Behaviour & Information Technology
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tbit20

Internet privacy concerns and their antecedents - measurement validity and a regression model

Tamara Dinev [a] & Paul Hart [b]

[a] Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, FL, 33431, USA E-mail:

[b] Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, FL, 33431, USA

Version of record first published: 08 Nov 2010.

To cite this article: Tamara Dinev & Paul Hart (2004): Internet privacy concerns and their antecedents - measurement validity and a regression model, Behaviour & Information Technology, 23:6, 413-422

To link to this article: http://dx.doi.org/10.1080/01449290410001715723

BEHAVIOUR & INFORMATION TECHNOLOGY, NOVEMBER–DECEMBER 2004, VOL. 23, NO. 6, 413–422

Internet privacy concerns and their antecedents – measurement validity and a regression model

TAMARA DINEV and PAUL HART

Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA; e-mail: tdinev@fau.edu

Abstract. This research focuses on the development and validation of an instrument to measure the privacy concerns of individuals who use the Internet and two antecedents, perceived vulnerability and perceived ability to control information. The results of exploratory factor analysis support the validity of the measures developed. In addition, the regression analysis results of a model including the three constructs provide strong support for the relationship between perceived vulnerability and privacy concerns, but only moderate support for the relationship between perceived ability to control information and privacy concerns. The latter unexpected results suggest that the relationship among the hypothesized antecedents and privacy concerns may be one that is more complex than is captured in the hypothesized model, in light of the strong theoretical justification for the role of information control in the extant literature on information privacy.

1. Introduction

Privacy has been a topic of interest to researchers in a number of disciplines including psychology (e.g. Kelvin 1973) and sociology (e.g. Etzioni 1999). However, in recent years, the explosive growth of information technology has fuelled debate about threats to privacy and, in particular, attracted the attention of information systems researchers. Prominent examples include the work of Mason (1986), Smith (1993), Culnan (1993, 1995), Milberg *et al*. (1995), Smith *et al*. (1996), Culnan and Armstrong (1999), Stewart and Segars (2002).

While we believe that interest in information privacy would have remained strong, the events of September 11th and the US government's initiatives to increase homeland security may prove to be an important catalyst in fuelling the debate about privacy protection for citizens of the USA (Johnston and van Natta 2001, Toner and Lewis 2001, Toner 2001), of European countries (Hoge 2001) and of other countries as well. This debate, in turn, could generate even more interest on the part of researchers over time.

The focus of the research reported here is on the antecedents to privacy concerns of individuals who use the Internet. Identifying the predictors of withholding or surrendering personal information when using the Internet is important for researchers interested in exploring the complexity of user behaviour when browsing for information and conducting transactions on the web. This research has further implications for managers seeking to encourage online shopping. In this paper we report on the development and validation of an instrument to measure privacy concerns and two antecedents, perceived vulnerability and perceived ability to control information. In addition, we use a linear regression model to explore hypothesized relationships among model constructs.

2. A theoretical model of privacy concerns

Increase in concern over protecting privacy has parallelled the development of digital network and storage technologies. The extant literature on information privacy can be differentiated by the focal parties engaged in information exchange. For example, one strand of research focuses on the exchange of information between employees and an organization. Employee perceptions of privacy values and beliefs have been examined across different types of organizations, and the consequences of different regulatory approaches have been investigated (Kelvin 1973, Tolchinsky *et al*. 1981, Stone *et al*. 1983, Milberg *et al*. 1995, Smith and Kallman 1995, Smith *et al*. 1996, Milberg *et al*. 2000).

Behaviour & Information Technology
ISSN 0144-929X print/ISSN 1362-3001 online © 2004 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/01449290410001715723

Another strand of research focuses on the exchange of information between consumers and corporations. Indeed, in recent years, the primary threat to privacy has been attributed to large corporations (e.g. banks, lending institutions, credit card, marketing, and insurance companies) that use information technologies to improve efficiencies and extend market scope. These issues have been addressed in theoretical and empirical research (e.g. Mason 1986, McCrohan 1989, Jones 1991, Culnan 1993, 1995, Rindfleish 1997, Thomas and Mauer 1997, Clarke 1998, Culnan and Armstrong 1999, Petty 2000, Phelps *et al.* 2000).

More recently, another strand, or sub-strand, of research has emerged which focuses on the exchange of information between Internet users and Internet goods, services, and information providers. Most of the research to date has focused on providers in the private sector. However, there is every reason to believe that in the future, researchers will be increasingly interested in interactivity with websites supported by government agencies, non-profit organizations, and shared-interest groups as well.

Culnan (2000) and Miyazaki and Fernandez (2000) examined Internet retail disclosures and self-regulatory practices. Their findings were consistent with arguments by Milberg *et al.* (2000) about the viability of the self-regulatory mechanisms. In addition, they found that the privacy policies and adherence to them vary across industries. Sheehan and Hoy (2000) conducted an e-mail survey to examine dimensions of privacy concerns among online users. Phelps *et al.* (2000) examined privacy concerns and the consumer willingness to provide personal information. Their study addresses the trade-offs consumers are willing to make when they exchange personal information for shopping benefits. However, the study focuses on traditional direct marketing channels rather than the Internet.

Increasingly, Internet users are becoming aware of the power of Internet technologies to monitor user behaviour and to gather information about them without their knowledge. Some users might develop concerns and suspicions, sometimes unwarranted, about the 'hidden' or undisclosed purposes of free software applications or websites, which claim to facilitate their browsing experience. These concerns might inhibit interactivity resulting in more limited information exchange and aversion to experimenting with new applications and/or web sites. Indeed, privacy and the requirement to submit personal data are the primary factors that discourage users from shopping online. Only one out of three initiated online shopping procedures result in actual purchases, primarily due to the reluctance of individuals to submit personal information via the Internet (UCLA 2000, 2001, 2002). Similarly, 70% of US consumers do not register at web sites primarily because of privacy concerns and 70% are more concerned about providing information through websites compared to the telephone or e-mail (BCG 1998).

The model we tested proposes to understand the underlying antecedents to privacy concerns, namely perceived vulnerability and perceived ability to control submitted personal information when using the Internet (figure 1). These two factors account for the amount of privacy concerns users develop when determining whether to disclose personal information. They are related to a 'privacy calculus' that is, an assessment individuals make 'that their personal information will subsequently be used fairly and they will not suffer negative consequences' (Culnan and Armstrong 1999: 106). When individuals perceive that information will not be used fairly and that there will be negative consequences, they will be less likely to engage in Internet activities that require information disclosure. In other words, individuals with high privacy concerns will seek to minimize their vulnerability by limiting Internet interactivity.

The relationships between the two antecedents in our model and privacy concerns are based on definitions of privacy that have emerged among scholars from a range of disciplines, including social psychology (e.g. Kelvin 1973, Laufer and Wolfe 1977, Margulis 1977, Goodwin 1991) and social domains, including US law and everyday speech. The following common-core definition of privacy, consistent with a variety of approaches, has been proposed by Margulis (1977: 10): 'Privacy represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability'. Two constructs are embedded in this definition and are common throughout the literature: (1) the notion of vulnerability and (2) individual control over disclosure of personal

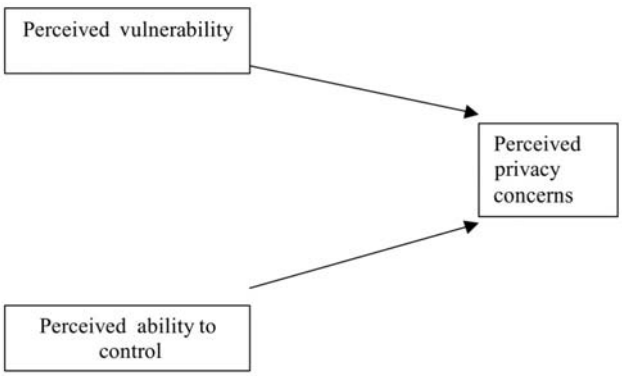

Figure 1. Model of antecedents to Internet privacy concerns.

information (Shils 1966, Westin 1967, Johnson 1974). This definition has been addressed in many studies and argued upon. Many authors reason that control and vulnerability are actually factors, among others, that shape privacy and that privacy is not control and vulnerability *per se* (see Margulis, 2003a,b). Rather, they consider control and vulnerability as factors which determine privacy state, although not exclusively. In this existing polemics we found enough justification to consider in our study control and vulnerability as separate factors, and to empirically test a model in which control and vulnerability are antecedents to the construct of privacy. Below, we present the theoretical foundation of the control and vulnerability constructs, and their relationship with privacy concerns, and the resulting hypotheses.

The notion of vulnerability emerges from the complex definition of privacy. It describes the perceived potential risk when personal information is revealed (Raab and Bennett 1998) and has been considered in the literature as a factor which determines the perceived state of privacy and individual experiences (Fusilier and Hoyer 1980, Petronio 1991, Petronio 2002). Because others may seek to use information to advance their own goals in ways that may have negative consequences for an individual, one's ability to maintain one's privacy implies an antagonism between the individual and others (Kelvin 1973). Expressing this antagonism, vulnerability is the perceived possible negative consequence of disclosure. Individuals who experience a positive outcome (e.g., a job offer) as a result of information disclosure, perceive less privacy invasion than those who did not experience a positive outcome (Fusilier and Hoyer 1980). In other words, perception of the outcome of information disclosure determines privacy concerns. Moreover, this perception of vulnerability might vary over time and thus be dependent on any given individual's experience.

Internet users are exposed to a risk of misuse and abuse of personal information that might raise the perception of vulnerability. Unauthorized access to information can be caused by any number of factors including: accidental disclosure, insider curiosity, insider subordination, unauthorized access, hacking into computer systems, security defects, scams (i.e. fraudulent web sites established for the purpose of obtaining information and money), and uncontrolled secondary usage of personal data (Rindfleish 1997). Because of these potential breaches of security, consumers risk several types of privacy invasions, including 'identity theft' (Saunders and Zucker 1999). Another type of vulnerability, involves the surreptitious collection of consumer information and consumer profiling (Budnitz 1998, FTC Report 1999). According to Culnan (2000), while 67% of the web sites post privacy disclosure, only 14% of these disclosures constitute comprehensive and fair privacy practices and policies. Similar results have been reported by Miyazaki and Fernandez (2000), with substantial differences across product categories. All these factors contribute to increasingly perceived vulnerability among Internet users, and thus, increased privacy concerns:

Hypothesis 1: There is a positive relationship between perceived vulnerability and privacy concerns.

The ability of the consumer to control submitted personal information offsets the risk of possible negative consequences. Privacy has sometimes been defined as the right to disclose information about oneself (Westin 1967). Thus, the ability to withhold information from being disclosed is a condition of that right. Technology and procedures that disallow the ability to control how or when information is disclosed can be viewed as an impediment to the execution of that right.

The definition offered by Margulis (1977), mentioned above, states that privacy involves the 'control of transactions' which would include information exchange. Control allows individuals to determine the impressions others form about them (Goffman 1963). Control is possible through limiting self-disclosure (Derlega and Chaikin 1977) or by determining how information disclosed will be used (Stone and Stone 1990). Individuals perceive information disclosure as less privacy-invasive when, among other things, they believe that they will be able to control future use of the information and that the information will be used to draw accurate inferences about them (Culnan and Armstrong 1999). When control is not allowed or when the future use of information is not known, individuals resist disclosure.

Culnan and Armstrong (1999) have argued that when procedural fairness (Lind and Tyler 1988) is applied to privacy practices in consumer marketing, individuals are more likely to assess that there will not be negative consequences in disclosing information. Thus, the result of the 'privacy calculus' is in favour of information disclosure. Procedural fairness refers to 'the perception by the individual that a particular activity in which they are participating is conducted fairly' (Culnan and Armstrong 1999: 107). They operationalized fairness in terms of procedures that provided individuals with control over disclosure and subsequent use of personal information. They found that when individuals were not informed about fair procedures, they were less willing to have personal information used. They also found that when individuals were informed about fair procedures, privacy concerns did not distinguish individuals who were willing from those who were unwilling to have

personal information used. In other words, privacy concerns washed out.

Other researchers reported similar findings. The ability to control information collection and use by third parties are not just a concern among online consumers (Sheehan and Hoy 2000) but a factor influencing the consumers' purchasing decisions (Phelps *et al.* 2000). Consumers find it unacceptable that the information about them is being collected without their consent (Nowak and Phelps 1995) and that marketers sell information about them (Nowak and Phelps 1992, Milne 2000). Cespedes and Smith (1993) found that use of consumer data without permission was viewed as an invasion of consumer privacy and that secondary usage of personal information potentially causes strenuous consumer objection (Wang and Petrison 1993). One survey indicated that 81% of the respondents 'believe that consumers have lost all control on how personal information about them is circulated and used' (Budnitz 1998). For this reason many (as much as 50%) consumers provide false information when asked to register at a web site or fill in surveys (Greenman 1999, BCG 1998).

To summarize the findings above, if people have a greater sense that they control the use of their information, they will have fewer privacy concerns. Although many researches have equated privacy concerns with control, there is ample evidence in the literature that points towards the fact that privacy is more than control, and control may be one of the variables that mediate privacy. Indeed, Laufer and Wolfe (1977), posit that while it is essential to consider the idea of control as a dimension of privacy, control is a major factor in many other issues in a highly individualized society such as the American society. They conceptualize control as a mediating variable in the privacy system. They argue that a situation is not necessarily a privacy situation simply because the individual has control. Conversely, the individual may not perceive he or she has a control, yet the environmental and interpersonal elements may create perception of privacy. Similar arguments have been advanced by Stone *et al.* (1983) and Stone and Stone (1990) where they introduce control as *one* of the privacy-related factors.

These considerations suggest that the ability to control personal information is a separate construct from privacy concerns, and that the two constructs are related. In this study, we develop a separate measurement for the perceived ability to control personal information and hypothesize that it is an antecedent to privacy concerns. Therefore, we advanced the following.

Hypothesis 2: There is a negative relationship between perceived ability to control and privacy concerns.

3. Methodology and instrument development

The research model was empirically tested using data collected from a survey. Participants were asked to fill in the survey consisting exclusively of questions, and choose what they believe was the best answer out of the provided Likert range. All items used were based on a 5-point Lickert scale. The development of the scales for the constructs considered in this study was initiated by examining prior work on similar constructs. The instruments existing in the literature, could not be readily applied to our study but provided an important guidance and base to build on. Following the best practices in scale development, we cast a wide net in identifying candidate items. Observing the trends in general survey data, following the analyses in the professional and popular literature, while reflecting on the underlying theory, we constructed an initial set of items. Privacy concerns items construction was based on the classic privacy concerns instruments developed by Smith *et al.* (1996) and further refined by Culnan and Armstrong (1999). Modification of the existing instruments were needed to reflect the specificity of the Internet, and to avoid capturing unrelated to our study set of beliefs about organizational policies, general computer anxiety, etc. The development of the control variable's items was guided by the need to extract this component from the previous privacy concerns' instruments mentioned above. The items for perceptions of vulnerability were developed by the authors based on the theoretical definitions given in the previous section.

Two pilot tests were conducted to develop the measures and these were followed by a broader survey. The first pilot test was conducted among a sample of 60 undergraduate MIS students, 15 MIS graduate students, seven employees at a banking institution, and 15 employees at a large retail store. After conducting exploratory factor analysis, reliability testing, and a careful examination of the correlations, several items were deleted, new items were added, and word modifications were made to many items resulting in an extensively revised instrument that warranted further testing.

The second pilot test was conducted among a sample of 70 undergraduate students. After careful consideration of the relevance of the items with respect to the constructs they measure, their face validity, as well as their corrected item–total correlations, some item were deleted from the instrument. Upon second examination they were found that they do not logically correlate with the rest of the items, as was also indicated by their low corrected item–total correlation. Following the same appropriate tests for data, purification of the instrument continued until the loading of the items and their validity was consistent and at satisfactory levels.

The final version of the survey was administered to a broad sample of individuals in the southeast including undergraduate and graduate students of a large university, employees of four local public schools, one large and one small high-tech company, one banking institution, three small retail and service businesses, as well as direct mailing to one neighbourhood. The response rate was 40%. The respondent profile of the final survey is presented in table 1. As seen from the demographics distribution, the sample is diverse, comprising a wide range of age, employment, education, and race, with equal representation of genders. The respondents are a heterogeneous group that may approximate a representative sample of a large population.

4. Exploratory factor analysis

Exploratory Factor Analysis (EFA) is a classical approach for establishing construct validity (Bagozzi *et al*. 1991). The potential latent sources of variance in the indicators can be discovered through EFA – items which adequately measure a latent variable should exhibit high factor loadings on that latent variable and small factor loadings on other latent variables that are measured by a different set of indicators. Such results provide an evidence of convergent and discriminant validity of the items (Segars and Grover 1993). Convergent validity indicates the extent to which different measures refer to the same conceptual construct. Discriminant validity assesses the extent to which the measure is adequately distinguishable from related constructs within the nomological net.

The primary goal of the Exploratory Factor Analysis (EFA) was to initially test the applicability and validate the proposed instrument. Reliability tests using Cronbach's alpha coefficients were used to assess the internal consistency of the scale items for each construct. In all cases, the coefficients were above 0.78 – much higher than the threshold level of 0.6 suggested for exploratory research (Nunnally 1978). The corrected item – total correlations which provide initial indications for reliability (Churchill 1979) were also high for most of the items.

Table 1. Descriptive statistics of survey respondents ($n = 369$)

Gender	Male	172 (46.6%)
	Female	197 (53.4%)
Race	White	193 (52.3%)
	Black	64 (17.3%)
	Hispanic	65 (17.6%)
	Other	47 (12.7%)
Age	< 20 years	13 (3.5%)
	21 – 30 years	245 (66.4%)
	31 – 40 years	73 (19.8 %)
	> 40 years	38 (10.3 %)
Education	High School	261 (70.7%)
	4 year college degree	67 (18.2%)
	Graduate degree	41 (11.1%)
Income	< \$60,000	257 (70.0%)
	\$61,001 – \$100,000	70 (19.0%)
	> \$100,000	33 (8.9%)
	Undisclosed	9 (2.1%)

The next stage of instrument validation was establishing convergent and discriminant validity of the items through EFA and by examining the correlations among all items of all constructs. Factor analysis with Varimax rotation and Kaiser normalization was utilized to make the initial assessment of the constructs' adequacy. All indicators loaded on the latent variables they were intended to measure, with insignificant cross-loadings of items. This ensures the face and content validity of the instrument. Furthermore, most of the factor loadings range between 0.7 and 0.9, as shown in tables 2, 3, and 4. In addition, all inter-item correlations were examined for further verification of discriminant validity. The values of the correlations between items measuring different constructs were significantly lower than the correlations between the items measuring one and the same construct. These results suggest that both discriminant and convergent validity were established through the classical EFA approach.

Tables 2, 3, and 4 list the full set of questions that were used in the final survey for each construct described in this study. A total of 26, they present the final sets of measurement of the privacy concerns – abuse (4 items) and finding (10 items), control (4 items), and vulnerability (8 items) variables. Table 2 lists the items for the privacy concerns construct. As evident from the factor loadings, the items load into two clearly defined factors. After closer examination of the items, we identified the two dimensions as privacy concerns for information finding (below referred as 'finding') and privacy concerns for information abuse (below referred as 'abuse'). The items for perceived vulnerability and perceived ability to control are listed in tables 3 and 4, respectively.

5. Regression models and testing of hypotheses

Once the measurements for the three constructs were validated following Exploratory Factor Analysis (EFA) techniques, we proceeded with hypothesis testing. This was accomplished by examining the standardized beta coefficients and the statistical significance of the relationships among the constructs, with privacy concerns constructs being the dependent variables. Examination of Pearson correlations revealed that the two

Table 2. Reliability statistics for privacy concerns

Alpha	Item	Mean	Standard deviation	Corrected item total correlation	Factor 1 ABUSE	Corrected item total correlation	Factor 2 FINDING
0.90	I am concerned that the information I submit on the Internet could be misused	3.78	1.09	0.67	0.78		
	When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet	3.84	1.11	0.77	0.82		
	I am concerned about submitting information on the Internet, because of what others might do with it	3.86	1.03	0.86	0.88		
	I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee	3.73	1.09	0.78	0.85		
0.94	When I am online, I have the feeling of being watched	2.72	1.22			0.66	0.61
	When I am online, I have the feeling that all my clicks and actions are being tracked and monitored	2.96	1.25			0.67	0.64
	I am concerned that a person can find the following information about:	x	x	x	x	x	x
	My date and place of birth, and the names of my parents	3.38	1.25			0.86	0.87
	Names and information about my immediate family members	3.36	1.23			0.86	0.88
	Addresses and telephones of my home/workplace	3.55	1.13			0.85	0.84
	Address and telephone of my current and Previous residences	3.52	1.16			0.84	0.86
	The location, the appraisal, and the price I paid for my assets/properties (house/apartment), as well as all the detailed information about my house	3.4	1.22			0.80	0.84
	My driving records	3.33	1.25			0.83	0.84
	Credit card/mortgage/other credit records	3.94	1.08			0.71	0.65

Table 3. Reliability statistics for perceived vulnerability (VULNERABILITY)

Alpha	Item	Mean	Standard deviation	Corrected item total correlation	Factor loading
0.92	Records of transactions could be sold to third parties	3.94	0.90	0.58	0.77
	Personal information submitted could be misused	3.93	0.86	0.73	0.89
	Personal information could be made available to unknown individuals or companies without my knowledge	4.11	0.82	0.71	0.84
	Personal information could be made available to government agencies	3.91	0.87	0.54	0.77
	Personal information could be inappropriately used	4.04	0.78	0.70	0.87
	Unauthorized charges could be made against credit card information submitted	3.91	0.99	0.60	0.78
	Unethical use of credit card information is attractive to some companies	3.7	1.00	0.69	0.77
	Legal but questionable use of credit card information is profitable to some companies	3.78	0.91	0.67	0.80

Table 4. Reliability statistics for perceived ability to control information (CONTROL)

Alpha	Item	Mean	Standard deviation	Corrected item total correlation	Factor loading
0.78	I would only submit accurate and personal information at a website if the site allowed me to control the information I volunteer	3.44	0.94	0.68	0.73
	I would only provide accurate and personal information at a website if the site allowed me to control the information they can use	3.5	1.00	0.73	0.78
	Being able to control the personal information I provide to a website is important to me	4.04	0.91	0.48	0.77
	I would only provide accurate and personal information at a website if their control policy is verified/monitored by a reputable third party	3.32	0.91	0.48	0.66

privacy concerns constructs, FINDING and ABUSE, were correlated – although the results of the factor analysis, described above, indicated there were also distinct constructs. This required retesting the regression models. Thus two sets of two regression models were run. The first set included two regression models for each of the dependent variables, FINDING and ABUSE, respectively, with only the hypothesized relationships (CONTROL and VULNERABILITY as antecedents) considered. The results are indicated in table 5. The second set of regression models, again each with FINDING and ABUSE, respectively, as dependent variables, was run with the alternative privacy concerns construct included as an independent variable. For example, if a regression model is run with FINDING as dependent variable, the set of independent variables includes CONTROL, VULNERABILITY, and ABUSE. The analysis reported in table 6 was undertaken to parse the independent influence of each construct on the respective dependent variable.

Table 5. Standardized beta coefficients and R^2 for privacy concerns with perceived vulnerability and perceived ability to control as independent variables

Dependent variable Independent variable	FINDING $R^2 = 0.15$	ABUSE $R^2 = 0.13$
CONTROL	NS	NS
VULNERABILITY	0.39**	0.35**

*$p < 0.05$. **$p < 0.01$. NS – Not statistically significant.

Table 6. Standardized beta coefficients and R^2 for privacy concerns with perceived vulnerability, perceived ability to control, and the alternative privacy constructs as independent variables

Dependent variable Independent variable	FINDING $R^2 = 0.36$	ABUSE $R^2 = 0.33$
CONTROL	NS	NS
VULNERABILITY	0.23**	0.15**
FINDING	–	0.50**
ABUSE	0.48**	–

*$p < 0.05$. **$p < 0.01$. NS – Not statistically significant.

6. Discussions and limitations

The purpose of this research was to develop, test, and validate measurement instruments for Internet privacy concerns, perceived ability to control submitted information and perceived vulnerability. An Exploratory Factor Analysis paradigm was used. In addition, relationships between these constructs were hypothesized and empirically tested – whether perceived vulnerability and perceived ability to control personal information submitted when using the Internet were antecedents to privacy concerns.

The results of the study, as reported here, validated the proposed instruments with high factor loadings and Cronbach's alpha which confirms the validity and reliability of the proposed instruments. In addition, two distinct privacy concerns constructs emerged from the factor analysis. A statistically significant relationship proved to exist between them, as exhibited by the Pearson correlation and the Beta regression coefficient. This suggests that users associate privacy concerns based on information access and privacy concerns based on information abuse. One possible interpretation may be that individuals believe that so long as personal information can be found on the Internet, the potential for abuse of that personal information is high. To the extent that this interpretation may be true, it surely reflects a negative assessment about the availability of personal information to be found on the Internet.

The findings provide empirical support of the propositions in this study that control and vulnerability are indeed separate constructs from privacy. The extensive Exploratory Factor Analysis and the psychometric characteristics of the constructs (as shown in tables 2, 3, and 4) show that the latent variables of the

study are distinguishable, conceptually different constructs which measure certain psychological dispositions and states of an individual using the Internet. Moreover, the analysis showed two distinguishable factors of privacy concerns – one for information finding and one for information abuse. All these well defined, validated, and conceptually and empirically clear factors – control, vulnerability, information privacy concerns and abuse privacy concerns – are related and form a complex nomological net, as stated in the hypotheses.

The findings reported in the previous section suggest partial support for the relationships described in the hypotheses and specified in the research model. As shown in tables 5 and 6, some of the relationships indicated in the hypotheses are statistically significant.

The first hypothesis focused on the relationships between perceived vulnerability and privacy concerns. The statistically significant standardized beta coefficients for vulnerability and privacy concerns about information finding (FINDING) and information abuse (ABUSE) are 0.39 and 0.35 respectively (table 5), suggesting support for these relationships. However, the standardized beta coefficients for ability to control and the two privacy concerns constructs were not statistically significant. These results will be discussed in the subsequent paragraphs.

The first set of regression models (for the two privacy constructs) run on the basis of the hypothesized relationships yielded a low R^2 of 0.15 for FINDING and 0.13 for ABUSE. Upon examining early indicators of statistical significance, such as Pearson correlations, we found a strong correlation between the two privacy constructs – FINDING and ABUSE. Although different, their correlations are statistically significant ($p < 0.01$). Therefore, each privacy construct was a good candidate to be included as an independent variable in each regression model. Thus a second set of regression models were run with the alternative privacy construct included as an independent variable, along with VULNERABILITY and CONTROL. The second set of regression models, shown in table 6, shows that both models yielded a much higher R^2 and provides a better fit for the data.

With the modified regression models, support for the two hypotheses has not changed. The standardized beta coefficients for the relationship between perceived vulnerability and FINDING and ABUSE are 0.23 and 0.15, respectively, and they are both statistically significant ($p < 0.01$). The relationships between FINDING and ABUSE are at strong 0.48 and 0.50, respectively, and statistically significant at the same level. The fact that the standardized beta coefficients for perceived vulnerability decreased from 0.39 and 0.35 (for the first set of models) to 0.23 and 0.15 (for the second set of models) is due to the masking effect of the stronger relationship of a non-present independent variable, in this case, the alternative privacy construct, in the first set of regression models.

An unexpected result of the analysis was the statistically non-significant relationship between the perceived ability to control submitted information and either of the privacy constructs. Given the strong theoretical justification supporting the relationship, this finding calls for further analysis and data collection. More rigorous statistical analysis may allow us to better understand and explain these relationships. Because 'control of transactions' is embedded in the definition of privacy, our findings have to be addressed with great caution but at the same time cannot be ignored because of the strong instrument validity and fit of the data.

One possible explanation is that the relationship is not simple. Perceived ability to control may indeed have no effect on the level of an individual's privacy concerns. It is probable that, while unidimensionality of the ability to control construct has been established, other dimensions have also been captured by the indicators. A distinction between the perceived *need* to have control over information and the actual perception that he or she indeed *has* control should be investigated in further studies. Perceived need to control information may have been captured to greater extent by the privacy concerns constructs because of the strong interdependence of the two variables, FINDING and ABUSE.

It should be noted also that the construct we are measuring is privacy concerns rather than privacy *per se*. As in most empirical studies, the phenomenon is operationalized indirectly rather than directly (i.e. through testing privacy concerns rather than privacy itself). While the definition of privacy embeds the control of transactions as integral part of the privacy construct, in our study we considered the construct of control of transaction as a separate construct that is distinct from privacy concerns. Thus the focus of the importance of control of transactions has to be on the privacy concerns. Therefore, our findings do not suggest a need to rewrite the definition of privacy. Rather, they point out that the perceived ability to control information may not be a major factor in mitigating privacy concerns when Internet transactions are involved.

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

Lastly, other factors, such as trust may play an important role in mediating the control–privacy relationship. This, in turn, would suggest that the there are more antecedents to Internet use and privacy concerns that are not captured in our theoretical model. This limitation is an argument that the antecedents to privacy concerns and their relationships to Internet use involve a complex pattern of perceptions and behaviours. Therefore, these findings also suggest the need for further empirical investigation of privacy and Internet use.

References

Bagozzi, R. P., Yi, Y., Phillips, L. W. 1991, Assessing construct validity in organizational research. *Administrative Science Quarterly*, **36,** 421–458.

BCG, Boston Consulting Group, 1998, Shop.org/BCG Survey of online customer, http://www.bcg.com.

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

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

Churchill, G. A. Jr. 1979, A paradigm for developing better measures for marketing constructs. *Journal of Marketing Research*, **16,** 64–73.

Clarke, R. A. 1998, Information technology and dataveillance. *Communications of the ACM*, **31,** 498–512.

Culnan, M. J. 1993, 'How did they know my name?' An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, **17,** 341–363.

Culnan, M. J. 1995, Consumer awareness of name removal procedures: implications for direct marketing. *Journal of Direct Marketing*, **9,** 10–19.

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

Culnan, M. J. and Armstrong, P. K. 1999, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science*, **10,** 104–115.

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

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

FTC, 1999, Self-Regulation and privacy online, *Report to Congress*.

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

Gofmann, E. 1963, *Stigma: Notes on Management of Spoiled Identity* (Englewood Cliffs, NJ: Prentice Hall).

Goodwin, C. 1991, Privacy: recognition of a consumer right. *Journal of Public Policy & Marketing*, **10,** 149–166.

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

Hoge, W. 2001, U.S. Terror attacks galvanize Europeans to tighten laws. *New York Times*, December 6, 2001.

Johnson, C. 1974, Privacy as personal control. In *Man–Environment Interactions: Evaluations and applications*, (Washington, DC: Environmental Design Research).

Johnston, D. and Van Natta, D., Jr. 2001, Ashcroft weighs easing F.B.I. limits for surveillance. *New York Times*, December 1, 2001.

Jones, M. G. 1991, Privacy: a significant marketing issue for the 1990s. *Journal of Public Policy and Marketing*, **10,** 133–148.

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

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

Lind, E and Tyler, T. R. 1988, *The Social Psychology of Procedural Justice*, (New York: Plenum Press).

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

Margulis, S. T. 2003A, On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, **59**(2), 411–429.

Margulis, S. T. 2003B, Privacy as a social issue and behavioral concept. *Journal of Social Issues*, **59**(2), 243–261.

Mason, R. O. 1986, Four ethical issues of the information age. *MIS Quarterly*, **10,** 4–12.

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

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

Milberg, S. J., Smith, H. J. and Burke, S. J. 2000, Information privacy: corporate management and national regulation. *Organization Science*, **11,** 35–37.

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

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

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

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

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

Nunnaly, J. 1978, *Psychometry Theory*, (New York: McGraw-Hill).

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

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

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

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

Raab, C. D. and Bennet, C. J. 1998, The distribution of privacy risks: who needs protection? *The Information Society*, **14**(4) 253–62.

Rindfleish, T. C. 1997, Privacy, Information Technology, and Health Care. *Communications of the ACM*, **40,** 92–100.

Saunders, K. and Zucker, B. 1999, Contracting identity fraud in the information age: the identity theft and assumption deterrence act, by, *International Review of Law, Computers & Technology*, **13,** 183.

Segars, A. and Grover, V. 1993, Re-examining perceived ease of use and usefulness: a Confirmatory Factor Analysis. *MISQ* **17**(4), 517–525.

Sheehan, K. B. and Hoy, M. G. 2000, Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, **19,** 62–75.

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

Smith, H. J. 1993, Privacy policies and practices: inside the organizational maze. *Communications of the ACM*, **36,** 105–122.

Smith, H. J. and Kallman, E. A. 1995, Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, **38**, 65–74.

Smith, H. J., Milberg, S. J. and Burke, S. J. 1996, Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, June, 167–196.

Stewart, K. A. and Segars, A. H. 2002, An empirical examination of the concern for information privacy instrument. *Information Systems Research*, **13,** 36–49.

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

Stone, E. F. and Stone, D. L. 1990, Privacy in organizations: theoretical issues, research findings, and protection mechanism. *Research in Personnel and Human Resources Management*, **8,** 349–411.

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

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

Toner, R. 2001, Few in congress questioning president over civil liberties. *New York Times*, December 5, 2001.

Toner, R. and Lewis, N. A. 2001, A familiar battle fought and won. *New York Times*, October 26, 2001.

UCLA Internet Report, 2000, 2001, 2002, Surveying the Digital Future, http://ccp.ucla.edu/pages/internet-report.asp.

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

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