care. *Communications of the ACM, 40*, 8 (1997), 92–100.
58. Segars, A.H., and Grover, V. Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Quarterly 17*, 4 (1993), 517–529.
59. Smith, H.J. Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*, 12 (1993), 105–122.
60. Smith, G.T., and McCarthy, D.M. Methodological considerations in the refinement of clinical assessment instruments. *Psychological Assessment, 7*, 3 (1995), 300–308.
61. Smith, H.J.; Milberg, S.J.; and Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*, 2 (1996), 167–196.
62. Spiekermann, S.; Grossklags, J.; and Berendt, B. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of EC'01: Third ACM Conference on Electronic Commerce.* New York: Association for Computing Machinery, 2001, pp. 38–47.
63. Staples, B. The battle against junk mail and spyware on the Web. *New York Times*, January 3, 2004, A14.
64. Steinem, G. *Outrageous Acts and Everyday Rebellions*. New York: American Library, 1983.
65. Stewart, K.A., and Segars, A.H. An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13*, 1 (2002), 36–49.
66. Suh, B., and Han, I. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce, 7*, 3 (spring 2003), 135–161.
67. Swift, J.S. Social consciousness and career awareness. ASHE-ERIC Higher Education Reports. Washington, DC: George Washington University, School of Education, 1990.
68. Swire, P.P. Financial privacy and the theory of high-tech government surveillance. *Washington University Law Quarterly, 77*, 2 (1999), 461–513.
69. Swire, P.P. Efficient confidentiality for privacy, security, and confidential

business information. In R.E. Litan and R. Herring (eds.), *Brookings-Wharton Papers on Financial Services.* Washington, DC: Brookings Institution Press, 2003, pp. 273–310.
70. Tan, Y.-H., and Thoen, W. Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce, 5*, 2 (winter 2000/2001), 61–74.
71. Taylor, C. What spies beneath (your PC). *Time* (October 2, 2002), 106–108.
72. Tillman, B. Internet privacy legislation emerges: New legislation could bring U.S. privacy protection laws into step with those of the European Union. Legislative and regulatory update. *Information Management Journal, 36*, 5 (2002), 14–18.
73. Tsui, L. Effects of campus culture on students' critical thinking. *Review of Higher Education, 23*, 4 (2000), 421–441.
74. UCLA, Los Angeles, Center for Communication Policy. Surveying the digital future. October 2000. Available at www.digitalcenter.org/pdf/InternetReportYearOne.pdf, accessed November 19, 2005.
75. UCLA, Los Angeles, Center for Communication Policy. Surveying the digital future—Year two. November 2001. Available at www.digitalcenter.org/pdf/InternetReportYearTwo.pdf, accessed November 19, 2005.
76. UCLA, Los Angeles, Center for Communication Policy. Surveying the Digital Future—Year three. January 2003. Available at www.digitalcenter.org/pdf/InternetReportYearThree.pdf, accessed November 19, 2005.
77. Venkatraman, N. Strategic orientation of business enterprises: The construct, dimensionality, and measurement. *Management Science, 35*, 8 (1989), 942–962.
78. Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967.
79. Westin, A. Prepared witness testimony. Opinion surveys: What consumers have to say about information privacy. House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection. W.J. "Billy" Tauzin, Chairman, May 8, 2001. Available at http://energycommerce.house.gov/107/hearings/05082001Hearing209/Westin309.htm.
80. Zhang, Y., and Espinoza, S. Affiliations of computer self-efficacy and attitudes with need for learning computer skills. *Journal of Educational Computing Research, 17*, 3 (1997), 371–383.

Appendix

Privacy Concerns and Intention to Transact Items

Construct	Item symbol	Item
Privacy concerns (PC)		Rate the extent to which you agree with the following:
	PC1	I am concerned that the information I submit on the Internet could be misused.
	PC2	When I shop on-line, I am concerned that the credit card information can be stolen while being transferred 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.
Intention transact (IU)		To what extent are you willing to use the Internet to do the following?
	IU1	Purchase goods (e.g., books, CDs) or services (e.g., airline tickets, hotel reservations) from Web sites that require me to submit accurate and identifiable information (i.e., credit card information).
	IU2	Retrieve information from Web sites 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 Web sites).
	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 Web sites that allow me to access my bank account or credit card account).

TAMARA DINEV (tdinev@fau.edu) is an assistant professor in the Department of Information Technology and Operations Management at Florida Atlantic University, Boca Raton. She received her Ph.D. in theoretical physics in 1997. Following several senior positions in IT companies, she became interested in MIS research and joined the Florida Atlantic University faculty in 2000. Her research interests include Internet privacy and trust in on-line vendors, multicultural aspects of e-commerce use, Internet self-efficacy, and anxiety of Internet users. She has published in *Communications of the ACM* and *Behavior and Information Technology* and has made numerous conference presentations. In 2003 she received the Best Paper Award for the OCIS division at the Academy of Management Meeting, Seattle.

PAUL HART (hart@fau.edu) is associate professor and chair of the Department of Information Technology and Operations Management at Florida Atlantic University, Boca Raton. He is also the assistant director of the InternetCoast Institute at Florida Atlantic University. His research interests include the role of computer networks in organizational boundaries and relations between customer and supplier firms; trust in on-line transactions, Web page design and impression management; co-location

requirements in engineering design environments; communication genres and video teleconferencing, and information privacy. He has published in a number of journals, including *Organization Science* and *Journal of Management Information Systems*. In 2003, he received the Best Paper Award for the OCIS division at the Academy of Management Meeting, Seattle.