Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model

Article *in* Information Systems Research · December 2004

DOI: 10.1287/isre.1040.0032 · Source: DBLP

CITATIONS
1,890

READS
7,308

3 authors:

Naresh Malhotra
Georgia Institute of Technology
194 PUBLICATIONS **22,428** CITATIONS

SEE PROFILE

Sung S. Kim
University of Wisconsin–Madison
21 PUBLICATIONS **6,520** CITATIONS

SEE PROFILE

James Agarwal
The University of Calgary
58 PUBLICATIONS **4,233** CITATIONS

SEE PROFILE

Information Systems Research
Vol. 15, No. 4, December 2004, pp. 336–355
ISSN 1047-7047 | EISSN 1526-5536 | 04 | 1504 | 0336

DOI 10.1287/isre.1040.0032

Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model

Naresh K. Malhotra
College of Management, Georgia Tech, 800 West Peachtree Street, Atlanta, Georgia 30332,
naresh.malhotra@mgt.gatech.edu

Sung S. Kim
School of Business, University of Wisconsin–Madison, 975 University Avenue, Madison, Wisconsin 53706,
skim@bus.wisc.edu

James Agarwal
Haskayne School of Business, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2N 1N4, Canada,
james.agarwal@haskayne.ucalgary.ca

The lack of consumer confidence in information privacy has been identified as a major problem hampering the growth of e-commerce. Despite the importance of understanding the nature of online consumers' concerns for information privacy, this topic has received little attention in the information systems community. To fill the gap in the literature, this article focuses on three distinct, yet closely related, issues. First, drawing on social contract theory, we offer a theoretical framework on the dimensionality of Internet users' information privacy concerns (IUIPC). Second, we attempt to operationalize the multidimensional notion of IUIPC using a second-order construct, and we develop a scale for it. Third, we propose and test a causal model on the relationship between IUIPC and behavioral intention toward releasing personal information at the request of a marketer. We conducted two separate field surveys and collected data from 742 household respondents in one-on-one, face-to-face interviews. The results of this study indicate that the second-order IUIPC factor, which consists of three first-order dimensions—namely, collection, control, and awareness—exhibited desirable psychometric properties in the context of online privacy. In addition, we found that the causal model centering on IUIPC fits the data satisfactorily and explains a large amount of variance in behavioral intention, suggesting that the proposed model will serve as a useful tool for analyzing online consumers' reactions to various privacy threats on the Internet.

Key words: information privacy; concerns for information privacy; Internet users' information privacy concerns; structural equation modeling; nomological network; causal model
History: Detmar Straub, Associate Editor. This paper was received on June 25, 2003, and was with the authors 5 months for 3 revisions.

1. Introduction

Despite the enormous potential of e-commerce, its share of the total economy remains small: less than 1% worldwide (U.S. Department of Commerce 2002). The lack of consumer confidence in online privacy has been identified as a major problem hampering the growth of e-commerce. Norman Mineta (2000), former U.S. Secretary of Commerce, remarked that the U.S. government regarded privacy as one of the most critical issues in the continued growth of the economy. In addition, a report showed that practically all Americans (94.5%), including Internet users and non-Internet users, are concerned about "the privacy of their personal information when or if they buy online" (University of California–Los Angeles Center for Communication Policy 2001, p. 44).

Personal information in a digital format can be easily copied, transmitted, and integrated, which enables online marketers to construct thorough descriptions of individuals. Therefore, this information could pose a serious threat to privacy if not properly handled; however, it also can be used to provide customers with personalized services and other benefits. In this sense, consumers, managers, and researchers should consider personal information a double-edged sword. Used carefully under proper safeguards, it can

increase public utility; but when used carelessly, its abuse can lead to invasion of information privacy (e.g., Laufer and Wolfe 1977, Culnan 2000).

During the past decade, the issue of information privacy has drawn considerable attention among researchers in disciplines such as law, public policy, marketing, organizational behavior, and information systems (Caudill and Murphy 2000, Culnan 2000, Goodwin 1991, Newman and Rao 2000, Regan 1995, Smith et al. 1996). However, much of the literature on this topic has addressed information privacy within the context of threats from traditional direct marketers (Phelps et al. 2000, Sheehan and Hoy 2000). Unlike traditional direct marketing channels, the Internet allows for interactive two-way communication and accordingly poses unique information privacy threats that differ from the issues previously addressed (Hoffman and Novak 1996, Smith et al. 1996, Sheehan and Hoy 2000). For this reason, Phelps et al. (2000, p. 40) stated that "research involving privacy and information issues related to e-commerce, however, remains primarily in a nascent stage" and called for more studies.

To maximize the potential of e-commerce, it seems critical to accurately understand online consumers' concerns for information privacy. However, although several pioneering studies exist that examine online privacy in general (e.g., Mehta and Sivadas 1995; Miyazaki and Fernandez 2000, 2001; Sheehan and Hoy 2000), few systematic attempts have been made to provide a theoretical framework on the specific nature of information privacy concerns among Internet users. To fill the gap in the literature, this article is intended to examine Internet users' information privacy concerns (IUIPC) by extending to the Internet domain the current body of knowledge centering on traditional marketing channels.

Specifically, we focus on three distinct, yet closely interrelated, issues. (1) We theoretically examine the nature and dimensionality of IUIPC; (2) we attempt to operationalize the multidimensional notion of IUIPC using a second-order construct and develop a scale for it; (3) we propose and test a causal model centering on IUIPC. Drawing on social contract (SC) theory, we propose that concerns of online consumers center on three major dimensions—namely, collection, control, and awareness of privacy practices (Donaldson 1989, Donaldson and Dunfee 1994, Dunfee et al. 1999, Phelps et al. 2000). This article also argues that the proposed model, strongly rooted in the trust-risk framework (McKnight et al. 1998) and the reasoned-action paradigm (Fishbein and Ajzen 1975), will serve as a useful tool for analyzing reactions of online consumers to various privacy threats on the Internet.

2. IUIPC

This section begins with the description of the notion of information privacy concerns and the review of existing scales designed to represent such concerns. Second, to accurately represent the privacy concerns of online consumers, we propose a second-order IUIPC factor incorporating three first-order dimensions. Finally, we develop a causal model on how IUIPC affects a consumer's reactions to a request by an online marketer for personal information.

2.1. Information Privacy, Information Privacy Concerns, and Existing Scales

Information privacy refers to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, p. 7). Although the notion of information privacy itself may sound straightforward, the practical boundary of information privacy in real life varies with numerous factors including industry sectors, cultures, and regulatory laws (Milberg et al. 1995, Culnan and Bies 2003, Andrews 2002). *Information privacy concerns* refer to an individual's subjective views of fairness within the context of information privacy (Campbell 1997). Obviously, an individual's privacy concerns will be influenced by these external conditions mentioned earlier (e.g., industry sectors, cultures, regulatory laws). However, an individual's perceptions of such external conditions will also vary with personal characteristics and past experiences (Donaldson and Dunfee 1994). Therefore, people often have different opinions about what is fair and what is not fair concerning a firm's collection and use of their personal information.

To measure individuals' concerns about information privacy, practitioners have often used a one-dimensional global information privacy concern (GIPC) scale (Smith et al. 1996). While GIPC indicates

privacy concerns in general, it is not intended to reveal the specific dimensions of such concerns. To understand the complexity of individuals' privacy concerns, Smith et al. (1996) conducted a series of studies using rigorous methodologies. Their efforts resulted in a new multidimensional scale, called concern for information privacy (CFIP), designed to capture individuals' concerns about organizational information privacy practices. The CFIP scale consists of 15 items and reflects 4 dimensions of information privacy concerns. Those four dimensions are *collection, unauthorized secondary use, improper access,* and *errors*. On the basis of a sample of 355 respondents, Stewart and Segars (2002) empirically confirmed the psychometric properties of this 15-item scale.

As a reliable and valid measure, the four-dimensional model of CFIP has been successfully applied within the context of offline direct marketing (Stewart and Segars 2002, Smith et al. 1996, Campbell 1997). However, as Smith et al. (1996) put it, "the dimensionality is neither absolute nor static, since perceptions of advocates, consumers, and scholars could shift over time" (p. 190). This is especially the case given the fundamental change in the marketing environment caused by the widespread adoption of the Internet. For instance, unlike traditional media, the Internet provides a variety of means for consumers to control personal information that is stored in an organization's database. Consequently, it is important to examine the shifting dimensions of privacy concerns because Internet users are likely to differ from offline consumers in their concerns about their personal information.

2.2. Nature of IUIPC

Consumers regard the release of personal information as a risky transaction because they become vulnerable to a company's potential opportunistic behaviors (Milne and Gordon 1993, Laufer and Wolf 1977). For this reason, a consumer's concerns about information privacy cannot be fully understood without investigating how individuals define justice in this long-term exchange of personal information. SC theory is especially useful for studying perceptions of fairness and justice (Donaldson and Dunfee 1994). This notion of SC has been applied widely to explain various phenomena including the consumer-firm relationship (Dunfee et al. 1999). This theory has also been used as a conceptual tool for explaining consumer behavior in the context of information privacy (Milne and Gordon 1993, Culnan and Bies 2003). One of the main principles of SC theory is that "norm-generating microsocial contracts must be grounded in informed consent, buttressed by rights of exit and voice" (Dunfee et al. 1999, p. 19). In other words, an equitable exchange involving a long-term relationship should be accompanied by shared understanding about contractual terms and self-control over the course of the relationship.

When applied to information privacy, SC theory suggests that a firm's *collection* of personally identifiable data is perceived to be fair only when the consumer is granted *control* over the information and the consumer is *informed* about the firm's intended use of the information. As a result, it is possible to characterize the notion of IUIPC in terms of three factors—namely, *collection, control,* and *awareness of privacy practices*. The *collection* factor captures the central theme of equitable information exchange based on the agreed social contract. Meanwhile, the *control* factor represents the freedom to voice an opinion or exit. Finally, the *awareness* factor indicates understanding about established conditions and actual practices. Thus, we conceptualize *IUIPC* as the degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used. The three IUIPC factors are described in detail as follows.

2.2.1. Collection. The very act of data collection, whether it is legal or illegal, is the starting point of various information privacy concerns. We define *collection*, the first dimension of IUIPC, as the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received. This collection factor is grounded on SC's principle of distributive justice, which relates to "the perceived fairness of outcomes that one receives" (Culnan and Bies 2003, p. 328). In an equitable exchange, consumers give up some information in return for something of value after evaluating the costs and benefits associated with the particular transaction. Thus, individuals will be reluctant to release their personal information if they expect negative outcomes (Cohen 1987).

In the domain of direct marketing, Phelps et al. (2000) found that a majority of respondents (85.6%) wanted to limit the amount of personal information collected by marketers. Cespedes and Smith (1993) argued that an idiosyncratic "privacy threshold" level existed for the amount of data people were willing to provide. Indeed, the collection factor constitutes one of the four CFIP dimensions[1] (Smith et al. 1996). Accordingly, it seems reasonable to expect that marketers' collection of personal information will continue to be an important source of privacy concerns among Internet users (Rendleman 2001). Thus, we posit collection, which is also a dimension of CFIP, as an important factor characterizing IUIPC.

2.2.2. Control. SC theory is strongly rooted in the principle of procedural justice (Gilliland 1993, Thibaut and Walker 1975, Tyler 1994). According to the principle of procedural justice, individuals view procedures as fair when they are vested with control of the procedures (Thibaut and Walker 1975, Tyler 1994). In other words, consumers want to exercise process control and influence changes in organizational policies they find to be objectionable (Gilliland 1993, Thibaut and Walker 1975). The issue of control becomes more pronounced when a large potential exists for opportunistic behavior and breach of the social contract in a relational exchange.

Control is especially important in the information privacy context because consumers take high risks in the submission of personal information. Based on the principles of procedural justice, moral contractors achieve control by exercising freedom to either accept or reject the process or decision outcome (Alge 2001). Thus, we propose that an individual's concerns for information privacy center on whether the individual has control over personal information as manifested by the existence of voice (i.e., approval, modification) or exit (i.e., opt-out) (Caudill and Murphy 2000).

Several studies have suggested that in reality people want to have the ability to control personal information. For example, Phelps et al. (2000) found that most people (84%) wanted to have more control over the use of personal data to restrict unwanted commercial advertisements. Nowak and Phelps (1995) also demonstrated that people were less worried about data collection when they explicitly give permission to firms or are given the choice to opt-out. The Internet technologies offer flexible ways for consumers to control their personal information in an organization's database. Consequently, lack of such control will increase online consumers' privacy concerns. Although less evident in CFIP, the control factor is thus likely to be one of the most important components reflecting IUIPC.

2.2.3. Awareness of Privacy Practices. On the basis of a review of the literature, Foxman and Kilcoyne (1993) argued that information privacy exists only when a person is (1) given control over personal information and (2) informed about data collection and other issues. Control is an active component of information privacy and it is often exercised through approval, modification, and opportunity to opt-in or opt-out. In contrast, awareness is a passive dimension of information privacy, and it refers to the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices (Culnan 1995, Foxman and Kilcoyne 1993). Accordingly, the awareness factor is highly interrelated with, but distinct from, its active counterpart (i.e., control) (Sheehan and Hoy 2000).

This awareness factor incorporates two types of justices—interactional and informational justice. Interactional justice includes issues of transparency and propriety of information made during the enactment of procedures. Violating interactional justice leads to decreased perceptions of fairness (Bies and Moag 1986, Greenberg 1990). Meanwhile, informational justice relates to the disclosure of specific information. Perceptions of fairness increased with the specificity of information used to provide justification (Shapiro et al. 1994).

According to Hoffman et al. (1999), a majority of Web users (69%) refused to reveal personal information to online firms because they were not sure how the data would be used. Similarly, Phelps et al. (2000) showed that about 50% of the respondents in their survey study were looking for more information

[1] Operationally, the collection scale measures the degree to which customers are concerned about data collection, but the other three factors pertain to the items that ask what organizations should do for fair privacy practices (for the CFIP scale, see the appendix). We believe that control and awareness effectively represent the other three CFIP dimensions. We test this proposition (i.e., comparison between CFIP and IUIPC).

Table 1 Comparison Between GIPC, CFIP, and IUIPC

	GIPC	CFIP	IUIPC
Purpose	To reflect the level of information privacy concerns in general	To reflect individuals' concerns about organizational information privacy practices	To reflect Internet users' concerns about information privacy
Focus	No particular focus	Organizations' responsibilities for the proper handling of customer information	Individuals' perceptions of fairness/justice in the context of information privacy
Context	Context-independent	Mostly offline or traditional direct marketing	Mostly online environment
Communication	Both one-way and two-way communication	Mostly one-way communication	Mostly two-way communication
Dimensions	One-dimensional construct	Collection, improper access, unauthorized secondary use, and error	Collection, control, awareness of privacy practices
Representation	A single latent factor	Correlated first-order factors; Stewart and Segars (2002) argued that CFIP is better represented as a second-order factor.	Second-order factor

and transparency about how organizations used individual-specific data. Indeed, these interactional/informational issues are captured through such CFIP factors as unauthorized secondary use, improper access, and errors. However, we believe that the awareness factor based on SC theory will succinctly convey these concerns about organizational practices. Thus, we posit awareness as the third and last factor characterizing IUIPC.

2.2.4. Second-Order IUIPC. Smith et al. (1996) operationalize CFIP as correlated first-order factors. From a theoretical perspective, however, their model excludes the possibility of a second-order factor that may govern the first-order factors. In this regard, Stewart and Segars (2002) argue that the four factors are not CFIP per se because "CFIP *leads to* various subconcerns" (p. 38, italics added). Within the framework of exchange theory, shared norms are similarly understood as a higher-order syndrome that regulates expectations of specific behaviors in an exchange relationship (Heide and John 1992). Using structural equation modeling, Stewart and Segars (2002) demonstrated that CFIP was indeed a second-order phenomenon that regulated the behavior of the four first-order factors.

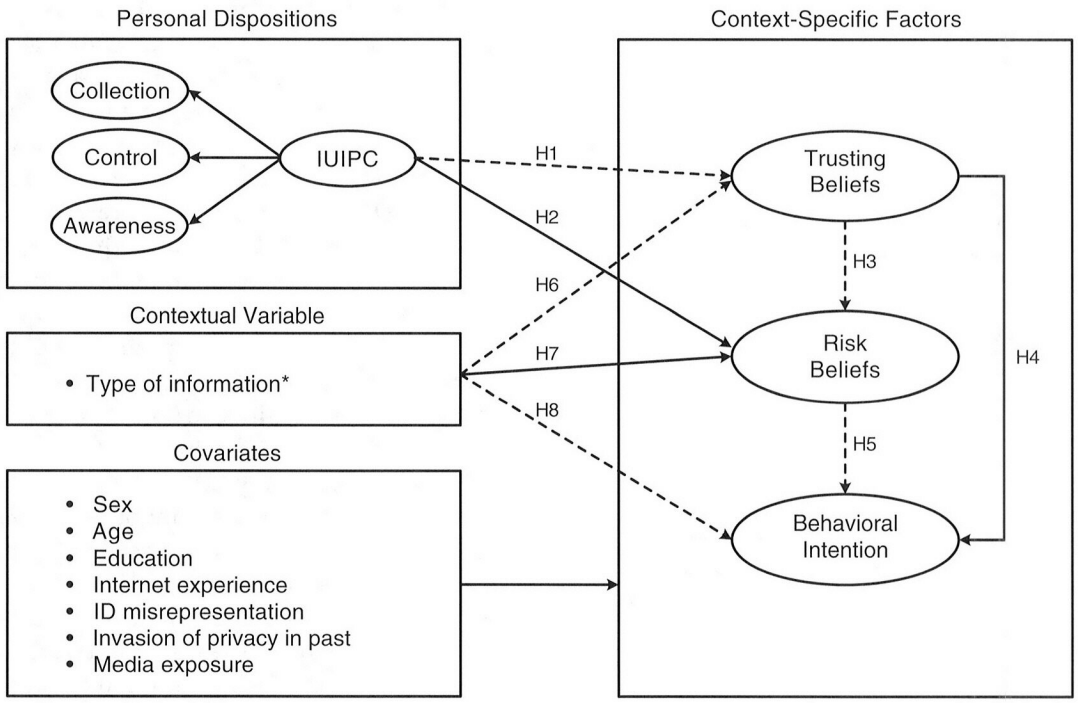
Given the strong theoretical and empirical evidence, we conceptualize IUIPC as a second-order factor. This conceptualization also avoids several problems in the interpretation of the role of IUIPC in a structural model. For example, a first-order model with multiple factors makes it difficult for researchers to clearly interpret the relationship between IUIPC and a research variable of interest. In addition, a high level of correlation between the first-order factors could cause a multicollinearity problem (Bagozzi and Heatherton 1994). However, the second-order model does not suffer from these problems; that is, it is theoretically sound, substantively meaningful, empirically justified, and operationally convenient. In summary, Table 1 describes the major differences between GIPC, CFIP, and IUIPC.

2.3. Causal Model

A long-term exchange relationship in the context of information privacy is initiated when a consumer releases personal information to a marketer. Thus, it is important for researchers to understand how one determines to engage in this long-term relationship. Moreover, marketers will have great interest in predicting consumer reactions to requests for personal information. Accordingly, we developed a causal model to describe how IUIPC influences a consumer's decision to release or not release personally identifiable data in a certain situation. Depicted in Figure 1, the causal model is developed based on the trust-risk framework (Mayer et al. 1995, McKnight et al. 1998, Jarvenpaa and Tractinsky 1999) and the theory of reasoned action (TRA) (Fishbein and Ajzen 1975). The research variables and their relationships in the model are explained in detail as follows.

2.3.1. Relationships Between IUIPC, Trusting Beliefs, Risk Beliefs, and Intention. In essence, the trust-risk model holds that in the situation in which

Figure 1 Proposed Model



Notes. *Less sensitive information (0), more sensitive information (1), positive effect ⟶, negative effect – – →.

potential *risks* are present, *trust* plays an important role in determining one's (trusting/risk taking) behavior (Luo 2002, Sirdeshmukh et al. 2002). This trust-risk model has been used to explain a variety of behaviors in an uncertain environment, including consumer-firm relationships (Wulf et al. 2001, Jarvenpaa and Tractinsky 1999) and employee-organization relationships (Mayer et al. 1995, McKnight et al. 1998). A great deal of the literature shows that trust and risk are the two most salient beliefs in information privacy-related contexts (Cespedes and Smith 1993, Milne and Rohm 2000, Miyazaki and Fernandez 2000, Sheehan and Hoy 2000). As shown in Figure 1, we include trusting beliefs and risk beliefs in the model to explain an individual's release of personal information at the request of an online marketer. Trusting beliefs are defined as the degree to which people believe a firm is dependable in protecting consumers' personal information (Grazioli and Jarvenpaa 2000, Gefen et al. 2003). On the other hand, risk beliefs refer to the expectation that a high potential for loss is associated with the release of personal information to the firm (Dowling and Staelin 1994).

A general consensus in the trust-risk literature shows that personal traits influence, to some extent, trusting beliefs and risk beliefs (Mayer et al. 1995, McKnight et al. 1998). This implies that one's tendency to worry over information privacy (i.e., IUIPC) will influence how the person perceives a specific situation in which an online marketer requests personal information (i.e., trusting and risk beliefs). More specifically, Internet users with a high degree of information privacy concerns are likely to be low on trusting beliefs and high on risk beliefs. This proposition is also consistent with TRA, which suggests that individual characteristics influence salient beliefs (Fishbein and Ajzen 1975, Ajzen 1991). Thus, as depicted in Figure 1, we propose that IUIPC will influence trusting beliefs negatively and risk beliefs positively.

Hypothesis 1. *Internet users' information privacy concerns will have a negative effect on trusting beliefs.*

Hypothesis 2. *Internet users' information privacy concerns will have a positive effect on risk beliefs.*

Evidence suggests that trusting beliefs also directly influence risk beliefs. For example, Moorman et al.

(1992) argued that trust would reduce "the perceived uncertainty and hence the perceived vulnerability" (p. 315). In other words, trusting beliefs are expected to mitigate risk perceptions. In the context of relationship marketing, Morgan and Hunt (1994) actually provided empirical support for the proposition mentioned above. Similarly, in a study of cross-cultural online retailing, Jarvenpaa and Tractinsky (1999) found that trust had a negative influence on risk perceptions. Taken as a whole, the more trust a consumer has in an online firm, the less likely he or she is to foresee the risk in providing personal information to the firm.

HYPOTHESIS 3. *Trusting beliefs will have a negative effect on risk beliefs.*

Within the framework of reasoned action, behavioral intention is a reliable predictor of actual behavior (Fishbein and Ajzen 1975, Ajzen 1991). It seems fair to argue then that intention to release personal information serves as a good proxy for whether one actually reveals personal information at the request of an online marketer. According to the trust-risk literature, trusting/risk beliefs are expected to exert a significant effect on behavioral intention. For example, McKnight et al. (1998) and McKnight and Chervany (2000) proposed that trusting beliefs would directly influence "trusting intention." Similarly, Jarvenpaa and Tractinsky (1999) showed that "risk perception" affected one's willingness to buy books from websites. Therefore, trusting/risk beliefs are likely to have a direct influence on intention. These hypotheses are depicted in Figure 1 and formally stated below.

HYPOTHESIS 4. *Trusting beliefs will have a positive effect on intention to reveal personal information.*

HYPOTHESIS 5. *Risk beliefs will have a negative effect on intention to reveal personal information.*

Note that the causal model implies that the impact of IUIPC on behavioral intention is fully mediated by trusting/risk beliefs. This is consistent with the premise of TRA that salient beliefs fully mediate the impact of individual differences on behavioral intention. Later, we will empirically examine whether this mediation proposition really holds in this particular context.

2.3.2. Contextual Variable. It is known that consumers' reactions to privacy threats depend on the type of information requested by marketers (Phelps et al. 2000, Sheehan and Hoy 2000, Wang and Petrison 1993). All things being equal, releasing more sensitive information is perceived as more risky than releasing less sensitive information (Milne and Gordon 1993). Although the perceived sensitivity of information varies widely with individual differences, in general financial data and medical information are known to be viewed by consumers as more sensitive information; in contrast, at an aggregate level, lifestyle characteristics and shopping/purchasing habits are considered less sensitive by consumers than financial data and medical information (Nowak and Phelps 1992, Sheehan and Hoy 2000, Phelps et al. 2000). The validity of a certain model cannot be established until it is shown to hold across a variety of personal data requested by marketers.

Despite the importance of this contextual difference resulting from various information requests, few studies have taken into account such difference explicitly within a causal model (Stewart and Segars 2002, Smith et al. 1996). To fill this gap in the literature, our model is specifically developed to control for the contingent effect of information on consumers' perceptions (Figure 1). In general, the causal model proposes that more sensitive information, compared with less sensitive information, will exert a more negative effect on consumers' attitudes and intentions toward revealing personal information. Specifically, we expect that a marketer's request for more sensitive information will make a consumer suspicious; consequently, this request will reduce the level of trust. Moreover, when sensitive information is requested, risk beliefs are hypothesized to increase. Finally, the model predicts that consumers will be more reluctant to reveal information that is more sensitive compared to information that is less sensitive. Thus, our final hypotheses are stated below.

HYPOTHESIS 6. *A marketer's request for more sensitive information will have a negative effect on trusting beliefs.*

HYPOTHESIS 7. *A marketer's request for more sensitive information will have a positive effect on risk beliefs.*

HYPOTHESIS 8. *A marketer's request for more sensitive information will have a negative effect on intention to reveal personal information.*

2.3.3. Covariates. Factors other than those mentioned previously may influence Internet users' reactions to information privacy threats. To control for those unknown effects, we have included several covariates in the model. Specifically, we included three demographic characteristics: sex (Milne and Rohm 2000), age (Culnan 1995, Milne and Rohm 2000, Wang and Petrison 1993), and education (Culnan 1995, Milne and Rohm 2000, Phelps et al. 2000, Wang and Petrison 1993). In addition, the causal model is tested with four additional variables related to personal experiences: Internet experience (Milne and Rohm 2000, Phelps et al. 2000), how often subjects provide falsified identification information to a marketer (Hoffman et al. 1999, Pew Internet Project 2000), whether the subject's privacy has been invaded in the past (Culnan 2000), and the amount of exposure to media reports of incidents of privacy invasion (Smith et al. 1996). Consequently, as Figure 1 shows, a total of seven control variables are taken into account in the causal model.

3. Methodology

We conducted two empirical studies to develop and test a new scale of IUIPC. The purpose of Study 1 was to develop measures for new dimensions of privacy concerns (e.g., control and awareness) that were not available from existing scales (e.g., collection, unauthorized secondary use, improper access, and errors). Study 2 was designed to establish the second-order IUIPC factor with the combination of new (i.e., control and awareness) and existing (i.e., collection) scales. In this latter study, we also formally tested the research model and hypotheses.

3.1. Empirical Study 1

The objective of Study 1 is to develop new scales for privacy concerns that were not part of the existing CFIP dimensions (i.e., collection, unauthorized secondary use, improper access, and errors). To identify various forms of salient privacy concerns, we first reviewed the relevant literature in different disciplines including law, public policy, marketing, communications, and information systems (Caudill and Murphy 2000, Culnan 2000, Goodwin 1991, Newman and Rao 2000, Regan 1995, Smith et al. 1996, Stewart and Segars 2002). This literature review was followed by qualitative research in an effort to further elicit privacy concerns that might have been missed in the previous step (Straub et al. 2004). This qualitative research was conducted through personal interviews with three subject matter experts and a group interview with eight Internet users in a nonstructured and natural manner (Malhotra 2004). As a result, a pool of new items was created to reflect Internet users' information privacy concerns. This first pool included 7 awareness items, 15 control items, and 21 other items that could potentially constitute online consumers' privacy concerns (e.g., security, honesty, the seal of assurance, social responsibility, etc). To reduce the length of the questionnaire, the existing scales were excluded from this item pool.

A structured questionnaire was developed based on the pool of new items. The survey was administered to household (nonstudent) respondents who had used the Internet for at least one hour in the previous month. Students in a marketing research class at a large southeastern university in the United States were given the task of collecting the survey data. Partial course credit was granted to each student for administering the survey, and strict instructions were laid out with regards to the quality of data collection. In this field survey, we collected a total of 293 completed questionnaires. Men (49%) and women (51%) were almost equally represented, and an average respondent was 35 years of age and had 4.5 years of Internet experience. The median household income per year was $60,000, and 71% of the respondents had bachelor's degrees or higher.

To discover discernible patterns of privacy dimensions, we performed exploratory factor analysis (EFA). From the results we found that control and awareness clearly emerged as independent factors. We chose three items for control and three items for awareness that exhibited the most desirable psychometric properties (Hair et al. 1995). Each of these selected items loaded higher than 0.70 on the designated factor and at the same time loaded less than 0.40 on other factors (Chin et al. 1997). Consequently, these six items, along with the existing four items for the collection factor adapted from CFIP, represented the 10-item IUIPC scale in the following study.

3.2. Empirical Study 2

To control for the effect that the type of information had on consumers' reactions, we employed an experimental design with a scenario-creation method (Webster and Trevino 1995, Straub and Karahanna 1998). Specifically, two types of scenarios were created according to the sensitivity of the personal information requested (for the categorization of personal information requested, see Phelps et al. 2000). The Type A questionnaire presented a scenario in which respondents were asked to provide personal shopping preferences in return for free membership, worth $50, at a discount store (less sensitive information). Type B presented the same scenario but the information requested concerned personal financial information (more sensitive information). In general, financial information is perceived to be more sensitive than personal preferences (Sheehan and Hoy 2000). Therefore, Type B should be viewed as a more sensitive situation than Type A. A pretest was conducted that confirmed the nature of the two scenarios.[2] We employed a between-subjects design in which respondents were given only one of the two scenarios (Keppel 1991).

Both scenarios had a common set of items that was independent of the type of information requested. Among the items were demographic information, general consumer behavior, and the three information privacy scales (GIPC, CFIP, and IUIPC). Scales specific to the scenarios were trusting beliefs, risk beliefs, and intention. Note that the operationalization of these context-contingent factors was directed toward online marketers in general as opposed to a specific firm. This was done because respondents could not be expected to have a meaningful experience with the hypothetical firm in the scenario. McKnight et al. (1998) proposed that initial trust would depend on "institutional cues that enable one person to trust another without firsthand knowledge" (p. 474). That is, at the initial stage, a consumer's opinions about an unknown firm will be similar to his or her opinions about typical firms. The appendix shows the specific items used in this study.

[2] Note that in this discount store example requesting financial information, as opposed to personal preferences, will be thought to be largely inappropriate. This also made Type B more sensitive than Type A.

To collect data, we conducted personal interviews similar to those of the first study. For this second study, interviewers were recruited from a different marketing research class to collect a fresh set of data. Using the personal contact information, we ensured that the respondents in the previous study were not included in the second study. As a result, we collected a total of 449 usable questionnaires from household respondents in one-on-one, face-to-face interviews. The sample consisted of 217 Type A and 232 Type B respondents. The demographic profile of the respondents was comparable to that of the first study (54% male, 53% 35 years of age or older, a median of 4.5 years of Internet experience, a median income of $60,000, and 76% bachelor's degrees or higher). No significant differences were found between the two types of data (A and B) in terms of gender, age, Internet experience, income, and education.

3.3. Measurement Model

The psychometrics literature suggests that to avoid misinterpretation of structural relationships, researchers should first estimate a measurement model before testing hypotheses (Anderson and Gerbing 1988). We adopted this two-step approach in which first a valid and reliable measurement was established, and subsequently the structural model of Figure 1 was tested. To examine the original measurement model, we conducted a confirmatory factor analysis (CFA) on the data collected from Study 2. In particular, model fit is assessed in terms of four indices: comparative fit index (CFI), goodness-of-fit index (GFI), root mean square error of approximation (RMSEA), and the consistent Akaike information criterion (CAIC). A model is considered to be satisfactory if CFI > 0.95, GFI > 0.90, and RMSEA < 0.06 (Bearden et al. 1993, Hu and Bentler 1999). CAIC, which is useful for comparing nonnested alternative models, has no cut-off values; instead, a smaller value implies better fit (Bozdogan 1987, Steenkamp and Baumgartner 1998).

The result of CFA indicated that the initial measurement model did not fit the data well [$\chi^2(734) = 1{,}753.61$, CFI $= 0.91$, GFI $= 0.84$, RMSEA $= 0.056$, CAIC $= 2{,}656.20$]. A careful inspection of the LISREL output revealed that some items did not load on the designated latent factors (completely standardized loading < 0.60), or were associated with

Table 2 Estimated Factor Correlation Matrix from the Revised Measurement Model

					Correlation matrix									
	Mean	SD	CR	AVE	1	2	3	4	5	6	7	8	9	10
1. COLL	5.63	1.09	0.83	0.55	0.74									
2. ERRO	5.16	1.18	0.88	0.64	0.52	0.80								
3. SECO	6.20	1.00	0.82	0.54	0.61	0.50	0.73							
4. IMPR	6.06	0.95	0.77	0.53	0.68	0.68	0.81	0.73						
5. AWAR	6.21	0.87	0.74	0.50	0.66	0.49	0.77	0.79	0.71					
6. CONT	5.67	1.06	0.78	0.54	0.53	0.47	0.56	0.68	0.75	0.73				
7. GIPC	5.01	1.29	0.75	0.50	0.70	0.48	0.53	0.62	0.70	0.55	0.71			
8. TRUST	3.24	1.33	0.78	0.54	−0.41	−0.08	−0.22	−0.24	−0.31	−0.25	−0.29	0.73		
9. RISK	4.56	1.59	0.92	0.74	0.38	0.32	0.32	0.36	0.26	0.25	0.40	−0.32	0.86	
10. INT	3.15	1.74	0.95	0.86	−0.34	−0.17	−0.23	−0.21	−0.22	−0.17	−0.31	−0.46	−0.78	0.93

Notes. COLL = collection; ERRO = errors; SECO = unauthorized secondary use; IMPR = improper access; AWAR = awareness; CONT = control; GIPC = global information privacy concern; TRUST = trusting beliefs; RISK = risk beliefs; INT = intention to give personal information; SD = standard deviations; CR = composite reliability; AVE = average variance extracted. Value on the diagonal is the square root of AVE.

high modification indices. To refine the measurement model, seven items were dropped from GIPC, trusting beliefs, risk beliefs, and intention (see the appendix). In spite of the measurement purification, we made no changes on CFIP and IUIPC factors to compare them impartially. With the remaining items, we again performed a CFA. Compared with the previous model, this new measurement model exhibited improved model fit [$\chi^2(482) = 1{,}049.40$, CFI = 0.94, GFI = 0.87, RMSEA = 0.051, CAIC = 1,852.495]. Table 2 describes the means, standard deviations, composite reliabilities (CR), and average variance extracted (AVE), and correlations of the factors based on the refined measurement model.

In addition to the model fit, we examined the reliability, the convergent validity, and the discriminant validity of the scale. Reliability was examined based on CR and AVE. A scale is said to be reliable if CR > 0.70 and AVE > 0.50 (Bagozzi and Yi 1988). As shown in Table 2, the CRs range from 0.74 to 0.95, and the AVEs range from 0.50 to 0.86, which are above recommended cut-off values. On the other hand, convergent validity is established if all item loadings are equal to or above the recommended cut-off level of 0.60 (Chin et al. 1997). We found the lowest loading of 0.61 in an item for awareness and the highest loading of 0.98 in an item for intention, suggesting the convergent validity of the scale. Discriminant validity is the extent to which an item does not relate to the measures of other constructs. Discriminant validity is achieved if the square root of the AVE is larger than correlation coefficients (Fornell and Larcker 1981, Chin 1998). We found that all of the correlation estimates met the criterion except in four cases. Two of the four exceptions were found across IUIPC and CFIP. This fact seems to pose less concern because IUIPC is assumed to include and extend CFIP. In other words, by definition, the two constructs are destined to be strongly correlated in many occasions. Meanwhile, the other two violations were identified within CFIP and IUIPC, respectively. However, because of the size of the correlation matrix, which includes 45 estimates, some violations can occur simply through chance (Campbell and Fiske 1959). Therefore, it can be argued that in this study at least a reasonable extent of discriminant validity was established.[3] Overall, the evidence of good model fit, reliability, convergent validity, and discriminant validity indicates that the measurement model was appropriate for testing the structural model at a subsequent stage.

[3] Alternatively, discriminant validity can be checked by examining whether a correlation between two constructs is significantly different from unity (Venkatraman 1989). More specifically, the correlation of the two constructs in question was freely estimated in the first model (i.e., a two-factor model) but set to 1 in the second model (i.e., a one-factor model). A chi-square difference was examined between the two models to determine whether the two constructs were significantly different. An examination of each pair of the constructs of Table 2 (45 pairs) revealed that the extra constraint consistently worsened model fit, supporting the discriminant validity of the constructs. That is, the results of chi-square difference tests provided further support that the constructs were reasonably different from one another.

3.4. The Second-Order IUIPC Scale

We tested a second-order IUIPC with three first-order dimensions (i.e., collection, control, and awareness) as specified in Figure 1. To provide a comparative perspective on the assessment of IUIPC, we also examined an alternative form of information privacy concerns, namely, a second-order CFIP (Stewart and Segars 2002). As shown in the appendix, the original CFIP scale was adapted to a new online context. Given the modification to the CFIP scale that we made (e.g., from "companies" to "online companies"), the results of CFIP in this present study should be interpreted with caution.

IUIPC met the fit criteria in terms of CFI, GFI, and RMSEA [$\chi^2(32) = 73.19$, CFI = 0.98, GFI = 0.97, RMSEA = 0.054, CAIC = 236.65], but the fit of CFIP was marginal in terms of RMSEA [$\chi^2(86) = 264.56$, CFI = 0.95, GFI = 0.93, RMSEA = 0.068, CAIC = 506.20]. The CAIC index also indicates that IUIPC (CAIC = 236.65) represents the reality better than CFIP (CAIC = 506.20), at least in this particular context. In general, the results indicated that IUIPC efficiently and effectively reflected Internet users' concerns for information privacy.

In addition to model fit, we examined concurrent validity, which refers to the degree to which a new scale of interest relates to an established measure representing the same or similar phenomenon (Cronbach 1990, Rogers 1995). For this particular test, a modified GIPC scale, which included the word "online" in two of its three items, was treated as the standard measure reflecting privacy concerns (Smith et al. 1996); thus, we examined the correlation between GIPC and the scale in question (i.e., IUIPC or CFIP) as an indicator for the degree of the concurrent validity of the scale.[4] The results showed that IUIPC had a stronger correlation to GIPC ($r = 0.59$) than did CFIP ($r = 0.53$). Using the Meng et al. (1992) Z-test method, we tested whether the correlation coefficients were significantly different. The test value (Z-value = 2.15) indicated that a significant difference existed between the correlation coefficients ($p < 0.05$), suggesting that IUIPC more strongly correlated with GIPC than did CFIP.

We further assessed the utility of IUIPC using different criteria. Understanding an individual's privacy concerns has significance to practitioners to the extent that it helps to predict various privacy-related behaviors. Thus, in this additional test, the utility of a scale is assessed by the correlation between a scale and a behavioral intention item toward a privacy-related behavior. We modified five behavioral intention items included in the study by Smith et al. (1996); specifically, the word "company" in the original items was replaced with "online company." The five items are: (1) How likely are you to refuse to give information to an online company because you think it is too personal?, (2) How likely are you to take actions to have your name removed from e-mail lists for catalogs, products, or services?, (3) How likely are you to write or call an online company to complain about the way it uses personal information?, (4) How likely are you to write or call an elected official or consumer organization to complain about the way online companies use personal information?, and (5) How likely are you to refuse to purchase a product because you disagree with the way an online company uses personal information?

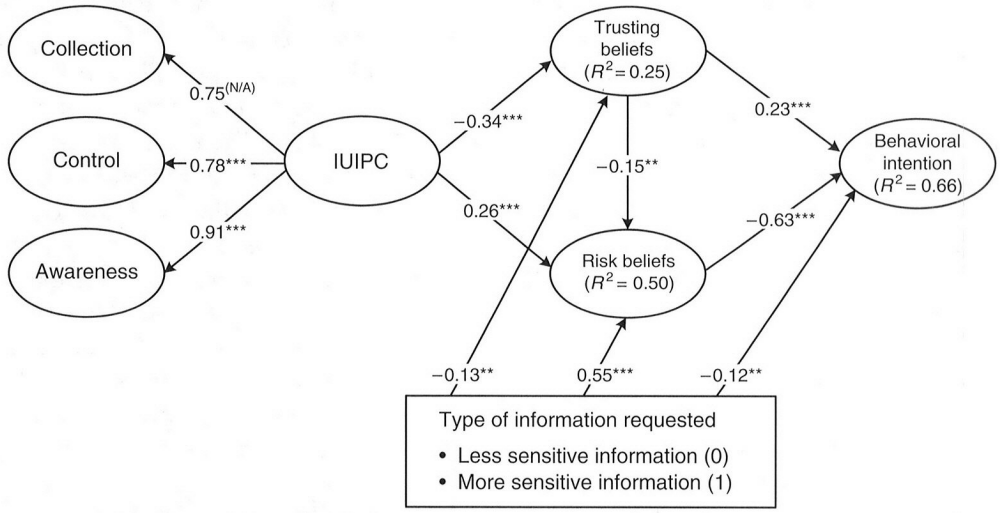
The correlations between CFIP and the five items were found to be 0.36, 0.16, 0.26, 0.20, and 0.33, respectively. On the other hand, IUIPC's correlations with the items were 0.43, 0.25, 0.24, 0.20, and 0.42. The result indicated that IUIPC correlated more strongly on three of the five items than did CFIP. Moreover, the results of Z-tests showed that these differences in the correlations were statistically significant (Z-values > 2.22, *ps* < 0.05, two-tailed), suggesting that IUIPC is likely to exceed CFIP as a predictor of consumer reactions to *online* privacy threats. Overall, the second-order IUIPC seems a reasonable representation of Internet users' information privacy concerns.

3.5. Nomological Validity

Nomological validity is defined as "the degree to which predictions from a formal theoretical network containing the concept under scrutiny are confirmed" (Bearden et al. 1993, p. 5). The establishment of nomological validity is said to be an important step in

[4] The correlation between CFIP and IUIPC should be known to compare their relationships with the criterion variable, i.e., GIPC (Meng et al. 1992). To calculate the correlation between CFIP and IUIPC, we used the "means of latent variable scores" (MLVS) technique available in PRELIS 2.3 and LISREL 8.3 (Jöreskog et al. 1999). This technique allowed us to create factor scores for CFIP, IUIPC, and GIPC, respectively. The factor scores were used to estimate the relationships between the three factors.

Figure 2 Results of SEM Analysis



Notes. Completely standardized estimates, controlled for seven variables in the proposed model (Figure 1), model fit [$x^2(290) = 574.75$; CFI = 0.95; CFI = 0.92; RMSEA = 0.047; CAIC = 1,399.16], $^*p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$ (two-tailed).

the scale development process (Straub et al. 2004, Campbell 1960). As discussed earlier, the trust-risk literature shows that personal disposition has significant relationships with both trusting beliefs and risk beliefs (Mayer et al. 1995, McKnight et al. 1998). Because the second-order IUIPC is conceptualized as personal disposition in this paper, its relationship with the beliefs constructs will indicate the nomological validity of IUIPC.

To assess the nomological validity of IUIPC, we specifically examined the relationship between the second-order IUIPC, trusting beliefs, and risk beliefs. The results of CFA showed that the fit of the model was acceptable: $\chi^2(114) = 290.36$, CFI = 0.95, GFI = 0.93, RMSEA = 0.059, CAIC = 567.53. We also found that IUIPC strongly correlated with trusting beliefs ($r = -0.43$, $p < 0.001$) and risk beliefs ($r = 0.38$, $p < 0.001$). Recently, Pavlou and Gefen (2004) examined the relationships between trust propensity, trust, and perceived risk to study potential buyers' bidding behaviors in online auction. Their study reported that the correlation between trust propensity and trust in sellers was 0.56 and that between trust propensity and perceived risk from sellers was −0.25. Considering that IUIPC resembles *distrust* propensity, the signs and magnitudes of the correlations between the two studies are quite comparable. Overall, our findings indicate that IUIPC related to other variables in a way that is highly consistent with theory and past findings, thus providing empirical evidence of the nomological validity of the proposed scale (Straub et al. 2004).

3.6. Structural Model and Research Hypotheses

We tested the causal model using the structural equation modeling (SEM) technique.[5] Figure 2 reports the results of SEM analysis. Fit indices indicate that the model is a realistic representation of the data [$\chi^2(290) = 574.75$, CFI = 0.95, GFI = 0.92, RMSEA = 0.047, CAIC = 1,399.16]. Furthermore, the model explained a fair amount of the variance in the outcome variables; for example, it explained 66% of the variance in intention to give personal information.

We found that all of the hypotheses proposed in the causal model were supported. Specifically, as hypothesized, IUIPC had a negative effect on trusting beliefs ($\beta = -0.34$, $p < 0.001$, two-tailed, Hypothesis 1 supported) and a positive effect on risk beliefs ($\beta = 0.26$, $p < 0.001$, Hypothesis 2 supported). In addition, trusting beliefs had a negative impact on risk beliefs

[5] We also estimated the fit of the structural equation model with the second-order CFIP. The model fit was slightly worse than that of the second-order IUIPC: $\chi^2(434) = 890.18$, CFI = 0.94, GFI = 0.89, RMSEA = 0.048, CAIC = 1,792.771. The model with CFIP also explained 21% of the variance in trusting beliefs, 50% in risk beliefs, and 66% in behavioral intention.

($\beta = -0.15$, $p < 0.01$, Hypothesis 3 supported). We also found that intention was influenced positively by trusting beliefs ($\beta = 0.23$, $p < 0.001$, Hypothesis 4 supported) and negatively by risk beliefs ($\beta = -0.63, p < 0.001$, Hypothesis 5 supported). On the other hand, the results showed that the type of information requested significantly influenced consumers' perceptions and intentions. In particular, more sensitive information significantly decreased trusting beliefs ($\beta = -0.13$, $p < 0.01$, Hypothesis 6 supported), increased risk beliefs ($\beta = 0.55$, $p < 0.001$, Hypothesis 7 supported), and decreased intention ($\beta = -0.12$, $p < 0.01$, Hypothesis 8 supported).

Although the causal model seems to succinctly represent consumer evaluation and behavior, we found that the effects of control variables on the context-contingent factors, i.e., trusting belief, risk beliefs, and intention, were not negligible—suggesting an area for potential improvement in the model. Specifically, 5 of 21 relationships (7 covariates $*$ 3 context-contingent variables) were significant: Age was negatively related with intention ($p < 0.05$, two-tailed), education was negatively related with trusting beliefs ($p < 0.01$), Internet experience reduced risk beliefs ($p < 0.001$), the experience of identification falsification was negatively correlated with intention, and media exposure reduced trusting beliefs ($p < 0.01$). In contrast, no effects of gender and experience as victims were found on the context-contingent factors.

Finally, we checked if the effect of IUIPC on intention was fully mediated by trusting and risk beliefs. As a way of testing the mediation effect, the direct path from IUIPC to intention was added and allowed to be free. The result indicated that in spite of the added path, the decrease in chi-square value was insignificant [$\Delta\chi^2(1) = 2.88$, ns]. Indeed, the IUIPC-intention path was found to be insignificant, thus supporting the full mediation hypothesis.

4. Discussion and Conclusions

The objective of this study was three-fold: (1) to describe the nature of IUIPC based on SC theory, (2) to develop a reliable and valid scale for IUIPC, and (3) to develop and test a causal model centering on IUIPC. First, this paper presents how useful the notion of justice/fairness is in clarifying the dimensionality of IUIPC, which consists of collection, control, and awareness. Second, we found from the results of this study that the second-order IUIPC factor exhibited desirable psychometric properties in the context of online privacy. Finally, the results demonstrated that the structural model including IUIPC fit the data satisfactorily and explained a large amount of variance in behavioral intention. Overall, our findings suggest that the theory-driven construct of IUIPC will serve as a useful tool for analyzing online consumers' privacy concerns and reactions to various privacy threats on the Internet. This section begins with a discussion on the theoretical and managerial implications of the findings of this study. We conclude this article by describing the limitations of this study and suggesting directions for further research.

4.1. Theoretical Contributions

4.1.1. IUIPC. SC theory is attracting considerable attention in many academic areas including relationship marketing, marketing ethics, and information privacy (e.g., Morgan and Hunt 1994, Dunfee et al. 1999, Milne and Gordon 1993). Drawing on SC theory, this article offers a theoretical framework to explain the dimensions of Internet users' concerns for information privacy. Specifically, we discussed notions of (1) distributive, (2) procedural, and (3) interactional/informational justice and tied them with the dimensions of online privacy concerns—"whether the exchange of personal information is equitable" (collection), "whether I have control over the data" (control), and "whether I am adequately informed about the use of the data" (awareness). As shown previously, IUIPC, compared to CFIP, had a better model fit and a significantly stronger correlation with criterion variables. These findings suggest that at least in the online privacy context, the coverage of IUIPC includes and extends that of CFIP. Thus, our theory-driven approach to privacy concerns seems to nicely complement the traditional practice-oriented approach. It is true that consumers' opinions about such organizational practices as secondary use, improper access, and errors (i.e., CFIP) can reasonably reflect their online privacy concerns. Yet, our findings indicate that consumers' concerns caused by those unfair organizational practices can be *succinctly* summarized into the SC-based IUIPC concept. Therefore, while inevitably correlated with CFIP, IUIPC is

considered as an efficient and effective representation of *online consumers' concerns for information privacy.*

IUIPC is originally developed to reflect recent changes in an individual's views on fairness/justice because of the widespread use of the Internet. Nevertheless, it is important to note that this scale is strongly rooted in a *general* conceptual framework drawing on SC theory. Therefore, under an assumption that the essence of privacy concerns lies in fairness perceptions, our justice-oriented scale is likely to be generalizable across a variety of other privacy contexts. For instance, as with the Internet environment, the direct marketing environment can be conceived as a case of social contract. Therefore, with appropriate rewording (e.g., deleting the word "online" in the items), the IUIPC scale is expected to reasonably apply to traditional direct marketing and other privacy contexts. Meanwhile, new privacy-threatening technologies such as cookies, Web bugs, and spyware are continuously being developed. Thus, a scale specific to particular technologies does not seem to be suitable for measuring consumers' privacy concerns in this fast-changing online environment. In contrast, as mentioned earlier, IUIPC centers on the perceptions of fairness; therefore, the scale is flexible enough to be adapted to minor technical changes that may occur in the future. We also can expect that the justice-oriented scale will be relatively robust against technological innovations. In sum, as compared with other specific, practice-oriented scales, our general, theory-based scale has the potential to be applicable to a variety of privacy-related contexts.

4.1.2. Causal Model. The present study regards IUIPC as personal disposition and the literature concurs with the view that this type of individual tendency has little impact on actual behavior (Mayer et al. 1995, Fishbein and Ajzen 1975, Ajzen 1991). As expected, this was the case in this particular study. Specifically, from the results of the causal model, we found that the correlation between the second-order IUIPC and behavioral intention was -0.32.[6] Given the moderate level of correlation, IUIPC alone will not be able to explain more than 10% of the variance in behavioral intention (Fornell and Larcker 1981). Furthermore, when trusting beliefs and risk beliefs were controlled for, no direct effect of IUIPC was found on behavioral intention. This finding implies that trusting beliefs and risk beliefs mediated the impact of IUIPC on behavioral intention.

While focusing on consumers' privacy concerns in general, privacy research in the IS domain has paid little attention to consumers' perceptions specific to a particular context (Smith et al. 1996, Stewart and Segars 2002). However, our findings clearly reveal that to have a complete understanding of consumer reactions to information privacy-related issues, researchers should examine not only consumers' privacy concerns at a general level, but also consider salient beliefs and contextual differences at a specific level. Overall, this study indicates that consumer behavior in the context of information privacy is a complex phenomenon; thus, researchers should be ready to employ sophisticated techniques to examine consumers' reactions to information privacy threats.

Finally, recall that IUIPC draws on SC theory, which sheds light on the nature of long-term relationships between stakeholders. Meanwhile, this study demonstrated that the trust-risk framework, which also deals with the issues related to long-term relationships, could be seamlessly integrated with the SC-based IUIPC concept. Furthermore, we demonstrated that intention models such as TRA were also helpful in understanding relational exchange especially within the context of information privacy. Consequently, one of the major contributions of this study is to develop the causal model integrating SC theory, the trust-risk framework, and TRA. We believe that the causal model will serve as a useful conceptual tool for further research on the relational exchange of personal information between consumers and marketers.

4.2. Managerial Implications

4.2.1. IUIPC. Our findings imply that the 10-item IUIPC scale, along with the 15-item CFIP scale, will be a worthy candidate for consideration as an indicator of online consumers' privacy concerns. From a managerial perspective, the lower number of items included in the IUIPC scale is desirable as a means of reducing the data-collection demands imposed on respondents, the length and duration of the questionnaire, and the cost of data collection. Nonetheless, it should also be noted that the validity of IUIPC has

[6] We do not report the statistical details because of space limitations.

yet to be established in contexts other than the Internet. Thus, practitioners will continue to have the need to rely on CFIP for many applications.

One of the major findings of this study is that online consumers consider it most important to (1) be aware of and (2) have direct control over personal information stored in marketers' databases. Therefore, at the very least, managers should make sure that their consumers can easily check what type of information is collected, whether the information is correct, and how this information is used in and outside the organization. In addition, as mentioned earlier, consumers should be allowed to control, i.e., add, delete, and modify at will, the information in the organization's database. This research suggests that these organizational efforts can jointly soothe an individual's information privacy concerns (Stewart and Segars 2002).

4.2.2. Causal Model. Consumers' privacy concerns are certainly a driving force of their reactions to a certain organizational practice. Yet, our findings suggest that trust in a marketer can significantly mitigate perceived risk and ultimately a customer's reluctance in releasing personal information. Thus, it is important for managers to understand how to boost customers' trust in their firms' handling of personal information. Drawing on Zucker's (1986) trust production mechanisms, Luo (2002) proposed several techniques such as third-party seal programs that are believed to facilitate the relational exchange of personal information between consumers and marketers. These techniques will be instrumental for practitioners to collect more valuable information without necessarily invading consumer privacy.

Unlike European countries with general and strict privacy laws, the United States has industry-specific regulatory rules (Culnan 2000). Thus, consumers' reactions to information privacy threats will vary with respect to the type of industry sector. Consequently, it is important for practitioners to understand not only privacy concerns in general (i.e., IUIPC), but also an individual's perceptions specific to the sector (i.e., trust and risk beliefs). The causal model proposed in this study incorporates both types of concepts to facilitate the in-depth investigation of consumers' reactions to an industry-specific practice. We hope the proposed model will be helpful in providing further insight into the problems as they manifest in various ways within industry (e.g., financial, medical, etc.) sectors.

4.3. Limitations and Further Research

Some limitations of this study should be mentioned. First, we modified the wordings of the original CFIP scale to suit the purpose of this present study—the examination of *online* privacy concerns. We found that the revised CFIP scale was reliable and valid, but it did not perform as well as IUIPC in this particular context. Nevertheless, the efficacy of IUICP over CFIP in the context of online privacy should be considered as tentative until the effect of the scale modification is fully understood. Our main objective in comparing IUIPC and CFIP was to provide additional evidence on the efficacy of IUIPC, as it is a new scale. Second, we continue to contend that consumers' reactions to a specific privacy threat are highly dependent on contextual factors. Thus, it remains to be seen whether or not the results of this study retain their validity with different contextual variables, e.g., type of information requested, reward offered by marketers (Phelps et al. 2000, Sheehan and Hoy 2000). Third, our study did not examine the impact of IUIPC on actual behavior. Although behavioral intention is known as a reliable predictor of actual behavior (Ajzen 1991), the theoretical framework presented in this paper should be reexamined with an additional measure of actual behavior using a longitudinal design. Last, the selection of the respondents was left to the interviewers and data collected for this study was specific to a given geographic location (i.e., the southeastern United States). Although this type of convenience sampling is more the norm than the exception in the IS domain (e.g., Smith et al. 1996, Stewart and Segars 2002), care must be taken in any effort to generalize our findings beyond the boundary of our sample.

Opportunities for further research are abundant. First, the borderless nature of the new economy is making the issue of online privacy more complicated than ever before (Milberg et al. 1995). To design information practices that fit a particular local market, global companies should first understand how consumers in the local area of interest define fairness in the context of information privacy. We believe that the theoretical framework presented in this study will provide a solid basis for examining cross-cultural

variations in consumer behavior. Second, this study considers two types of beliefs as most salient in the context of information privacy—namely, trusting beliefs and risk beliefs. Yet, it is possible that other forms of beliefs also play an important role in consumer behavior. For example, individuals are likely to perceive a lack of justice when they are not satisfied with a marketer's actual information practice. Because IUIPC is conceptualized/operationalized at a general level, perceived lack of justice, which is highly specific to a particular practice by the marketer, was not captured precisely in this study (Culnan and Bies 2003). Thus, further research should examine not only privacy concerns at a general level, but also perceived problems within a particular context at a specific level.

In summary, information privacy has been frequently identified as a major problem holding back consumer confidence in online business transactions. To address this problem, we should first understand the very nature of online consumers' privacy concerns. This article introduced a 10-item scale of IUIPC, which was shown to reasonably represent the dimensionality of privacy concerns, categorized as collection, control, and awareness. Using this scale, we were also able to demonstrate how consumers' privacy concerns negatively influenced their willingness to carry on relationships with online companies. We hope that many researchers will employ the theoretical framework and the new scale for further investigation of this important area.

Acknowledgments

The authors are indebted to Senior Editor Robert Zmud and Associate Editor Detmar Straub for their valuable help and guidance throughout the review process. Helpful and constructive comments provided by the three anonymous *Information Systems Research* reviewers are deeply appreciated. The authors are grateful to Jan Heide at the University of Wisconsin and Robert Peterson at the University of Texas for their valuable comments on earlier versions of this paper. The authors would also like to thank Seoyoung Kim for her help with literature review and J. Stanford Fisher for his editorial help.

Appendix. Research Constructs and Measures

Control: Seven-point scales anchored with "strongly disagree" and "strongly agree" (newly developed).

(1) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

(2) Consumer control of personal information lies at the heart of consumer privacy.

(3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

Awareness (of Privacy Practices): Seven-point scales anchored with "strongly disagree" and "strongly agree" (newly developed).

(1) Companies seeking information online should disclose the way the data are collected, processed, and used.

(2) A good consumer online privacy policy should have a clear and conspicuous disclosure.

(3) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

Collection: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Smith et al. 1996). Adapted to an Internet environment (e.g., companies ⇒ online companies).

(1) It usually bothers me when online companies ask me for personal information.

(2) When online companies ask me for personal information, I sometimes think twice before providing it.

(3) It bothers me to give personal information to so many online companies.

(4) I'm concerned that online companies are collecting too much personal information about me.

Errors: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Smith et al. 1996). Adapted to an Internet environment (e.g., companies ⇒ online companies).

(1) All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.

(2) Online companies should take more steps to make sure that the personal information in their files is accurate.

(3) Online companies should have better procedures to correct errors in personal information.

(4) Online companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

Unauthorized Secondary Use: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Smith et al. 1996). Adapted to an Internet environment (e.g., companies ⇒ online companies).

(1) Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided information.

(2) When people give personal information to an online company for some reason, the online company should never use the information for any other reason.

(3) Online companies should never sell the personal information in their computer databases to other companies.

(4) Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

Improper Access: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Smith et al. 1996). Adapted to an Internet environment (e.g., companies ⇒ online companies).

(1) Online companies should devote more time and effort to preventing unauthorized access to personal information.

(2) Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.

(3) Online companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Global Information Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Smith et al. 1996, some items newly developed).

(1) All things considered, the Internet would cause serious privacy problems.*

(2) Compared to others, I am more sensitive about the way online companies handle my personal information.

(3) To me, it is the most important thing to keep my privacy intact from online companies.

(4) I believe other people are too much concerned with online privacy issues.*

(5) Compared with other subjects on my mind, personal privacy is very important.*

(6) I am concerned about threats to my personal privacy today.

Scenario Type A (Less Sensitive Information)
You are visiting a website of a discount club. The club offers discounts on consumer products (e.g., electronics, CDs, books) to its members. Generally, an annual membership fee is $50. To obtain free membership, you are required to fill out your *personal purchase preference information* (e.g., favorite product category, brand, design).

Scenario Type B (More Sensitive Information)
You are visiting a website of a discount club. The club offers discounts on consumer products (e.g., electronics, CDs, books) to its members. Generally, an annual membership fee is $50. To obtain free membership, you are required to fill out your *personal financial information* (e.g., annual income, current debt, annual mortgage payment, checking and saving balances, any other investments).

Trusting Beliefs: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Jarvenpaa and Tractinsky 1999, some items newly developed).

(1) Online companies would be trustworthy in handling (the information).*

(2) Online companies would tell the truth and fulfill promises related to (the information) provided by me.*

(3) I trust that online companies would keep my best interests in mind when dealing with (the information).

(4) Online companies are in general predictable and consistent regarding the usage of (the information).

(5) Online companies are always honest with customers when it comes to using (the information) that I would provide.

Risk Beliefs: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Jarvenpaa and Tractinsky 1999, some items newly developed).

(1) In general, it would be risky to give (the information) to online companies.

(2) There would be high potential for loss associated with giving (the information) to online firms.

(3) There would be too much uncertainty associated with giving (the information) to online firms.

(4) Providing online firms with (the information) would involve many unexpected problems.

(5) I would feel safe giving (the information) to online companies. (*r*)*

Intention to Give Information: Seven-point semantic scales (MacKenzie and Spreng 1992).

Given this hypothetical scenario, specify the extent to which you would reveal (the information) through the Internet.

(1) Unlikely/likely
(2) Not probable/probable
(3) Possible/impossible (*r*)*
(4) Willing/unwilling (*r*)

Covariates: Smith et al. (1996) and some items newly developed.

(1) Sex: (1 = male; 2 = female).

(2) Age: (1 = 25–34; 2 = 35–44; 3 = 45–54; 4 = 55–64; 5 = over 65 years).

(3) Education: (1 = some school, no degree; 2 = high school graduate; 3 = some college, no degree; 4 = bachelor's degree; 5 = master's degree; 6 = professional degree; 7 = doctorate degree).

(4) Internet experience: (1 = less than a year; 2 = 1–less than 2 years; 3 = 2–less than 3 years; 4 = 3–less than 4 years; 5 = 4–less than 5 years; 6 = 5–less than 6 years; 7 = 6–less than 7 years; 8 = more than 7 years).

(5) Misrepresentation of identification: Some websites ask for you to register with the site by providing personal information. When asked for such information, what percent of the time do you falsify the information? (1 = I have never falsified information; 2 = under 25% of the time; 3 = 26%–50% of the time; 4 = 51%–75% of the time; 5 = over 75% of the time)

(6) Privacy victim: How frequently have you personally been the victim of what you felt was an improper invasion of privacy? (1 = very infrequently; 7 = very frequently)

(7) Media exposure: How much have you heard or read during the last year about the use and potential misuse of the information collected from the Internet? (1 = not at all; 7 = very much)

Notes. Items under collection, control, and awareness constitute the 10-item IUIPC scale. Items under collection, errors, unauthorized secondary use, and improper access constitute the 15-item CFIP scale.

*Item deleted; (*r*) reverse item.

References

Ajzen, I. 1991. The theory of planned behavior, *Organ. Behavior Human Decision Processes* **50** 179–211.

Alge, B. J. 2001. Effects of computer surveillance on perceptions of privacy and procedural justice. *J. App. Psych.* **86**(4) 797–804.

Anderson, J. C., D. W. Gerbing. 1988. Structural equation modeling in practice: A review and recommended two-step approach. *Psych. Bull.* **103**(3) 411–423.

Andrews, S. 2002. Privacy and human rights 2002: An international survey of privacy laws and developments. http://www.privacyinternational.org/survey/phr2002/.

Bagozzi, R. P., T. F. Heatherton. 1994. A general approach to representing multifaceted personality constructs: Application to state self-esteem. *Structural Equation Model* **1**(1) 35–67.

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

Bearden, W. O., R. G. Netemeyer, M. F. Mobley. 1993. *Handbook of Marketing Scales: Multi-item Measures for Marketing and Consumer Behavior Research.* Sage Publications, Newbury Park, CA.

Bies, R. J., J. S. Moag. 1986. Interactional justice: Communication criteria of fairness. M. Bazerman, R. Lewicki, B. Sheppard, eds. *Research on Negotiations in Organizations*, Vol. 1. JAI Press, Greenwich, CT, 43–55.

Bozdogan, H. 1987. Model selection and Akaike's information criterion (AIC): The general theory and its analytical extensions. *Psychometrika* **52**(3) 345–370.

Campbell, A. J. 1997. Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *J. Direct Marketing* **11**(3) 44–57.

Campbell, D. T. 1960. Recommendations for APA test standards regarding construct, trait, or discriminant validity. *Amer. Psych.* **15**(August) 546–553.

Campbell, D. T., D. W. Fiske. 1959. Convergent and discriminant validation by the multi-trait–multi-method matrix. *Psych. Bull.* **56** 2(March) 81–105.

Caudill, E. M., P. E. Murphy. 2000. Consumer online privacy: Legal and ethical issues. *J. Public Policy Marketing* **19**(1) 7–19.

Cespedes, F. V., H. J. Smith. 1993. Database marketing: New rules for policy and practice. *Sloan Management Rev.* **34**(4) 7–22.

Chin, W. W. 1998. The partial least squares approach to structural equation modeling. G. A. Marcoulides ed. *Modern Methods for Business Research.* Lawrence Erlbaum Associates, Mahwah, NJ, 295–336.

Chin, W. W., A. Gopal, W. D. Salisbury. 1997. Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation. *Inform. Systems Res.* **8**(4) 342–367.

Cohen, R. L. 1987. Distributive justice: Theory and research. *Soc. Justice Res.* **1** 19–40.

Cronbach, L. J. 1990. *Essentials of Psychological Testing.* Harper-Row, New York.

Culnan, M. J. 1995. Consumer awareness of name removal procedures: Implications for direct marketing. *J. Direct Marketing* **9**(2) 10–19.

Culnan, M. J. 2000. Protecting privacy online: Is self-regulation working? *J. Public Policy Marketing* **19**(1) 20–26.

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

Donaldson, T. 1989. *The Ethics of International Business.* Oxford University Press, New York.

Donaldson, T., T. W. Dunfee. 1994. Towards a unified conception of business ethics: Integrative social contracts theory. *Acad. Management Rev.* **19**(2) 252–284.

Dowling, G. R., R. Staelin. 1994. A model of perceived risk and intended risk-handling activity. *J. Consumer Res.* **21**(June) 119–134.

Dunfee, T. W., N. C. Smith, W. T. Ross Jr. 1999. Social contracts and marketing ethics. *J. Marketing* **63**(July) 14–32.

Fishbein, M., I. Ajzen. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.* Addison-Wesley, Reading, MA.

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

Foxman, E. R., P. Kilcoyne. 1993. Information technology, marketing practice, and consumer privacy: Ethical issues. *J. Public Policy Marketing* **12**(1) 106–119.

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

Gilliland, S. W. 1993. The perceived fairness of selection systems: An organizational justice perspective. *Acad. Management Rev.* **18**(4) 694–734.

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

Grazioli, S., S. L. Jarvenpaa. 2000. Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Tran. Systems, Man, Cybernetics, Part A: Systems Humans* **30**(4) 395–410.

Greenberg, J. 1990. Organizational justice: Yesterday, today, and tomorrow. *J. Management* **16** 399–432.

Hair J. F., R. E. Anderson, R. L. Tatham, W. C. Black. 1995. *Multivariate Data Analysis with Readings*, 4th ed. Prentice Hall, Upper Saddle River, NJ.

Heide, J. B., G. John. 1992. Do norms matter in marketing relationships? *J. Marketing* **56**(April) 32–44.

Hoffman, D. L., T. P. Novak. 1996. Marketing in hypermedia computer-mediated environments: Conceptual foundations. *J. Marketing* **60**(July) 50–68.

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

Hu, L., P. M. Bentler. 1999. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Model* **6**(1) 1–55.

Jarvenpaa, S. L., N. Tractinsky. 1999. Consumer trust in an internet store: A cross-cultural validation. *J. Comput.-Mediated Comm.* **5**(2), http://www.ascusc.org/jcmc/vol5/issue2/jarvenpaa.html.

Jöreskog, K., D. Sorbom, S. Toit, M. Toit. 1999. *LISREL8: New Statistical Features*. Scientific Software International, Chicago, IL.

Keppel, G. 1991. *Design and Analysis: A Researcher's Handbook*. Prentice-Hall, Englewood Cliffs, NJ.

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

Luo, X. 2002. Trust production and privacy concerns on the internet: A framework based on relationship marketing and social exchange theory. *Indust. Marketing Management* **31**(2) 111–118.

MacKenzie, S. B., R. A. Spreng. 1992. How does motivation moderate the impact of central and peripheral processing on brand attitudes and intentions? *J. Consumer Res.* **18**(March) 519–529.

Malhotra, N. K. 2004. *Marketing Research: An Applied Orientation*, 4th ed. Prentice Hall, Upper Saddle River, NJ.

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

McKnight, D. H., N. L. Chervany. 2000. What is trust? A conceptual analysis and an interdisciplinary model. *Proc. 2000 Americas Conf. Inform. Systems*, Long Beach, CA, 827–833.

McKnight, D., L. L. Cummings, N. L. Chervany. 1998. Initial trust formation in new organizational relationships. *Acad. Management Rev.* **23**(3) 473–490.

Mehta, R., E. Sivadas. 1995. Direct marketing on the Internet: An empirical assessment of consumer attitudes. *J. Direct Marketing* **9**(3) 21–32.

Meng, X., R. Rosenthal, D. B. Rubin. 1992. Comparing correlated coefficients. *Psych. Bull.* **111** 172–75.

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

Milne, G. R., M. E. Gordon. 1993. Direct mail privacy-efficiency trade-offs within an implied social contract framework. *J. Public Policy Marketing* **12**(2) 206–215.

Milne, G. R., A. J. Rohm. 2000. Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *J. Public Policy Marketing* **19**(2) 238–249.

Mineta, N. 2000. *Opening Statement at Online Privacy Technologies Workshop and Technology Fair*. U.S. Department of Commerce, Washington, D.C. (September 19) http://www.ntia.doc.gov/ntiahome/privacy/900workshop/mineta91900.htm.

Miyazaki, A. D., A. Fernandez. 2000. Internet privacy and security: An examination of online retailer disclosures. *J. Public Policy Marketing* **19**(1) 54–61.

Miyazaki, A. D., A. Fernandez. 2001. Consumer perceptions of privacy and security risks for online shopping. *J. Consumer Affairs* **35**(1) 27–44.

Moorman, C., G. Zaltman, R. Deshpande. 1992. Relationships between providers and users of marketing research: The dynamics of trust within and between organizations. *J. Marketing Res.* **29**(August) 314–329.

Morgan, R. M., S. D. Hunt. 1994. The commitment-trust theory of relationship marketing. *J. Marketing* **58**(3) 20–38.

Newman, D., S. Rao. 2000. Regulatory aspects of privacy and security: A view from the advanced communications technologies and services programme. *Inform. Comm. Tech. Law* **9**(2) 161–166.

Nowak, G. J., J. Phelps. 1992. Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *J. Direct Marketing* **6**(4) 28–39.

Nowak, G. J., J. Phelps. 1995. Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *J. Direct Marketing* **9**(3) 46–60.

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

Pew Internet Project. 2000. Trust and privacy online: Why Americans want to rewrite the rules. Pew Internet & American Life Project, http://www.pewinternet.org/reports/toc.asp?Report=19.

Phelps, J., G. Nowak, E. Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *J. Public Policy Marketing* **19**(1) 27–41.

Regan, P. M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, Chapel Hill, NC.

Rendleman, J. 2001. Customer data means money. *InformationWeek* **851**(August) 49–50.

Rogers, T. B. 1995. *The Psychological Testing Enterprise*. Brooks/Cole Publishing Company, Pacific Grove, CA.

Shapiro, D. L., E. H. Buttner, B. Barry. 1994. Explanations: What factors enhance their perceived adequacy? *Organ. Behavior Human Decision Processes* **58** 346–368.

Sheehan, K. B., M. G. Hoy. 2000. Dimensions of privacy concern among online consumers. *J. Public Policy Marketing* **19**(1) 62–73.

Sirdeshmukh, D., J. Singh, B. Sabol. 2002. Consumer trust, value, and loyalty in relational exchanges. *J. Marketing* **66**(January) 15–37.

Smith, H. J., S. J. Milberg, S. J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* **20**(2) 167–196.

Steenkamp, J. E. M., H. Baumgartner. 1998. Assessing measurement invariance in cross-national consumer research. *J. Consumer Res.* **25**(June) 78–90.

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

Straub, D., E. Karahanna. 1998. Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organ. Sci.* **9**(2) 160–175.

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

Thibaut, J., L. Walker. 1975. *Procedural Justice: A Psychological Analysis*. Erlbaum, Hillsdale, NJ.

Tyler, T. R. 1994. Psychological models of the justice motive: Antecedents of distributive and procedural justice. *J. Personality Soc. Psych.* **67** 850–863.

U.S. Department of Commerce. 2002. Digital economy 2002. http://www.esa.doc.gov/pdf/DE2002r1.pdf.

University of California–Los Angeles Center for Communication Policy. 2001. The UCLA Internet report 2001: Surveying the digital future. http://ccp.ucla.edu/pdf/UCLA-Internet-Report-2001.pdf.

Venkatraman, N. 1989. Strategic orientation of business enterprises—The construct, dimensionality, and measurement. *Management Sci.* **35**(8) 942–962.

Wang, P., L. A. Petrison. 1993. Direct marketing activities and personal privacy: A consumer survey. *J. Direct Marketing* **7**(1) 7–19.

Webster, J., L. K. Trevino. 1995. Rational and social theories as complementary explanations of communication media choices: Two policy capturing studies. *Acad. Management J.* **28**(6) 1544–1572.

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

Wulf, K. D., G. Odekerken-Schröder, D. Iacobucci. 2001. Investments in consumer relationships: A cross-country and cross-industry exploration. *J. Marketing* **65**(October) 33–50.

Zucker, Lynne G. 1986. Production of trust: Institutional sources of economic structure, 1840–1920. *Res. Organ. Behavior* **8** 53–111.