MIS Quarterly

RESEARCH ARTICLE

INTERNET USERS' INFORMATION PRIVACY-PROTECTIVE RESPONSES: A TAXONOMY AND A NOMOLOGICAL MODEL[1]

By: **Jai-Yeol Son**
School of Business
Yonsei University
134 Shinchon-Dong, Seodaemoon-ku
Seoul 120-749
KOREA
tmisrj@gmail.com

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

Abstract

*Although Internet users are expected to respond in various ways to privacy threats from online companies, little attention has been paid so far to the complex nature of how users respond to these threats. This paper has two specific goals in its effort to fill this gap in the literature. The first, so that these outcomes can be systematically investigated, is to develop a taxonomy of information privacy-protective responses (IPPR). This taxonomy consists of six types of behavioral responses—**refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies,** and **complaining indirectly to third-party organizations**—that are classified into three categories: **information provision, private action,** and **public action.** Our second goal is to develop a nomological model with several salient antecedents—**concerns for information privacy, perceived justice,** and **societal benefits from complaining**—of IPPR, and to show how the antecedents differentially affect the six types of IPPR. The nomological model is tested with data collected from 523 Internet users. The results indicate that some discernible patterns emerge in the relationships between the antecedents and the three groups of IPPR. These patterns enable researchers to better understand why a certain type of IPPR is similar to or distinct from other types of IPPR. Such an understanding could enable researchers to analyze a variety of behavioral responses to information privacy threats in a fairly systematic manner. Overall, this paper contributes to researchers' theory-building efforts in the area of information privacy by breaking new ground for the study of individuals' responses to information privacy threats.*

Keywords: Information privacy, responses to information privacy threats, information privacy concerns, ethical issues, structural equation modeling, causal model

Introduction

Since the dawn of electronic commerce, information privacy has been regarded as one of the greatest impediments to the growth of electronic commerce. Consequently, much attention has been devoted to information privacy as one of the issues critical to the success of e-commerce. Nonetheless, the information privacy of many individuals seems to have been seriously threatened, if not compromised. A survey on information privacy found that about 25 percent of Americans

[1]Bernard C. Y. Tan was the accepting senior editor for this paper. Jeff Smith was the associate editor. Norm Chervany, Bradley Alge, and May Lwin served as reviewers.

consider themselves victimized by invasion of their information privacy (*BusinessWeek* 2000). It also has been reported that the personal information of 33.6 million Americans has been used for fraudulent purposes since 1990 (CNET News 2004). Furthermore, as firms use technologies such as customer relationship management to launch individually targeted marketing programs, their information practices may conflict with the information privacy rights of customers. Because of the potentially serious consequences, such as identity theft, of violations of the privacy of information, many Internet users are expected to adopt certain forms of behavior to protect their information privacy.

Much research to date has focused on understanding what motivates Internet users to divulge personal information and what inhibits them from divulging it. In particular, Internet users' privacy concerns have received considerable attention as one of the salient factors that determines their willingness or unwillingness to divulge personal information to online companies (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). Information privacy concerns refer to the extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Smith et al. 1996). Studies have unequivocally found Internet users' information privacy concerns to be a major antecedent of their willingness to divulge personal information to online companies.

The major assumption underlying this line of research is that individuals with a high concern for the privacy of their information will try to protect this privacy by responding unfavorably to organization's information practices when they think their privacy rights are threatened (Smith et al. 1996; Stone et al. 1983). However, most studies focusing on privacy concerns (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002) have examined only a single type of Internet users' responses—refusal to provide personal information—as a major behavioral response to these threats. This one-dimensional approach ignores the possibility that online users can perceive threats to the privacy of their information in numerous practices by online companies and respond in ways not limited to refusal to divulge information. Among the other options available to wary online users are removal of their personal information from the database of online companies and the lodging of complaints with third-party privacy organizations. Therefore, it is important to systematically understand other possible responses by Internet users to information privacy threats.

The main objective of this paper is to offer a systematic understanding of a variety of Internet users' information privacy-protective responses (IPPR) so as to advance theoretical development in the information privacy arena. To achieve the objective, we first propose a taxonomy of IPPR. This taxonomy is designed to capture and classify an array of individuals' responses to information privacy threats; it is expected to assist in understanding how various types of responses resemble or differ from each other. Second, although individuals' concerns for information privacy are likely to play a major role in determining their IPPR, such responses are expected to be a function of other factors in addition to their concerns for the privacy of their information. Thus, our second objective is to identify other salient determinants of IPPR that can demonstrate how the antecedents differentially affect six types of IPPR over and above concerns about information privacy. In this way, we may be able to better understand *why* a certain type of response resembles or differs from other types. Overall, this research is expected to contribute to researchers' theory-building efforts in the area of information privacy by enabling them to build a wealth of knowledge about relationships between types of IPPR and other constructs.

Information Privacy-Protective Responses

Information privacy refers to an individual's ability to control when, how, and to what extent his or her personal information is communicated to others (Stone et al. 1983; Westin 1967). The notion of information privacy has recently come to be viewed as a critical ethical issue that deserves attention from both scholars and practitioners (Smith et al. 1996). Successfully addressing information privacy issues in an online environment is particularly relevant to the growth of the information age. This is especially true for online companies because their success and quality of customer service hinge largely on their ability to collect and analyze a large amount of personal information about Internet users. Thus it is critical for online companies to understand various types of Internet users' responses to their information practices.

In this study, we are introducing the notion of ***information privacy-protective responses*** (IPPR) and define it as a set of Internet users' behavioral responses to their perception of information privacy threats that result from companies' information practices. Internet users can perceive threats to their information privacy merely when they are asked to provide personal information to online companies and also in other numerous and more subtle ways in their interactions with online companies in which the companies' information practices and policies are involved. Several responses are open to them in the face of such perceived threats. In particular, IPPR

focuses on three broad types of behavioral responses to information privacy threats among Internet users: ***information provision***, ***private action***, and ***public action*** (see Figure 1). When Internet users perceive information privacy threats from requests to provide personal information, their main response for protection of information privacy is to refuse to disclose their personal information. Internet users can be dissatisfied with how online companies handle their personal information after they find out that online companies mishandle it.[2] Accordingly, drawing on the literature on customer dissatisfaction that has proposed a taxonomy of complaint behavior (Day and Landon 1977; Singh 1988), we add two other categories of private and public actions based on whether or not Internet users seek redress for online companies' mishandling of personal information. For instance, when Internet users perceive that their personal information is mishandled, they may take private actions by no longer patronizing online companies and/or by communicating their negative experience to others, including friends and relatives. Also, they may seek redress by engaging in public actions by complaining to online companies and/or to third-party privacy organizations.

Information Provision

As a condition of access or usage, many online companies require Internet users to complete a registration form that requires personal information. However, because users are concerned about their information privacy, such requests are often refused, or if not, completed with falsified data (Milne and Boza 1999). Thus, the literature treats an individual's refusal to provide information and an individual's response with falsified information as two of the major ways that Internet users protect their information privacy.

First, several studies on information privacy have focused on whether or not individuals refuse marketers' requests for personal information (Malhotra et al. 2004; Phelps et al. 2000; Smith et al. 1996; Stewart and Segars 2002). Online companies generally use the information as a stepping stone to building long-term relationships with their customers. Of course, certain types of personal information about Internet users can be collected by analyzing their online behaviors (e.g., cookies, clickstream technologies). Many Internet users are not fully aware of such involuntary disclosure of their personal information until they receive targeted marketing messages from online companies (Milne 2000). Although data about Internet users' online behaviors can be collected through such involuntary disclosure, much of the important personal information necessary for online companies to implement targeted marketing programs can be obtained only through Internet users' voluntary disclosures (e.g., filling out a registration form). Thus, Internet users' ***refusal*** to provide their personal information to online companies is believed to be an important form of information provision behavior.

Second, in a similar vein, scholars have noted that what really matters to online businesses is to induce Internet users to divulge correct personal information (Teo et al. 2004). Several past surveys within the context of information privacy reported that 20 percent to 50 percent of the responding Internet users had falsified the personal information submitted to online companies (Cavoukian and Hamilton 2002; Hoffman et al. 1999). Consumers highly concerned about threats to their information privacy may consider misrepresentation a less costly and more convenient option compared with recourse to complaining to third-party privacy organizations (Lwin and Williams 2003). This is problematic to online companies because errors in their customer databases are costly. Incorrect information in customer databases can propagate errors in other databases and jeopardize targeted marketing efforts (Lwin and Williams 2003). Thus, information provision is not simply a matter of whether to release information but also a matter of whether to release correct information. Consequently, along with Internet users' refusal to provide personal information, their ***misrepresentation*** of personal information is regarded as another important form of information provision behavior designed to protect the privacy of their information.

In summary, we propose that information provision constitutes one of the important responses that individuals can use to protect their information privacy. This study focuses on two specific forms of responses—refusal and misrepresentation—and classifies them in the information provision category of IPPR.

Private Action

Information privacy can be threatened when Internet users lose control over how online companies collect and handle their personal information (Malhotra et al. 2004). Examples of such loss of control range from receiving unwanted e-mail

[2]According to a cognitive perspective on consumer satisfaction, consumers generally form preconsumption expectancies, compare actual performance of products/services with expectations, and form disconfirmation perceptions, which will in turn determine their level of satisfaction/dissatisfaction with the products/services (Oliver 1993). Similarly, Internet users may form expectations about how online companies should handle their personal information, and perceive high levels of information threats when their expectations are disconfirmed with the information practices of online companies. The extent to which they are disconfirmed is expected to determine the level of satisfaction/dissatisfaction with online companies' handling of personal information.

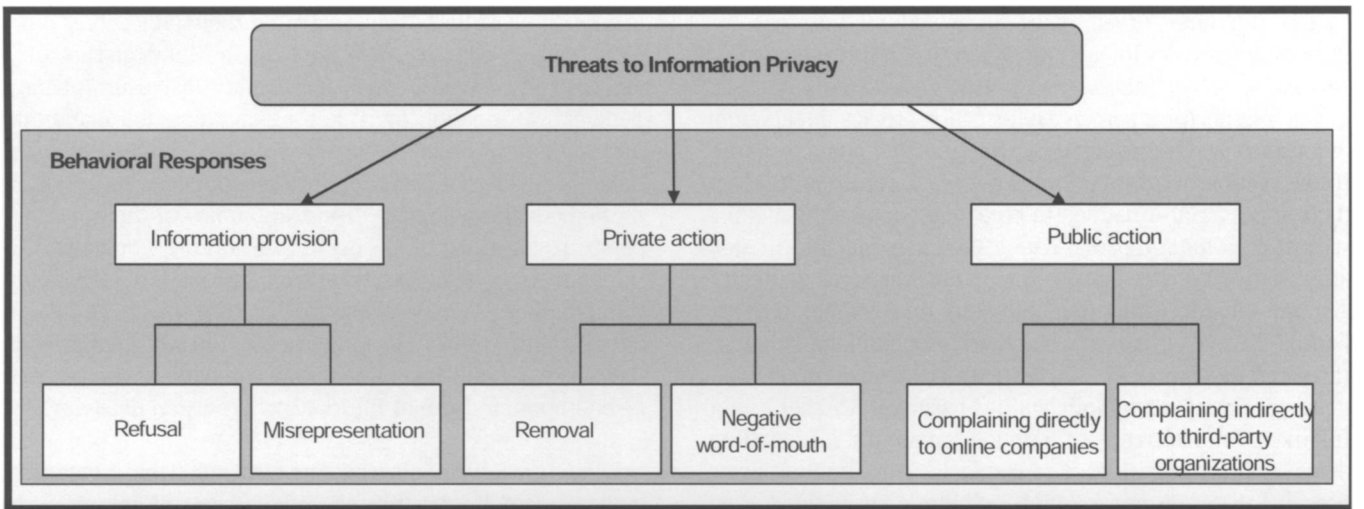

Figure 1. A Taxonomy of IPPR

marketing messages to tracking by online companies of their activities on the companies' websites and to the selling of customers' personal information to other online companies. Particular attention has been paid to the literature on customer complaint behavior to identify additional categories within a taxonomy of IPPR. The literature suggests that dissatisfied customers often undertake certain forms of private action (Day 1980; Day and Landon 1977; Singh 1988). Examples include a personal boycott of a particular seller and negative word-of-mouth. The primary recourse through private action is to quit patronizing a store and to communicate dissatisfaction to acquaintances, including friends and relatives (Day and Landon 1977).

Similar to a dissatisfied customer's personal boycott of a particular seller, one specific form of private action that an individual can take in response to an information privacy threat is ***removal*** of his or her personal information from online companies' databases (Smith et al. 1996). For instance, Internet users can choose opt-out procedures when they perceive high levels of threats to information privacy because of customized marketing messages via e-mail from online companies. Another form of private action is Internet users' ***negative word-of-mouth*** communication to acquaintances about their experiences with offending online companies. That is, Internet users may share their negative experiences with their friends and relatives when online companies threaten their information privacy. Negative word-of-mouth communication is expected to damage the reputation of online companies and reduce their future sales (Resnick et al. 2000).

Public Action

The literature on customer complaint behavior suggests that dissatisfied customers often undertake certain forms of public action (Day 1980; Day and Landon 1977; Singh 1988). The primary goal of taking public action is to seek a specific remedy (Singh 1988). Public action generally fits into two behavioral types: direct complaints to sellers and indirect complaints made to third-party organizations. Dissatisfied customers generally take action through third-party organizations when they do not obtain satisfactory redress by direct complaints (Singh 1989). However, researchers also indicate that customers often do not complain directly to sellers but instead seek a remedy through third-party organizations. They noted this is especially true when customers feel helpless in confronting sellers (Brown and Swartz 1984).

Similarly, we propose that Internet users dissatisfied with online companies' handling of their personal information have two forms of public recourse in seeking a remedy: ***complaining directly to online companies*** and ***complaining indirectly to third-party organizations***. First, an Internet user who feels threatened by an online company can contact the company to complain. Second, an Internet user may respond by either complaining to independent third-party privacy groups (e.g., BBBOnline, TRUSTe, etc.) or by engaging in privacy litigation. For instance, if the company that is the source of the threat is a TRUSTe seal holder, an Internet user can file a complaint form with TRUSTe and the nonprofit, privacy advocate will try to mediate a solution (Benassi

1999). This behavior differs from private action taken in the form of negative word-of-mouth because, in the latter case, the negative experience is merely communicated to relatives and acquaintances without any pursuit of a remedy. By complaining to independent third-party privacy groups, an Internet user will try not only for an individual benefit but also to benefit other Internet users by preventing the company from similar future privacy violations. Just as proper handling of complaints can lead to customer retention (Kelley et al. 1993), online companies may be able to rebuild a relationship with their customers if they can properly handle complaints received either directly from customers or indirectly through third-party privacy groups.

Antecedents of IPPR

The preceding section offered a taxonomy of IPPR as a guideline to understanding multiple behavioral responses that Internet users may make in situations in which online companies threaten their information privacy rights. In this section, we will develop a nomological model by identifying three types of antecedent beliefs—information privacy concerns, perceived justice, and societal benefits from complaining—as the major determinants of IPPR and by proposing various differential effects of these antecedents. We chose the three antecedents because we found them to be among the most salient antecedents of IPPR and to demonstrate satisfactorily the taxonomy structure of IPPR. Specifically, the three antecedents were identified by incorporating theoretical reasoning and empirical evidence obtained from three literature streams: information privacy, justice framework, and consumer complaint behavior. Of course, other types of antecedent beliefs may exist that have strong impacts on certain types of IPPR. However, this study focuses on a parsimonious set of three antecedents, given that the primary objective of developing the nomological model is to validate the proposed taxonomy structure of IPPR rather than to offer a comprehensive set of antecedents.

The nomological model is built on the belief–behavioral intention link because the antecedents identified are several types of Internet users' beliefs that are expected to influence their intention to take certain forms of IPPR. Many IS researchers relied on the belief–behavioral intention link to examine users' behaviors within a variety of contexts: IT adoption (Davis 1989; Davis et al. 1989), online trust (McKnight et al. 2002), and information privacy (Dinev and Hart 2006; Malhotra et al. 2004). They have suggested that the belief–behavioral intention link is tightly rooted in the theory of reasoned action (TRA) (Ajzen and Fishbein 1980). Although other components like attitude and subjective norm are included in TRA, they viewed belief and behavioral intention as "the primary elements of the TRA model" (Dinev and Hart 2006, p. 62).

Based on the belief–behavioral intention link, the three sets of salient beliefs are posited to influence Internet users' intention to engage in IPPR. Specifically, by empirically testing the nomological model that will be developed in this section, we aim to validate the proposed taxonomy structure of IPPR within a nomological model in which the six types of behaviors have theoretically different patterns, correlated and uncorrelated, with a set of antecedent constructs (Cronbach and Meehl 1955). The nomological model of the six dimensions of IPPR and their antecedents is provided in Figure 2. Antecedent beliefs are listed in Table 1, along with their operationalized definitions.

Information Privacy Concerns

Past research into issues associated with information privacy has focused on understanding what motivates Internet users to divulge personal information and what inhibits them from divulging it. Of several constructs examined in earlier studies, Internet users' concerns for information privacy have received considerable attention as a salient belief that determines their willingness or unwillingness to divulge personal information to online companies (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). Because of a variety of factors such as culture, regulatory laws, past experiences, and personal characteristics, Internet users exhibit different levels of concerns about information privacy (Malhotra et al. 2004). Internet users with high levels of concerns about information privacy believe that companies generally tend to behave opportunistically with their personal information. Hence, in response to a request from online companies for personal information, they will likely respond by undertaking two specific forms of IPPR under the information provision category: refusing to provide personal information (Dinev and Hart 2006) and/or providing incorrect personal information (Teo et al. 2004).

Individuals with information privacy concerns are concerned about online companies' practices related not only to the collection but also to the use of their personal information (Smith et al. 1996). In particular, individuals with high levels of concerns about information privacy believe that online companies' misuse of their personal information can result in considerable loss (Dinev and Hart 2006; Van Slyke et al. 2006). Thus, to prevent such opportunism and minimize the loss from misuse, they are more likely to take other types of

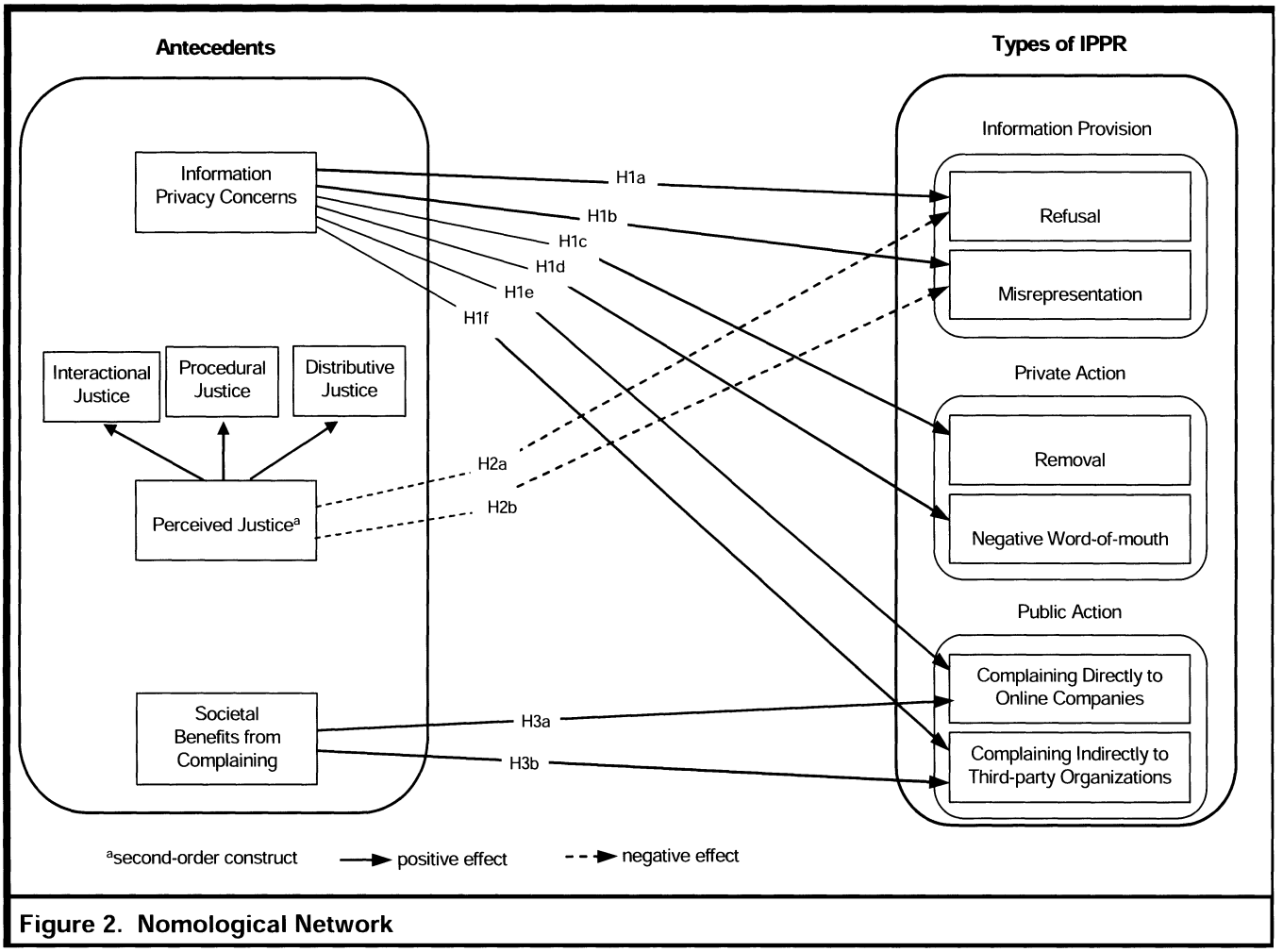

Figure 2. Nomological Network

Table 1. Antecedent Beliefs of IPPR

Constructs	Definition
Information privacy concerns	Degree to which an Internet user is concerned about online companies' practices related to the collection and use of his or her personal information
Perceived justice	Degree of fairness that an Internet user perceives about online companies' treatment related to information privacy
Distributive justice	Degree to which an Internet user perceives as fair the benefits he or she receives from online companies in return for the release of personal information
Procedural justice	Degree to which an Internet user perceives that online companies give him or her procedures for control of information privacy and make him or her aware of the procedures
Interactional justice	Degree to which an Internet user perceives of online companies as honest and trustworthy in complying with their promises related to information privacy
Societal benefits from complaining	Degree to which an Internet user perceives that complaining about privacy invasions will benefit other Internet users by preventing them from being similarly victimized

IPPR (i.e., private and public actions) in response to the companies' misuse of their personal information. For instance, they are likely to remove personal information from the databases of online companies in response to threats associated with misuse of their personal information (Milne et al. 2004). Because many online companies rely on certain personal information to maintain relationships with their customers, Internet users can end the relationship by simply removing personal information from the companies' databases. Further, when online companies mishandle their personal information, Internet users with high levels of information privacy concerns are more likely to share their negative experiences with their friends and relatives because these Internet users tend to believe that the loss from the companies' opportunism will be significant to their close acquaintances. By sharing their negative experiences, Internet users with high levels of concerns about information privacy intend to prevent their acquaintances from being victimized by similar privacy violations.

In addition to taking two forms of private actions (i.e., removal and negative word-of-mouth), Internet users with high levels of information privacy concerns are more likely to speak against online companies that threaten their information privacy (Smith et al. 1996). Specifically, to seek a remedy for the violation, they can complain directly to online companies and indirectly to third-party organizations when their information privacy is threatened (Smith et al. 1996). This is because Internet users with high levels of information privacy concerns think that the loss from privacy violations is considerable. Smith et al. (1996) offered preliminary empirical evidence to support such an assertion. They viewed various types of information privacy protective behaviors collectively as a single construct and measured the construct with items related to different types of protective behaviors (e.g., refusal, removal, complaining directly to online companies, complaining indirectly to third-party organizations). They re ported a high level of correlation between individuals' concerns for information privacy and the single construct of information privacy protective behaviors. We therefore propose information privacy concerns as an important determinant of each of the six types of IPPR and develop the following hypotheses:

H1a: Information privacy concerns will have a positive impact on Internet users' refusal to provide their personal information to online companies.

H1b: Information privacy concerns will have a positive impact on Internet users' misrepresentation of personal information to online companies.

H1c: Information privacy concerns will have a positive impact on Internet users' removal of personal information from the databases of online companies that threaten information privacy.

H1d: Information privacy concerns will have a positive impact on Internet users' negative word-of-mouth communication to others about online companies' threats to information privacy.

H1e: Information privacy concerns will have a positive impact on Internet users' complaining directly to online companies that threaten information privacy.

H1f: Information privacy concerns will have a positive impact on Internet users' complaining indirectly to third-party privacy organizations about online companies' threats to information privacy.

Perceived Justice

Justice (also known as *fairness*) is viewed as a central concern in social exchange relationships (Cialdini 1993). According to a justice perspective, the degree of fairness a party (A) perceives about its treatment by another party (B) over the course of the relationship has a profound impact on various behaviors of A in regard to interactions with B (Culnan 1995; Martinez-Tur et al. 2006). The justice perspective has been applied widely as a theoretical foundation to the understanding of various phenomena, including relationships between employees and their employers (McFarlin and Sweeney 1992), between customers and merchants (Bettencourt et al. 2005; Martinez-Tur et al. 2006), and between firms at adjacent stages in a value chain (Kumar et al. 1995). For instance, employees' perceptions of justice received from their employer are strong predictors of their job satisfaction (McFarlin and Sweeney 1992). Similarly, customer satisfaction is largely influenced by how customers evaluate the justice of procedures and outcomes associated with the purchase of products and services (Martinez-Tur et al. 2006).

The notion of justice has recently received growing attention as a central variable that should be examined in situations in which privacy becomes a critical concern between parties. Accordingly, scholarly effort has been devoted to the understanding of the interrelationships between justice and privacy (Bies 1993). For instance, in situations in which employers monitored their employees for control or for performance evaluation purposes, the employees considered electronic

monitoring unfair when they felt high levels of privacy invasion because of the electronic monitoring (Alge 2001; Zweig and Webster 2002). Employees' perceptions of justice generally relate negatively to their privacy perceptions (Eddy et al. 1999). In consumer marketing, it has been suggested that consumers' justice perceptions of how companies deal with their personal information could motivate them to disclose personal information, although they might also perceive the requests to provide personal information as a threat to their information privacy (Culnan and Armstrong 1999; Culnan and Bies 2003). Drawing on the wealth of literature on the justice framework, we conceptualized and operationalized the perceived justice construct with three distinct, but closely interrelated, dimensions: distributive, procedural, and interactional justice (Culnan and Bies 2003).

Distributive Justice

Rooted in equity theory, distributive justice is mainly concerned with the perceived fairness of outcomes or rewards that a party receives from another party in an exchange relationship (Homans 1961; Martinez-Tur et al. 2006). For instance, in the customer–irm exchange relationship, customers invest inputs like money and time in anticipation of receiving outcomes like products or services (Martinez-Tur et al. 2006). Customers will weigh the amount of input against the quality of products or services, and their subjective evaluations of the balance between them will become the basis of their overall satisfaction. Similarly, Internet users apply a comparable cost–benefit analysis when they are asked to disclose personal information to online companies. They will carefully assess whether what they give up in terms of personal information will outweigh what will be received (Culnan and Bies 2003; Dinev and Hart 2006; Tam et al. 2002). We therefore applied the concept of distributive justice to the context of information privacy in an Internet environment. We define it as Internet users' perceived fairness of the outcome that they receive from online companies in return for releasing their personal information.

Internet users are enticed to reveal their personal information not only because of immediate monetary rewards but also because online companies will provide a high level of service over the long term by using the personal information provided. For example, according to a survey conducted by the Ponemon Institute, a research firm dedicated to privacy management practices in business, about 82 percent of the responding individuals like to be contacted by online companies if the companies offer incentives such as discounts or free offers (Germain 2005). In addition to immediate monetary rewards, Internet users are likely to reveal their personal information to online companies when they expect the information to be used to forge a mutually beneficial relationship. For instance, Internet users anticipate that they can be offered products and services better suited for their needs and preferences when online companies possess their personal information. Accordingly, Internet users will be less reluctant to provide their personal information when their assessment, referred to as a ***privacy calculus***, indicates that they can derive large benefits from online companies' possession of their personal information without suffering negative consequences (Dinev and Hart 2006; Laufer and Wolfe 1977).

Procedural Justice

Justice researchers have indicated that one party evaluates justice received from another party in an exchange relationship not only on the basis of the outcomes from the relationship but also on the formal procedures used to arrive at the outcome (Martinez-Tur et al. 2006; Thibaut and Walker 1975). Along with distributive justice, this type of justice, labeled procedural justice, has been proposed as another important dimension that influences one's overall assessment of justice received from another (Bettencourt et al. 2005). In an exchange relationship, one party (A) generally seeks assurance against unfavorable treatment from another party (B) over the long-term. The presence of formal procedures provides A with such assurance so that A will react more favorably to a request from B (Rahim et al. 2000). Within the context of consumer privacy, Culnan and Armstrong (1999) found that when customers are told explicitly that a company will observe fair information procedures, they are more willing to disclose their personal information to the company and to allow the company to subsequently use the information to develop target marketing.

When applied within the context of information privacy in the online environment, what have been referred to as ***control*** and ***awareness*** are identified as among the most relevant practices that online companies can use to assure Internet users of procedural fairness (Malhotra et al. 2004). Internet users who are vested with control of online companies' information privacy procedures view these procedures as fair. Accordingly, to increase the perceived fairness of their procedures for handling personal information, online companies need to give their customers a certain level of control over the collection and use of their personal information. For example, online companies can give their customers a choice of whether to be included in their database to receive targeted marketing messages (Culnan and Bies 2003). It should also be noted that Internet users generally develop their perceptions of procedural fairness not only on their level of control

over information privacy procedures but also on their awareness of these procedures (Foxman and Kilcoyne 1993). The fact that well-designed information procedures are present does not guarantee awareness by users of how their personal information will be handled, which means online companies should undertake to ensure that their customers are aware of the procedures (Culnan and Bies 2003). For example, Hui et al. (2007) found that Internet users are more likely to reveal their personal information when they read a privacy statement outlining information practices of online companies. To summarize, the closely interrelated concepts of control and awareness play a key role in developing Internet users' perceptions of fair information procedures. We accordingly conceptualize procedural justice in the context of information privacy as the extent to which Internet users perceive that online companies give them procedures for control over information privacy and make them aware of the procedures.

Interactional Justice

Interactional justice, which refers to a party's perceived fairness of interpersonal treatment by another party in an exchange relationship (Bettencourt et al. 2005), was first introduced by Bies and Moag (1986). Since then, many justice researchers have regarded it as another important dimension that a party can use to evaluate the overall justice received from another party (Colquitt 2001). In particular, interactional justice was identified as conceptually distinct from procedural justice. Procedural justice focuses on issues related to the fairness of policies and procedures enacted to govern exchange relationships; interactional justice mainly deals with the exchange parties' responsibilities associated with ensuring fairness in the implementation of the policies and procedures over the course of the relationship (Bies and Moag 1986). Trustworthiness, empathy, and propriety were considered influential in shaping a party's perceptions about interactional justice received from another party (Colquitt 2001; Martinez-Tur et al. 2006).

The notion of interactional justice is applicable to the context of information privacy in the online environment and is defined as the extent to which an Internet user perceives online companies as honest and trustworthy in their compliance with promises related to information privacy (Culnan and Bies 2003). Internet users not only focus on the benefits of disclosing their personal information (i.e., distributive justice) and the procedures enacted to safeguard against the mishandling of their information (i.e., procedural justice), but also keep their eyes open to ensure that online companies fulfill their promises associated with the benefits and procedures (Culnan and Bies 2003). In fact, given that trust in social exchange relationships is mainly concerned with honesty and fulfillment of promises (Lewicki et al. 1998), interactional justice is closely related to the fundamental concept of trust that has received considerable attention since the dawn of e-commerce (Culnan and Bies 2003). As such, earlier studies in information privacy have studied the issue of interactional justice under the rubric of trust and found that trust fosters Internet users' willingness to give personal information to online companies (Malhotra et al. 2004; McKnight et al. 2002).

Second-Order Perceived Justice and Hypotheses

The three dimensions of the perceived justice construct described above offered a conceptual foundation for understanding different, but closely interrelated, facets of the construct. We could view the three dimensions of perceived justice as three distinct factors without developing a higher-order construct; however, for the following reasons, we conceptualize the perceived justice construct as a second-order construct with the three first-order factors as its reflective indicators. Our first reason for this conceptualization is that a very high correlation is expected between the three dimensions, a result that can yield a multicollinearity problem unless a higher-order construct is developed (Bagozzi and Heatherton 1994). Because of this high level of correlation, earlier studies often combined two subconstructs, such as procedural and interactional justice, into a single factor (Mansour-Cole and Scott 1998; Skarlicki and Latham 1997). We therefore view perceived justice as a second-order construct manifested in the three first-order factors.

Second, relationships with other constructs are proposed to be the same for the three dimensions. Specifically, this study proposes that the three dimensions have the same set of outcome variables: refusal and misrepresentation. Accordingly, it seems reasonable to develop a second-order construct with first-order factors as its reflective indicators and to formulate research hypotheses at the higher-order factor level rather than at the individual subconstruct level (Jarvis et al. 2003). In addition, we will provide later in this paper empirical support for the development of the second-order construct.

Culnan and Bies (2003) recently proposed that the justice perspective offers a useful conceptual tool for analyzing Internet users' behaviors within the context of information privacy. For example, they indicated that Internet users' perceptions of the fairness of online companies—manifested in the three dimensions of distributive, procedural, and interactional justice—have important implications for their willingness to

disclose personal information to online companies. Their conceptual arguments on the relationship between justice perceptions and behavior in the disclosure of personal information have not been buttressed by empirical evidence. Nevertheless, the conceptual argument of perceived justice as fundamental to the determination of Internet users' willingness to disclose personal information is worth examining. This is especially worthwhile because perceived justice becomes particularly salient when consumers become vulnerable to opportunistic behaviors, such as in the release of personal information to an online firm (Malhotra et al. 2004). We therefore formulate the following research hypotheses that posit negative impacts of perceived justice on refusal and misrepresentation.

H2a: Justice perceptions will have a negative impact on Internet users' refusal to provide their personal information to online companies.

H2b: Justice perceptions will have a negative impact on Internet users' misrepresentation of personal information to online companies.

However, we contend that justice perceptions do *not* have strong impacts on other types of IPPR—private action and public action—that we viewed as Internet users' responses when their information privacy is seriously threatened because of online companies' mishandling of personal information rather than simply being requested to provide personal information. Our study focuses on justice perceptions developed in general from prior experiences with online companies rather than on those perceptions developed after online companies mishandle personal information. The latter may have strong impacts on Internet users' decisions to engage in private and public actions. For example, when online companies seriously mishandle personal information, Internet users would perceive that online companies do not deal justly with them, which can lead them to engage in private and public actions.

On the other hand, justice perceptions developed in general from prior experiences with online companies are not expected to have strong impacts on private and public actions because Internet users' justice perceptions will be redeveloped in situations in which online companies mishandle their personal information. That is, although Internet users develop high levels of justice perceptions in general from prior experiences with online companies, those justice perceptions cannot be sustained in situations in which the companies mishandle their personal information. This is because, like trust, which is believed to be fragile (Baier 1986; Dasgupta 1988), Internet users' justice perceptions by nature are delicate and fragile. Thus, in situations in which online companies threaten information privacy to a great extent by mishandling personal information, Internet users' preexisting justice perceptions can be easily destroyed, and they will redevelop justice perceptions. It is these newly developed justice perceptions that may influence Internet users' decision to take private and public actions.

Societal Benefits from Complaining

Not all dissatisfied customers complain to seek a remedy (Jacoby and Jaccard 1981). The literature on customer dissatisfaction has suggested that attitudes toward complaining directly predict the complaining behavior of dissatisfied customers (Oh 2003; Singh 1990). Specifically, an individual's beliefs about the societal benefits resulting from complaining have received special attention as an important dimension of attitudes toward complaining (Singh 1990). When customers are dissatisfied with products or services, they may complain directly to the seller (or service provider) and/or indirectly to a third-party organization. Such complaints may be motivated by their desire not only to seek a remedy for themselves but also by a desire to prevent others from having the same problem. Similar reasoning was offered as an explanation for why employees report wrongdoing by their employer or by a colleague to an organization or a person who can take action against the wrongdoing (also known as *whistle-blowing behavior*). One main motivation for employees to engage in whistle-blowing is to prevent others from being victimized by the same wrongdoing of their employer or colleague (Dozier and Miceli 1985).

Similarly, when online companies threaten the privacy rights of Internet users, their beliefs about the societal benefits of complaining will play a key role in determining whether they complain directly to the online companies and indirectly to third-party organizations. For instance, when an Internet user becomes a victim of secondary use of personal information, he or she may think that complaining immediately will prevent many other Internet users from experiencing the same problem. Such beliefs about the societal benefits of complaining will have a strong impact on the two specific forms of public action behaviors: complaining directly to online companies and complaining indirectly to third-party organizations.

H3a: Societal benefits resulting from complaining will have a positive impact on Internet users' complaining directly to online companies that threaten information privacy.

H3b: Societal benefits resulting from complaining will have a positive impact on Internet users' complaining indirectly to third-party organizations about online companies that threaten information privacy.

Given that the notion of societal benefits deals directly with the expected outcomes of complaining to a third-party or a company, we do not propose causal relationships from societal benefits to the other types of IPPR: refusal, misrepresentation, removal, and negative word-of-mouth. In other words, the notion of societal benefits presumes occurrences of information privacy invasion and refers to Internet users' perceptions regarding complaints about that victimization. In this sense, no well-grounded reasoning is found to propose the existence of causal relationships from Internet users' beliefs about the societal benefits associated with complaining to information privacy protective behaviors, such as information disclosure (e.g., refusal and misrepresentation) and private actions (removal and negative word-of-mouth).

Method

Scale Development

Most of the measurement scales for research constructs in this study were adapted from earlier studies in which the measurement scales were proven to be reliable and valid. Otherwise, new measures were developed by closely operationalizing the concept of research constructs. Antecedent constructs—information privacy concerns, the three dimensions of perceived justice, and societal benefits from complaining—were measured with multiple items on seven-point Likert scales, anchored with strongly disagree to strongly agree; on the other hand, the six specific forms of IPPR—refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies, and complaining indirectly to third-party organizations—were measured with multiple items on seven-point semantic scales.

The six specific forms of IPPR were assessed using an approach similar to the one taken to measure the purchase intention construct found in Mackenzie and Spreng (1992). This was accomplished by asking respondents to use three 7-point semantic differential scales to indicate their probability of engaging in each of the behaviors: very unlikely/unlikely, not probable/probable, and impossible/possible. Because our study examines the behavioral intentions of Internet users in situations containing information privacy threats, the subjects were asked to indicate the probability of engaging in IPPR if they were confronted with situations threatening their information privacy (e.g., request to provide personal information, mishandling of personal information). Since single-item measures were available in prior studies for each of the six types of IPPR (e.g., Smith et al. 1996), those measures were used to describe the different types of IPPR when the respondents were asked to provide probability.

The measurement items for information privacy concerns were directly adapted from Dinev and Hart (2006) in which the conceptualization of the construct closely matches ours. Adhering to our conceptualization of perceived justice as a second-order construct with three first-order factors, we did not directly measure the second-order construct. Instead, each of the three first-order factors—distributive, procedural, and interactional—of perceived justice was measured with multiple items either developed for this study or adapted from prior research. Distributive justice was operationalized by tightly following our conceptualization of the construct in this study. Procedural justice was also measured with multiple items developed for this study based on the two most important procedures—control and awareness—that online companies should provide Internet users as an assurance of procedural fairness (Culnan and Bies 2003). The measurement items for interactional justice were adapted from Malhotra et al. (2004) in which the trusting beliefs construct was conceptualized similar to the conceptualization of interactional justice used in this study. The societal benefits from complaining were measured with three items adapted from Singh (1990).

Several faculty members and doctoral students reviewed the initial version of the questionnaire and provided their feedback on the content validity and on the clarity of instructions. Their feedback led to several changes in item wording for the final version of the questionnaire. All measurement items are included in Appendix A.

Data Collection

Since Internet users were the target population for data collection in this study, it seemed appropriate to collect data through a Web-based online survey questionnaire. The sampling frame was drawn from panel members of a market research firm. All the panel members included in the sampling frame were Internet users from throughout the United States. We chose this approach so that our sample could better represent the general population of Internet users than was possible with other convenient samples (e.g., university students) often used in studies on information privacy. The market research firm sent an e-mail invitation to 1,500 panel

members to solicit their participation in a Web-based online survey. The e-mail invitation included a hyperlink to the online survey questionnaire, which also had a short description of the study that informed potential respondents that we were seeking their opinion about privacy in the general environment. Each panel member received a unique identification number in the e-mail invitation and was asked to provide the number when completing the survey questionnaire. The online survey ran for five days in May 2006.

We obtained 541 responses from the panel members who received the invitation, yielding a response rate of 36.1 percent. Eighteen responses were eliminated because of a large number of incomplete answers. This resulted in a dataset of 523 usable and valid responses, yielding an effective response rate of 34.9 percent. The respondents in the final sample had a median age of 41, and 53 percent of them were female. They also reported that they spent about 15 hours a week on average on the Internet and had used the Internet for 7 years. The profile of the respondents closely matched that of Internet users reported in recent studies, which led us to believe that our sample closely represents the targeted population of Internet users.[3] As recommended by Armstrong and Overton (1977), nonresponse bias was assessed by comparing early and late respondents. No significant differences between the first third and last third of all respondents were found on either the key research variables under study or on the demographic variables. These results suggest that nonresponse bias was not a serious concern in this study.

Data Analysis and Results

Structural equation modeling was chosen as a data analysis approach because of its ability to account for measurement errors for unobserved constructs and to simultaneously examine the predictive relationships among them (Rigdon 1998). Specifically, we followed the two-step approach suggested by Anderson and Gerbing (1988). As such, we first analyzed a measurement model to assess the measurement quality of constructs by using a confirmatory factor analysis (CFA) approach. Subsequently, we estimated a structural model to test the research hypotheses included in the nomological network described earlier. The AMOS program (version 6.0) was used to estimate both the measurement and structural models by analyzing the covariance matrix.

Measurement Model

An 11-factor measurement model was set up to assess the measurement quality of constructs under a CFA approach. Each item was restricted so as to load only on its prespecified factor while the factors themselves were allowed to correlate freely. Various overall fit indices indicated a reasonable fit of the model to the data because most of the indices were above or below the recommended thresholds. Fit indices of the measurement model (χ^2 (610) = 1626.0) were as follows: χ^2/df = 2.67, standardized root mean square residual [SRMR] = .039, root mean square error of approximation [RMSEA] = .056, normed fit index [NFI] = .92, comparative fit index [CFI] = .95, goodness-of-fit index [GFI] = .86, adjusted goodness-of-fit index [AGFI] = .83, Tucker-Lewis Index [TLI] = .94.[4] The means and standard deviations of the constructs are shown in Table 2, along with composite reliability (CR), average variance extracted (AVE), and correlations between them.

The measurement quality of constructs was further examined by assessing several types of psychometric properties, such as convergent and discriminant validities and reliability. First, convergent validity was assessed by comparing the item loadings with the recommended minimum value of .60 (Chin et al. 1997). The lowest item loading between an indicator and its posited underlying construct factor was greater than 0.68 (see Appendix A), adequately demonstrating convergent validity. Second, discriminant validity was assessed by comparing the square root of AVE for each construct with the correlations between the construct and other constructs (Barclay et al. 1995; Chin 1998). As shown in Table 2, the square root of the AVE (diagonal elements) was found to be larger than the correlations (off-diagonal elements) between the constructs, adequately demonstrating discriminant validity. We also assessed the discriminant validity of the constructs by comparing the original measurement model (i.e.,

[3]A study conducted in 2005 by the Center for the Digital Future at the University of South California reports that Internet users have average Internet experience of 5.3 years and spend an average of 13.3 hours a week online (Center for the Digital Future 2005). The average age of Internet users reported on Georgia Tech's WWW User Survey conducted in 1998 is 37.6 years old (GVU 1999). More recent studies indicate that the Internet is becoming increasingly popular with older people (Center for the Digital Future 2005). Studies also report that Internet users are evenly divided between men and women (Center for Communication Policy 2003; Pew Internet & American Life Project 2003).

[4]Recommended thresholds for these fit indices are as follows: below 1:3 (Gefen et al. 2000) for χ^2/df; below .05 (Gefen et al. 2000) or .08 (Hu and Bentler 1999) for SRMR; below .06 (Hu and Bentler 1999) or .08 (Byrne 1998) for RMSEA; above .90 for NFI (Gefen et al. 2000); above .95 (Hu and Bentler 1999) or .90 (Bentler 1992; Hoyle 1995) for CFI; above .90 for GFI (Gefen et al. 2000); above .80 for AGFI (Gefen et al. 2000); and above .90 for TLI (Tucker and Lewis 1973).

Table 2. Descriptive Statistics, Reliability, Average Variance Extracted, and Construct Correlation Matrix

					Correlations										
	Mean	SD	CR	AVE	1	2	3	4	5	6	7	8	9	10	11
CITO	5.97	1.41	0.97	0.92	0.96										
CDOC	6.38	1.03	0.95	0.87	0.62	0.93									
NWOM	6.49	1.06	0.97	0.92	0.38	0.37	0.96								
Removal	6.41	1.08	0.95	0.87	0.27	0.38	0.49	0.94							
Misrepresentation	2.92	1.98	0.98	0.94	-0.04	-0.05	-0.07	-0.09	0.97						
Refusal	4.67	1.65	0.94	0.85	0.15	0.13	0.24	0.19	0.18	0.92					
Societal Benefits	5.14	1.31	0.88	0.71	0.21	0.24	0.09	0.10	-0.17	-0.04	0.84				
IPC	5.82	1.26	0.93	0.78	0.27	0.28	0.27	0.28	0.02	0.33	0.14	0.88			
Interactional Justice	4.22	1.21	0.93	0.74	0.00	0.00	-0.09	-0.04	-0.15	-0.26	0.37	-0.03	0.86		
Procedural Justice	4.78	1.24	0.87	0.62	0.06	0.07	0.00	0.04	-0.14	-0.16	0.37	0.04	0.72	0.78	
Distributive Justice	3.80	1.30	0.85	0.60	0.01	-0.05	-0.11	-0.14	-0.05	-0.16	0.31	0.01	0.52	0.50	0.77

Notes:

1. SD = standard deviations, CR = composite reliability, AVE = average variance extracted
2. Diagonal elements display the square root of AVE.
3. NWOM = negative word-of-mouth, CDOC = complaining directly to online companies, CITO = complaining indirectly to third-party organizations, IPC = information privacy concerns

unconstrained measurement model) with each of constrained models in which two constructs in question were combined as one construct (Anderson and Gerbing 1988; Gefen et al. 2000). A chi-square difference test was performed to compare the unconstrained model with each of the constrained models. As reported in Appendix B, all of the chi-square difference tests were found to be significant ($p < .001$), suggesting that the unconstrained model is superior to any of the unconstrained models. That is, any pair of two constructs could not be united as one construct. Thus, discriminant validity was adequately demonstrated. Finally, scale reliability was assessed based on the composite construct reliabilities. As shown in Table 2, the minimum level of 0.85 was greater than the commonly accepted cutoff value of .70 (Gefen et al. 2000), adequately demonstrating measurement reliability for constructs.

Second-Order Factor Model

We also empirically validated our conceptualization of perceived justice as a second-order factor with three first-order factors—distributive, procedural, and interactional—as reflective indicators. As described above, the three first-order factors were found to be highly correlated with, but distinct from, each other. We therefore first set up a first-order factor model in which the three first-order factors are freely correlated with each other. Subsequently, we set up a second-order factor model in which the three first factors are viewed as reflective indicators of the second-order construct of perceived justice. As suggested by Venkatraman (1990) and Tanriverdi (2005), we introduced an external criterion variable, refusal to provide personal information, into each of the two models because the second-order factor is just identified with only three first-order factors.

Two different criteria were used in the comparison of the second-order factor model with the first-order factor model (Tanriverdi 2005). We first compared model statistics of the two models (Venkatraman 1990). Fit indices of the two models are very similar (see Table 3). Therefore, the second-order factor model is preferred over the first-order factor model because it explains more parsimoniously the covariance among the first-order factors (Tanriverdi 2005). In addition, we computed the target (T) coefficient to compare the two models (Marsh and Hocevar 1985). When the target coefficient is close to its upper bound of 1.0, the second-order factor model is preferred over the first-order factor model (Stewart and Segars 2002). A target coefficient value of 0.99, which is very close to the upper limit of 1.0, was obtained, suggesting the superiority of the second-order factor model over the first-order factor model.

Table 3. Goodness-of-Fit Indices of First and Second-Order Factor Models		
Fit Indices	**First-Order Factor Model**	**Second-Order Factor Model**
χ^2	412.7	418.7
df	98	100
χ^2/df	4.21	4.19
CFI	.95	.95
GFI	.90	.90
AGFI	.87	.87
NFI	.94	.94
TLI	.94	.94
RMSEA	.078	.078
SRMR	.053	.055

Structural Model

A structural model was set up by specifying the second order construct of perceived justice, information privacy concerns, and societal benefits as exogenous constructs; and the three first dimensions of perceived justice (distributive, procedural, and interactional) and six specific types of IPPR (refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies, and complaining indirectly to third-party organizations as endogenous constructs). All exogenous constructs are allowed to covary freely, and paths are added based on hypotheses that proposed strong relationships between constructs.[5] As in the estimation of the measurement model, various overall fit indices indicated a reasonable fit of the model to the data because most indices were above or below the recommended thresholds. Fit indices of the measurement model (χ^2 (634) = 1667.1) were as follows: χ^2/df = 2.63, SRMR = .050, RMSEA = .056, NFI = .92, CFI = .95, GFI = .85, AGFI = .83, TLI = .94.

The results of the structural model testing, including standardized path coefficients, their t-statistics and significance based on two-tailed t tests, and the amount of variances explained (R^2) are shown in Figure 3. Two-tailed t tests were used to test research hypotheses that propose strong relationships between IPPR and their major determinants. Based on the significance of the path coefficients, all of the research hypotheses except H1b were supported.

We used model comparison techniques to further examine the differential effects of antecedents on six specific types of IPPR. Two alternative models (alternative Models 1 and 2) were constructed by adding nonhypothesized paths to six specific types of IPPR from perceived justice and beliefs about societal benefits. As shown in Table 4, the results of the chi-square difference tests indicated that the additional paths in the two alternative models did not improve the model fit. To provide additional supporting evidence, we also analyzed the significance of coefficients on the nonhypothesized paths. None of the newly added paths, except for a path from societal benefits to misrepresentation, were significant. Taken together, we concluded that the theoretical research model was preferable to the competing models and that nonhypothesized effects were not present (Gefen et al. 2000).

Finally, because our data were collected through a survey questionnaire, it was possible that common method variance (CMV) affected the results of this study. Accordingly, we examined such potential biases using the marker-variable technique (Lindell and Whitney 2001; Malhotra et al. 2006). Specifically, we added a theoretically unrelated variable of fantasizing (i.e., marker variable) and examined correlations between the marker variable and other constructs in the nomological model.[6] Under the marker-variable technique, CMV is assessed based on correlation between the marker variable and research constructs in the study because they are assumed to have no relationships. The results of this analysis indicated that CMV, if any, was not substantial because the

[5]Note that the structural errors for the six types of IPPR were allowed to correlate freely; this specification was necessary to take into account potential relationships between outcomes outside the focus of this study (Fornell and Bagozzi 1983).

[6]We measured the marker variable of fantasizing with three items directly adapted from O'Guinn and Faber (1989).

Table 4. Analyses of Alternative Models

		Alternative Model 1	Alternative Model 2
Paths Added			
Causes	Effects		
Perceived Justice			
	Removal	-0.03	
	Negative word-of-mouth	-0.07	
	Complaining directly to online companies	-0.07	
	Complaining indirectly to 3rd-party organizations	-0.05	
Societal Benefits			
	Refusal		0.03
	Misrepresentation		-0.12*
	Removal		0.06
	Negative word-of-mouth		0.05
Model Comparison			
$\Delta\chi^2$		2.7	6.7
Δdf		4	4
p-value		> 0.10	> 0.10

*p < 0.05, **p < 0.01 (two-tailed)

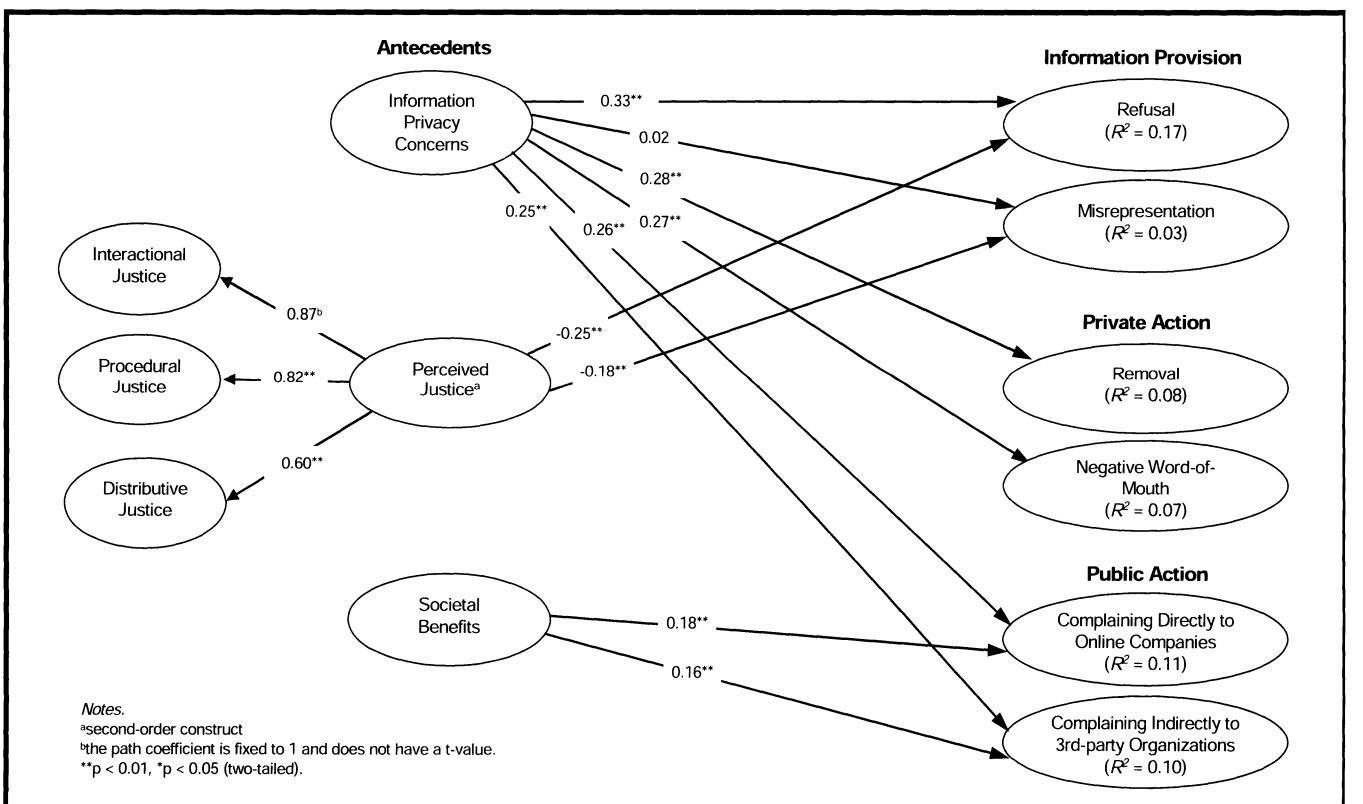

Figure 3. Estimation Results

average correlation coefficient was close to 0 ($r = 0.03$, n.s.).[7] Thus, it seems reasonable to argue that this present study is relatively robust against common method biases.

Discussion and Implications

The main purpose of this study was to advance theoretical development in the area of information privacy by developing a taxonomy of IPPR, which classifies into three categories a wide range of Internet users' responses to information privacy threats. Without a well-developed taxonomy, it is difficult to understand about how various types of Internet users' responses to information privacy threats resemble or differ from each other. Such an understanding would enhance the ability of researchers in this area to systematically accumulate research findings related to Internet users' responses to information privacy threats.

Our findings indicate that each IPPR factor generally has a stronger correlation with an IPPR factor in the same category than with a factor in the different categories, which suggests that the classification scheme of IPPR proposed in this study is quite reasonable. Next, as expected, some discernible patterns emerged in the relationships between IPPR and their antecedents; in particular, whereas privacy concerns influence all of the IPPR categories (i.e., information provision, private action, and public action), justice perceptions affect only information provision, and societal benefits determine only public actions. Taken together, this research suggests that although IPPR represents diverse types of behavioral response to information privacy threats, their similarities, differences, and variations can be understood systematically through the theoretical lens this study offers.

Theoretical Implications

Taxonomy of IPPR

Past research on information privacy in the IS domain has placed much emphasis on the conceptualization and/or operationalization of individuals' concerns for information privacy (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). However, little research attention has been paid thus far to an array of the behavioral outcomes of these concerns, that is, to customers' responses to privacy threats that stem from organizations' information practices. Even in some exceptional studies that examine IPPR, various types of IPPR have been treated collectively as a single outcome of privacy concerns (Smith et al. 1996; Stewart and Segars 2002). Thus, although shedding light on IPPR as a whole, the IS literature offers little insight into how common or unique a particular response may be in comparison with others. This lack of attention to the outcome responses is problematic because it is not mere concerns but actual responses that have direct impacts on customer–firm relationships and ultimately on a firm's overall performance.

This study provides a systematic investigation into IPPR by using a classification scheme drawn from the marketing literature on customer dissatisfaction (Day 1980; Day and Landon 1977; Singh 1988). In particular, it presents a list of possible responses and theorizes why a particular type of response is similar to and distinct from other types of responses. The findings of this study generally indicate that the proposed taxonomy is helpful in analyzing a variety of IPPR that commonly result from privacy concerns but often involve more complex formation mechanisms. Thus, we expect that the taxonomy will serve as a useful tool for the in-depth examination of Internet users' responses to information privacy threats.

Nomological Network

In an attempt to further assess the efficacy of our classification scheme, we developed and tested a nomological network. Consistent with contemporary privacy research (Dinev and Hart 2006), the proposed model, built on the belief–behavioral intention link, specifically identifies three types of salient beliefs (i.e., privacy concerns, perceived justice, and societal benefits of complaining) as the determinants of behavioral intentions (i.e., IPPR). First of all, the findings of this study suggest that individuals' privacy concerns are the major source of IPPR and that their effects on IPPR generally remain significant even after taking into account perceived justice and societal benefits. Although earlier research examined the relationships between information privacy concerns and certain types of IPPR (Malhotra et al. 2004; Sheehan and Hoy 2000; Stewart and Segars 2002), such investigations were performed in a rather *ad hoc* manner with little attention to potentially relevant determinants or outcomes. To the best of our knowledge, this study is the first to systematically show the effects of privacy concerns on a wide range of IPPR over and above other important salient beliefs.

However, unlike our expectation (H1b), privacy concerns did not have a strong impact on Internet users' intention to falsify their personal information. Although our finding might be

[7]Malhotra et al. (2006) found that, when the coefficient is less than 0.10, CMV effects are not substantial, and thus CMV is not a serious threat.

simply the outcome of random fluctuations, a plausible explanation of this finding is that the likelihood of providing falsified information is probably a function of other types of factors rather than of privacy concerns. For instance, as evidenced in our study and others (Horne et al. 2007), justice perceptions of Internet users have a strong impact on their decision to falsify their personal information. Moreover, requests to provide certain types of personal information have a strong impact on the likelihood of providing falsified information (Metzger 2007).

Drawing on the justice perspective, we show theoretically and empirically that perceived justice is the key to motivating Internet users to disclose correct personal information to online companies. Previous studies indicated that information provision acts of Internet users are known to occur only under certain conditions. Among those factors identified in the literature are expected benefits, control over personal information, and/or confidence about the other's goodwill (Dinev and Hart 2006). Although these variables have been studied as facilitating the customer–firm relationship in the context of information privacy, no theoretical framework was available to collectively explain the nature and types of factors facilitating information provision behavior. In this sense, the present study contributes to the information privacy literature by conceptualizing and operationalizing the three main components (i.e., distributive, procedural, interactional) of the justice framework within the context of information privacy. Despite the enormous potential of the justice perspective, IS researchers have rarely applied this theory to the issue of information privacy. This study is important in that it sheds light on the significance of fairness perceptions, and we hope that more privacy research will pay attention to the critical role that perceptions of fairness play in shaping consumer behavior.

Singh (1989) argued that "consumers' right to recourse and redress" constitutes one of the key characteristics of the modern trend of consumerism (p. 329). However, we do not know much about the nature of public actions in the domain of information privacy, except that to some extent they are related to privacy concerns. To fill the gap in the literature, we further examined the unique characteristics of public actions and then identified an additional predictor that is specific to public actions. As shown in the results, public actions were determined not only by privacy concerns but also by the societal benefits of complaining; however, societal benefits have little impact on other responses. To summarize, this present study contributes to the information privacy literature by showing that public action is qualitatively distinct from other categories of responses in IPPR, and thus, they should not be treated as concepts similar, or equivalent, to information provision and private action.

Managerial Implications

This study has important implications for managers whose customers may believe their privacy rights are threatened.[8] The IPPR taxonomy developed in this study alerts managers that such customers could take various actions that go beyond merely refusing to provide their personal information to online companies. For example, as shown in this study, these customers may engage in private actions such as removal and negative word-of-mouth. Customers' private actions are especially harmful to online firms because (1) removal means the immediate loss of a potentially loyal customer, and (2) word-of-mouth is known to be the key to the long-term success of businesses (Reichheld and Schefter 2000). Our study also suggests that those customers may complain directly to an online company and/or file a complaint to third-party privacy organizations, such as BBBOnline or TRUSTe, if the offending company displays a privacy seal. Further, they can file a complaint to OnGuard Online (onguardonline.gov), managed by the Federal Trade Commission or file a lawsuit. For example, several members of AOL recently sued the company over its release of data containing its members' search engine activities (Perez 2006). Such publicized privacy invasions can easily erode the reputation of online companies. It is also worth mentioning to managers that a recent study found that publicized privacy invasions had negative impacts on the market value of the violators (Acquisto et al. 2006).

Given the significant consequences of IPPR, we recommend both proactive and reactive approaches that managers could take in dealing with customers who may feel their privacy rights have been or may be threatened. A proactive approach could be undertaken to minimize the possibility that customers will engage in IPPR in response to privacy threats. On the other hand, a reactive approach could be undertaken to minimize the adverse consequences for online firms whose customers engage in IPPR. Figure 4 lists both the proactive and reactive actions with regard to IPPR that can be potentially taken by online companies.

As a proactive approach, we recommend that online firms strive to find an effective and efficient way to lessen consumers' concerns about information privacy. Our study found that privacy concerns are the trigger for most types of IPPR undertaken by Internet users. Hence, to minimize the possibility of most types of IPPR, online firms are advised to consider the three mechanisms that Luo (2002) proposed to mitigate consumers' concerns about information privacy:

[8]We are greatly indebted to the associate editor for providing valuable feedback that has considerably improved the "Managerial Implications" section.

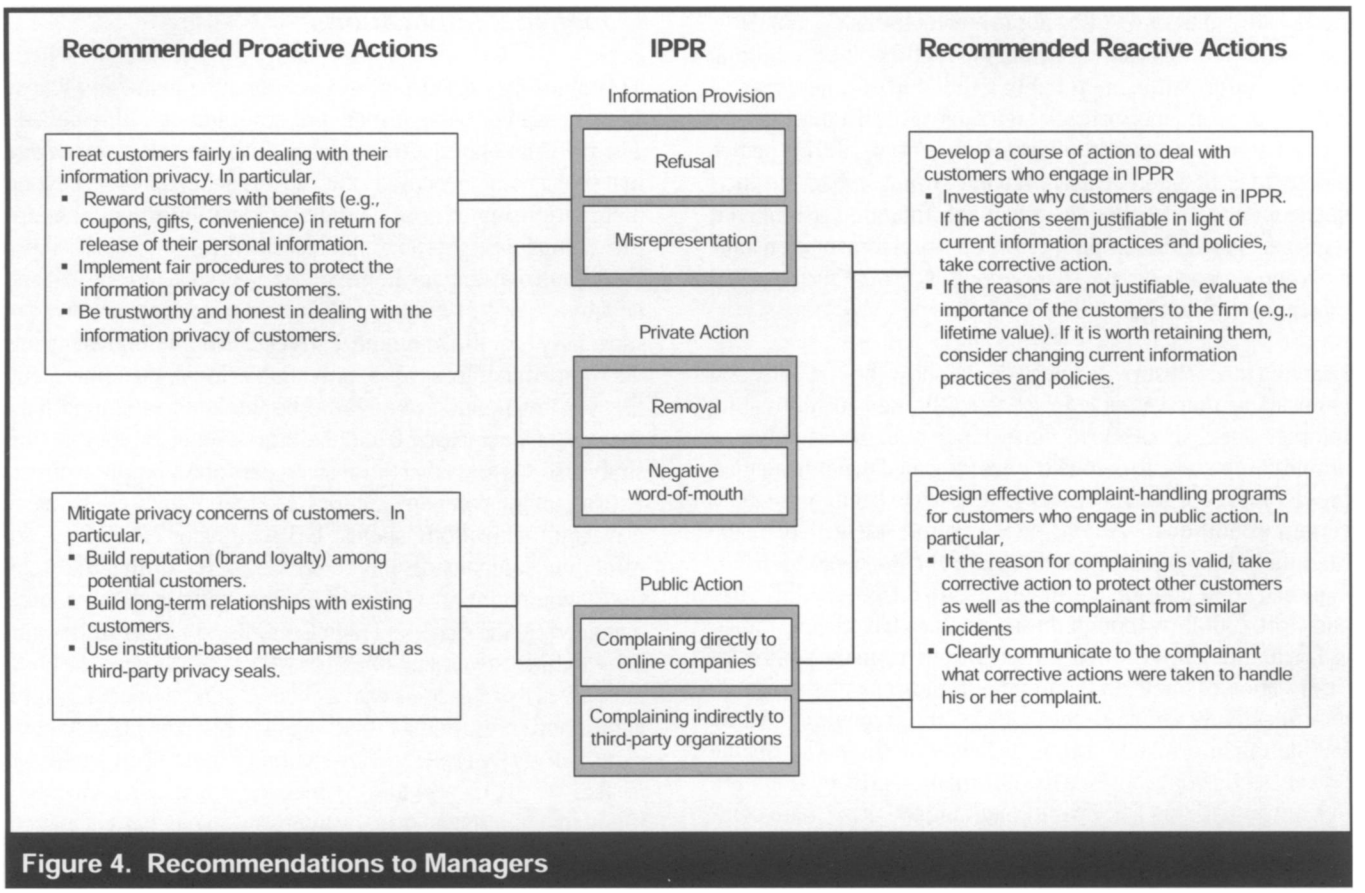

Figure 4. Recommendations to Managers

(1) a characteristic-based mechanism that centers on building "brand loyalty through the sense of e-community" (p. 114); (2) a processed-based mechanism that emphasizes repeated visits and long-lasting relationships; and (3) an institution-based mechanism that uses structural safeguards, such as third-party privacy seals.

As another proactive approach, online firms are advised to increase customers' perceptions of fairness that center on distributive, procedural, and interactional justice. Our study found that Internet users who consider themselves treated fairly by online companies respond favorably to requests for personal information. That is, justice perceptions of customers can reduce the possibility that customers will resort to two types of IPPR: refusal and misrepresentation. We recommend three specific guidelines to increase customers' perceptions of fairness. First, online firms are advised to offer customers major benefits in return for releasing personal information and to ensure that customers are aware of these benefits (i.e., distributive justice). For instance, online companies may consider offering coupons or discounts to customers who provide their personal information. In addition, online companies are advised to provide customers with other benefits such as convenience (e.g., Amazon's one-click shopping) in return for the release of personal information. Second, online firms are advised to implement fair procedures to protect the information privacy of customers and disclose these procedures (i.e., procedural justice). For instance, opt-in and opt-out procedures should be in place so that customers can have a high degree of control over how their personal information is used. Finally, online companies should be trustworthy and honest in dealing with information privacy (i.e., interactional justice). Even when online companies deliver valuable benefits to customers in return for the release of personal information and implement procedures to deal fairly with information privacy, gains in customers' perceptions of justice can quickly vanish in the wake of dishonesty or betrayal of trust.

Online companies are also advised to develop reactive approaches so that they can deal strategically with customers who engage in IPPR. As a reactive approach, we recommend that online companies establish a course of action to take when customers engage in IPPR. For instance, when a

customer engages in IPPR, online companies may need to investigate why the customer engages in IPPR, whether the customer's reasons for taking IPPR are valid, and what corrective actions, if necessary, are to be taken to rebuild a relationship with the customer. Of course, if customers do not engage in public action, it may not be a simple task for online firms to determine why customers engage in IPPR. In this regard, online companies may consider offering incentives to motivate customers to reveal why they engage in IPPR. After the companies learn why customers engage in IPPR, they also need to determine if those IPPR actions have some validity in terms of the companies' information practices and policies. If the actions are deemed unreasonable or unwarranted, the companies may not pursue corrective actions. However, even when the companies decide the customers' actions are baseless, they may nevertheless need to consider changes in their information practices and policies, especially when a number of highly valued customers engage in IPPR for reasons similar to those initially rejected by the companies.

Another reactive approach we recommend is that online companies establish effective complaint handling programs for customers who engage in public action. Our study reveals that potential benefits to other users are a major motivation for complaints by Internet users to online companies or to third-party organizations. This finding can steer online companies toward designing effective programs to handle complaints. To satisfy an Internet user who complains about a privacy violation, an online company should take corrective steps to protect not only the complainant but also other customers from similar future violations. In doing so, it is particularly critical to clearly communicate to the complainant that corrective actions were taken to handle his or her complaint and that these actions will benefit other customers as well. Otherwise, an Internet user disposed to consider societal benefits important will be dissatisfied with how a company handles the complaint and will not return to the company.

Further Research Suggestions

This study opens up several exciting avenues for further research. One interesting direction for research is to extend this study by exploring the determinants of the antecedents of IPPR. We believe that the antecedents of IPPR identified in this study act as the mediators between the deeper-seated determinants and IPPR. Thus, from the theoretical perspective, it is important to identify the causal determinants of the mediators (i.e., information privacy concerns, perceived justice, and societal benefits from complaining). Such causal determinants include not only personal characteristics and experiences but also organizations' information practices and website designs. From a managerial perspective, this type of an investigation has significant implications in that practitioners can gain concrete, actionable ideas that help to lessen customers' overly defensive responses that easily jeopardize the (otherwise mutually beneficial) customer–firm exchange relationship. We believe that this "upstream" research on information privacy will be nicely complemented with our current downstream research.

Another avenue for future research is to further examine the similarities and differences of the factors within the same IPPR category. For example, our findings imply that refusal and misrepresentation are rather distinct, even though the two factors are classified under the same category of information provision. Specifically, unlike refusal that is influenced by information privacy concerns and by perceived justice, misrepresentation is determined by perceived justice but not by information privacy concerns. In any case, IPPR are likely to exhibit different patterns even under the same category, and therefore, future research should attempt to gain a more in-depth understanding of IPPR.

In addition, it would be worthwhile for researchers to investigate how online companies can properly handle privacy-related complaint behaviors, such as when complaints are addressed directly to online companies or taken indirectly to third-party organizations, and whether proper handling of such complaints would favorably dispose the customers to the information practices of the companies. Earlier studies have found that firms are able to turn dissatisfied customers into satisfied ones through proper complaint management (Maxham and Netemeyer 2002). Furthermore, consumers often paid attention to a company's handling of complaints from other customers, and their perception of how the complaints were handled influenced the creation of their trust in the company (Lee and Lee 2006). In light of these findings, it is worth investigating within the context of information privacy how complaints are managed and how these management practices affect customers.

Limitations of the Study

Several limitations of this study deserve consideration. One limitation relates to our use of intentional variables to examine IPPR. Although behavioral intention on its own—as the mediator between the antecedents and actual behavior—is of interest to researchers and in many information privacy studies is often treated as a good proxy for actual behavior (Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002), the study of behavioral intention will be more meaningful when intention replicates actual behavior. In this

regard, Singh (1988) demonstrated that customers' complaint intentions reasonably reflect complaint behaviors. Thus, although it seems reasonable to expect that information privacy-protective intentions generally determine actual behaviors, the findings of this study should be interpreted with caution until such evidence is provided.

Second, it is worth noting that the nomological network presented in this study was primarily designed to show the validity of the taxonomy of IPPR, not to explain variations in types of IPPR. Thus, we chose only three antecedent variables that can satisfactorily show discernible patterns in their relationships with types of IPPR. As such, the levels of R^2 for some types of IPPR were not high. Many more variables could exist as antecedents to explain variations in types of IPPR. To better understand the formation of IPPR, future research should examine a more comprehensive set of antecedents by incorporating other potentially important predictors (e.g., personal characteristics, situation-specific variables, etc.).

Third, it should be noted that this research examines IPPR only in a general context (i.e., a context that is not specific to a particular exchange situation). For a better understanding of Internet users' behaviors, research should take into account as many "episode-specific measures" as practicable (Singh 1990). For example, Malhotra et al. (2004) differentiated between the two types of information requested by a marketer (i.e., sensitive and insensitive information) to take an in-depth look at Internet users' willingness to release the requested information. In addition to type of information, episode-specific measures may also include experience with a marketer, cost/benefit evaluations, presence/proximity of third-party organizations, etc. The present study focuses on the conceptualization of IPPR as a whole; inevitably, less attention has been paid to such episode-specific measures. Yet, future research will be able to explain more variations (R^2) in IPPR by additionally controlling for various episode-specific variables.

Finally, in this study the conceptualization and operationalization of all research variables were made at a general level (i.e., online companies in general) rather than at a specific level (a certain company in particular). For example, we examined whether perceptions of justice that were formed based on one's experiences with online companies in general could influence willingness to provide personal information to online companies in general. This approach is often found in the literature on information privacy (Dinev and Hart 2006; Malhotra et al. 2004; Stewart and Segars 2002). However, it is reasonable to expect that, when faced with information privacy threats from a specific online company, an Internet user is likely to engage in certain forms of IPPR mainly based on his or her experiences with this specific company. Accordingly, until our study is replicated at the level of an online firm, it remains to be seen whether our model presented here can be applied to the setting specific to a particular firm. In this regard, a recent study by Van Slyke et al. (2006) empirically demonstrated that research findings related to information privacy at a general level would hold up well even at a specific setting. Although Van Slyke et al.'s study suggests that the applicability of our findings is not necessarily limited to the setting examined in the present study, caution should be taken nevertheless in generalizing such findings to the context of a specific online firm.

Conclusion

Organizations' information practices should be carefully planned and implemented only after thoughtful consideration of customers' potential responses to such organizational practices. Despite the importance of understanding individuals' *reactions* to information privacy threats, extant research has focused mostly on their *concerns* that were not yet manifested in the form of IPPR. Without a systematic, holistic approach to the study of the outcome responses, our ability to comprehend a customer–firm relationship in the context of information privacy will be severely limited. To shed light on this important yet underexplored issue, we attempted to offer a theoretical framework that categorizes a variety of information privacy-protective responses and their differential relationships with their antecedents. In general, our taxonomy and nomological networks are shown to be useful in understanding how the various responses are manifested as a way for consumers to protect the privacy of their information. We hope that more research on the phenomena will extend beyond mere privacy concerns and that our theoretical framework will be found helpful for such research endeavors.

Acknowledgments

The authors would like to thank Professor Bernard Tan (senior editor), the associate editor, and the three anonymous reviewers for their constructive comments and suggestions that helped improve the quality of the paper significantly. This research was partially supported by the Social Sciences and Humanities Research Council of Canada. The authors also thank J. Stanford Fisher for his editorial help.

References

Acquisto, A., Friedman, A., and Telang, R. 2006. "Is There a Cost to Privacy Breaches? An Event Study," in *Proceedings of the 27th International Conference on Information Systems*, Milwaukee, WI, pp. 1563-1580.

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

Alge, B. J. 2001. "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice," *Journal of Applied Psychology* (86:4), pp. 797-804.

Anderson, J. C., and Gerbing, D. W. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach," *Psychological Bulletin* (103:3), pp. 411-423.

Armstrong, J. S., and Overton, T. S. 1977. "Estimating Nonresponse Bias in Mail Surveys," *Journal of Marketing Research* (14:3), pp. 396-402.

Bagozzi, R. P., and Heatherton, T. F. 1994. "A General Approach to Representing Multifaceted Personality Constructs: Application to State Self-Esteem," *Structural Equation Modeling* (1:1), pp. 35-67.

Baier, A. 1986. "Trust and Antitrust," *Ethics* (96:2), pp. 231-260.

Barclay, D., Higgins, C. A., and Thompson, R. L. 1995. "The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2:2), pp. 285-309.

Benassi, P. 1999. "Truste: An Online Privacy Seal Program," *Communications of the ACM* (42:2), pp. 56-59.

Bentler, P. M. 1992. "On the Fit of Models to Covariances and Methodology to the Bulletin," *Psychological Bulletin* (112:3), pp. 400-404.

Bettencourt, L. A., Brown, S. W., and MacKenzie, S. B. 2005. "Customer-Oriented Boundary-Spanning Behaviors: Test of a Social Exchange Model of Antecedents," *Journal of Retailing* (81:2), pp. 141-157.

Bies, R. J. 1993. "Privacy and Procedural Justice in Organizations," *Social Justice Research* (6:1), pp. 69-86.

Bies, R. J., and Moag, J. F. 1986. "Interactional Justice: Communication Criteria of Fairness," in *Research on Negotiations in Organizations,* R. J. Lewicki, B. H. Sheppard, and M. H. Bazerman (eds.), Greenwich, CT: JAI Press, pp. 43-55.

Brown, S. W., and Swartz, T. A. 1984. "Consumer Medical Complaint Behavior: Determinants of and Alternatives to Malpractice Litigation," *Journal of Public Policy and Marketing* (3:1), pp. 85-98.

BusinessWeek. 2000. "Business Week/Harris Pool: A Growing Threat," March 20 (available at http://businessweek.com/2000/00_12/b3673010.htm).

Byrne, B. M. 1998. *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS: Basic Concepts, Applications, and Programming*, Mahwah, NJ: Lawrence Erlbaum Associates.

Cavoukian, A., and Hamilton, T. 2002. *The Privacy Payoff: How Successful Businesses Build Customer Trust*, Toronto: McGraw-Hill Ryerson Limited.

Center for the Digital Future. 2005. Highlights from the report, "Year Four of the Digital Future Project," University of Southern California Annenberg School, Los Angeles, December 7 (available at http://www.digitalcenter.org/pdf/Center-for-the-Digital-Future-2005-Highlights.pdf).

Center for Communication Policy. 2003. "The UCLA Internet Report: Surveying the Digital Future: Year Three," University of California, Los Angeles, February (available at http://www.digitalcenter.org/pdf/InternetReportYearThree.pdf).

Chin, W. W. "The Partial Least Squares Approach to Structural Equation Modeling," in *Modern Methods for Business Research,* G. A. Marcoulides (ed.), Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295-336.

Chin, W. W., Gopal, A., and Salisbury, W. D. 1997. "Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation," *Information Systems Research* (8:4), pp. 342-367.

Cialdini, R. B. 1993. *Influence: Science and Practice*, New York: HarperCollins.

CNET News. 2004. "Privacy in the Age of Transparency," March 14 (available at http://news.com.com/2030-1069_2033-5172731.html).

Colquitt, J. A. 2001. "On the Dimensionality of Organizational Justice: A Construct Validation of a Measure," *Journal of Applied Psychology* (86:3), pp. 386-400.

Cronbach, L. S., and Meehl, P. 1955. "Construct Validity in Psychological Tests," *Psychological Bulletin* (52:4), pp. 281-302.

Culnan, M. J. 1995. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* (9), pp. 10-15.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323-342.

Dasgupta, P. 1988. "Trust as a Commodity," in *Trust: Making and Breaking Cooperative Relations,* D. Gambetta (ed.), New York: Blackwell, pp. 47-72.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319-340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1989. "User Acceptance of Computer-Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), pp. 982-1003.

Day, R. 1980. "Research Perspectives on Consumer Complaining Behavior," in *Theoretical Developments in Marketing,* C. W. Lamb and P. M. Dunne (eds.), Chicago: American Marketing Association, pp. 211-215.

Day, R., and Landon, E. J. 1977. "Toward a Theory of Consumer Complaining Behavior," in *Consumer and Industrial Buying Behavior,* A. G. Woodside, J. N. Sheth, and P. D. Bennett (eds.), Amsterdam: North Holland Publishing Co., pp. 425-437.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Dozier, J. B., and Miceli, M. P. 1985. "Potential Predictors of Whistle-Blowing: A Pro-Social Behavior Perspective," *Academy of Management Review* (10:4), pp. 823-836.

Eddy, E. R., Stone, D. L., and Stone-Romero, E. F. 1999. "The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology* (52:3), pp. 335-358.

Fornell, C., and Bagozzi, R. P. 1983. "Issues in the Application of Covariance Structure Analysis: Comments," *Journal of Consumer Research* (9:4), pp. 443-450.

Foxman, E. R., and Kilcoyne, P. 1993. "Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues," *Journal of Public Policy and Marketing* (12:1), pp. 106-119.

Gefen, D., Straub, D., and Boudreau, M. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:7), pp. 1-77.

Germain, J. M. 2005. "Internet Marketing, Privacy Survey Finds Relevancy the Key," *E-Commerce Times*, February 1 (available at http://www.macnewsworld.com/story/40146.html).

GVU. 1999. Tenth WWW User Survey. Graphic, Visualization & Usability Center, Georgia Institute of Technology, Atlanta, GA (available at http://www-static.cc.gatech.edu/gvu/user_surveys/survey-1998-10/reports/1998-10-General.html).

Hoffman, D. L., Novak, T. P., and Peralta, M. A. 1999. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2), pp. 129-139.

Homans, G. C. 1961. *Social Behavior: Its Elementary Forms*, New York: Hartcourt, Brace & World.

Horne, D. R., Norberg, P. A., and Ekin, A. C. 2007. "Exploring Consumer Lying in Information-based Exchanges," *Journal of Consumer Marketing* (24:2), pp. 90-99.

Hoyle, R. H. 1995. *Structural Equation Modeling. Concepts, Issues, and Applications*, Thousand Oaks, CA: Sage Publications.

Hu, L.-T., and Bentler, P. M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," *Structural Equation Modeling* (6:1), pp. 1-55.

Hui, K. L., Teo, H. H., and Lee, S. Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp. 19-33.

Jacoby, J., and Jaccard, J. J. 1981. "The Sources, Meaning, and Validity of Consumer Complaint Behavior: A Psychological Analysis," *Journal of Retailing* (57:3), pp. 4-24.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *Journal of Consumer Research* (30:2), pp. 199-218.

Kelley, S. W., Hoffman, K. D., and Davis, M. A. 1993. "A Typology of Retail Failures and Recoveries," *Journal of Retailing* (69:4), pp. 429-452.

Kumar, N., Scheer, L. K., and Steenkamp, J. 1995. "The Effects of Supplier Fairness on Vulnerable Resellers," *Journal of Marketing Research* (32:1), pp. 54-65.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Lee, S. J., and Lee, Z. 2006. "An Experimental Study of Online Complaint Management in the Online Feedback Forum," *Journal of Organizational Computing and Electronic Commerce* (16:1), pp. 65-85.

Lewicki, R. J., McAllister, D. J., and Bies, R. J. 1998. "Trust and Distrust: New Relationships and Realities," *Academy of Management Review* (23:3), pp. 438-458.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.

Luo, X. M. 2002. "Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory," *Industrial Marketing Management* (31:2), pp. 111-118.

Lwin, M. O., and Williams, J. D. 2003. "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online," *Marketing Letters* (14:4), pp. 257-272.

Mackenzie, S. B., and Spreng, R. A. 1992. "How Does Motivation Moderate the Impact of Central and Peripheral Processing on Brand Attitudes and Intentions," *Journal of Consumer Research* (18:4), pp. 519-529.

Malhotra, N., Kim, S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Malhotra, N., Kim, S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp. 1865-1883.

Mansour-Cole, D. M., and Scott, S. G. 1998. "Hearing It through the Grapevine: The Influence of Source, Leader-Relations and Legitimacy on Survivors' Fairness Perceptions," *Personnel Psychology* (51:1), pp. 25-54.

Marsh, H. W., and Hocevar, D. 1985. "Application of Confirmatory Factor Analysis to the Study of Self-Concept: First- and Higher-Order Factor Models and Their Invariance across Groups," *Psychological Bulletin* (97:3), pp. 562-582.

Martinez-Tur, V., Peiro, J. M., Ramos, J., and Moliner, C. 2006. "Justice Perceptions as Predictors of Customer Satisfaction: The Impact of Distributive, Procedural, and Interactional Justice," *Journal of Applied Social Psychology* (36:1), pp. 100-119.

Maxham, J. G., and Netemeyer, R. G. 2002. "Modeling Customer Perceptions of Complaint Handling over Time: The Effects of Perceived Justice on Satisfaction and Intent," *Journal of Retailing* (78:4), pp. 239-252.

McFarlin, D. B., and Sweeney, P. D. 1992. "Distributive and Procedural Justice as Predictors of Satisfaction with Personal and Organizational Outcomes," *Academy of Management Journal* (35:3), pp. 626-637.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), pp. 334-359.

Metzger, M. J. 2007. "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication* (12), pp. 335-361.

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 and Marketing* (19:1), pp. 1-6.

Milne, G. R., and Boza, M. 1999. "Trust and Concerns in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1), pp. 5-24.

Milne, G. R., Rohm, A. J., and Bahl, S. 2004. "Consumers' Protection of Online Privacy and Identity," *Journal of Consumer Affairs* (38:2), pp. 217-232.

O'Guinn, T. C., and Faber, R. J. 1989. "Compulsive Buying: A Phenomenological Exploration," *Journal of Consumer Research* (16:2), pp. 147-157.

Oh, D. G. 2003. "Complaining Behavior of Public Library Users in South Korea," *Library & Information Science Research* (25:1), pp. 43-62.

Oliver, R. L. 1993. "Cognitive, Affective, and Attribute Bases of the Satisfaction Response," *Journal of Consumer Research* (20:3), pp. 418-430.

Perez, J. C. 2006. "AOL Members Sue over Search Data Release," *Computerworld*, September 26 (available at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003619).

Pew Internet and American Life Project. 2003. "Internet Use by Region in the United States," Pew Internet & American Life Project, Washington, DC, August 27 (available at http://www.pewinternet.org/pdfs/PIP_Regional_Report_Aug_2003.pdf).

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp. 27-41.

Rahim, M. A., Magner, N. R., and Shapiro, D. L. 2000. "Do Justice Perceptions Influence Styles of Handling Conflict with Supervisors? What Justice Perceptions, Precisely?," *International Journal of Conflict Management* (11:1), pp. 9-31.

Reichheld, F. F., and Schefter, P. 2000. "E-Loyalty: Your Secret Weapon on the Web," *Harvard Business Review* (78:4), pp. 105-113.

Resnick, P., Zeckhauser, R., Friedman, E., and Kuwabara, K. 2000. "Reputation Systems," *Communications of the ACM* (43:12), pp. 45-48.

Rigdon, E. 1998. "Structural Equation Modeling," in *Modern Methods for Business Research*, G. A. Marcoulides (ed.), Mahwah, NJ: Lawrence Erlbaum Associates, pp. 251-294.

Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy and Marketing* (19:1), pp. 62-73.

Singh, J. 1988. "Consumer Complaint Intentions and Behavior: Definitional and Taxonomical Issues," *Journal of Marketing* (52:1), pp. 93-107.

Singh, J. 1989. "Determinants of Consumers Decisions to Seek Third Party Redress: An Empirical Study of Dissatisfied Patients," *Journal of Consumer Affairs* (23:2), pp. 329-363.

Singh, J. 1990. "A Typology of Consumer Dissatisfaction Response Styles," *Journal of Retailing* (66:1), pp. 57-99.

Skarlicki, D. P., and Latham, G. P. 1997. "Leadership Training in Organizational Justice to Increase Citizenship Behavior Within a Labor Union: A Replication," *Personnel Psychology* (50:3), pp. 617-633.

Smith, H. J., Milburg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167-196.

Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.

Stone, E. F., Gardner, D. G., Gueutal, H. G., and McClure, S. 1983. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations," *Journal of Applied Psychology* (68:3), pp. 459-468.

Tam, E., Hui, K., and Tan, B. C. Y. 2002. "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses," in *Proceedings of the 23rd International Conference on Information Systems*, L. Applegate, R. Galliers, and J. I. DeGross (eds.), Barcelona, Spain, pp. 11-21.

Tanriverdi, H. 2005. "Information Technology Relatedness, Knowledge Management Capability, and Performance of Multibusiness Firms," *MIS Quarterly* (29:2), pp. 311-334.

Teo, H. H., Wan, W., and Li, L. 2004. "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Initiatives, and Reward on Online Consumer Behavior," in *Proceedings of the 37th Hawaii International Conferences on Systems Sciences*, Los Alamitos, CA: IEEE Computer Society Press, pp. 1-10.

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

Truman, G. E. 2000. "Integration in Electronic Exchange Environments," *Journal of Management Information Systems* (17:1), pp. 209-244.

Tucker, L. R., and Lewis, C. 1973. "Reliability Coefficient for Maximum Likelihood Factor Analysis," *Psychometrika* (38:1), pp. 1-10.

Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. 2006. "Concern for Information Privacy," *Journal of the Association for Information Systems* (7:6), pp. 415-444.

Venkatraman, N. 1990. "Performance Implications of Strategic Coalignment: A Methodological Perspective," *Journal of Management Studies* (27:1), pp. 19-41.

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

Zweig, D., and Webster, J. 2002. "Where Is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23:5), pp. 605-633.

About the Authors

Jai-Yeol Son is an associate professor of Information Systems at Yonsei University, Seoul, Korea. His research focuses on business-to-business electronic commerce, organizational adoption of IT, and individual acceptance of B2C electronic commerce. His research has appeared (or will appear) in *MIS Quarterly*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, and *Communications of the Association for Information Systems*. He received his Ph.D. in Information Technology Management from Georgia Tech.

Sung S. Kim is an associate professor of operations and information management at the University of Wisconsin, Madison. He holds a B.S. in electronic engineering from Yonsei University, Seoul, Korea, an M.S. in information systems from the University of Wisconsin, Madison, and a Ph.D. from Georgia Tech in information technology management with a minor in industrial and systems engineering. His research has been published in *Management Science*, *Information Systems Research*, *Journal of the Association for Information Systems*, and *Decision Sciences*. His primary research focuses on automaticity in IT use, online consumer behavior, information privacy, and philosophical and methodological issues in IS research.

Appendix A

Measurement Items and Standardized Item Loadings

Internet Privacy Concerns: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Dinev and Hart 2006)
1. I am concerned that the information I submit to online companies could be misused.
2. I am concerned that a person can find private information about me on the Internet.
3. I am concerned about providing personal information to online companies, because of what others might do with it.
4. I am concerned about providing personal information to online companies, because it could be used in a way I did not foresee.

Standardized item loadings: 0.86[(n/a)], 0.83***, 0.93***, 0.91***

Distributive Justice: Seven-point scales anchored with "strongly disagree" and "strongly agree" (developed for this study)
1. Online companies that have my personal information provide better value than those without holding my personal information.
2. The level of service from online companies that use my personal information is superior to the service from companies that do not use my personal information.
3. What I give up in terms of releasing my personal information to online companies is commensurate with what I receive in return from the companies.
4. Given the potential problem of releasing my personal information to online companies, the benefits I receive from the companies are fair.

Standardized item loadings: 0.83[(n/a)], 0.84***, 0.72***, 0.68***

Procedural Justice: Seven-point scales anchored with "strongly disagree" and "strongly agree" (developed for this study)
1. Online companies make a reasonable effort to clearly reveal how personal information is collected and used.
2. Online companies make a reasonable effort to get consent before they collect sensitive personal information from online consumers.
3. Online companies make a reasonable effort to allow their customers to correct inaccurate personal information stored in their databases.
4. Online companies make a reasonable effort to prevent unauthorized access to personal information stored in their databases.

Standardized item loadings: 0.80[(n/a)], 0.82***, 0.72***, 0.80***

Interactional Justice: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Malhotra et al. 2004)
1. Online companies tell the truth related to the collection and use of the personal information of their customers.
2. Online companies are honest with customers when it comes to collecting and using the personal information of their customers.
3. Online companies fulfill their promises about collecting and using personal information of their customers.
4. Online companies are in general predictable and consistent regarding the usage of the personal information of their customers.
5. Online companies are trustworthy in handling the personal information of their customers.

Standardized item loadings: 0.89[(n/a)], 0.93***, 0.89***, 0.73***, 0.86***

Societal Benefits: Seven-point scales anchored with "strongly disagree" and "strongly agree" (Singh 1990)
1. By making complaints about unsatisfactory services, in the long run the quality of services will improve.
2. By complaining about bad services, I may prevent other consumers from experiencing the same problem.
3. People have a responsibility to tell companies when a service they receive is unsatisfactory.

Standardized item loadings: 0.75[(n/a)], 0.92***, 0.86***

Refusal: Seven-point semantic scales (Smith et al. 1996)
Please specify the extent to which you would refuse to give information to online companies because you think it is too personal within the next three years.
1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.91[(n/a)], 0.98***, 0.86***

Misrepresentation: Seven-point semantic scales (Malhotra et al. 2004)
Please specify the extent to which you would falsify some of your personal information if it is asked for by online companies within the next three years.
1. Very unlikely/very likely

2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.99(n/a), 0.95***, 0.97***

Removal: Seven-point semantic scales (Smith et al. 1996)

Please specify the extent to which you would take actions to have your information removed from online companies' database when your personal information was not properly handled.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.91(n/a), 0.93***, 0.96***

Negative Word-of-Mouth: Seven-point semantic scales (Singh 1988)

Please specify the extent to which you would speak to your friends and/or relatives about your bad experience with online companies' mishandling personal information when your personal information was not properly handled.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.96(n/a), 0.98***, 0.93***

Complaining Directly to Online Companies: Seven-point semantic scales (Smith et al. 1996)

Please specify the extent to which you would write or call online companies to complain about the way they use personal information when your personal information was not properly handled.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.94(n/a), 0.93***, 0.92***

Complaining Indirectly to Third-Party Organizations: Seven-point semantic scales (Smith et al. 1996)

Please specify the extent to which you would write or call an elected official or consumer organization to complain about the way online companies use personal information when your personal information was not properly handled.

1. Very unlikely/very likely
2. Not probable/probable
3. Impossible/possible

Standardized item loadings: 0.92(n/a), 0.99***, 0.93***

Notes: ***p < .001

The first item loading in each construct does not have a t-value because it is fixed to 1.00.

Appendix B

Pairwise Discriminant Validity Analyses

Two Factor Combinations for Constrained Measurement Models	χ^2	df	χ^2 Difference
Complaining Indirectly to Third-Party Organizations with			
Complaining Directly to Online Companies	2781.9	611	1155.9***
Negative Word-of-Mouth	3662.0	611	2036.0***
Removal	3217.1	611	1591.1***
Misrepresentation	4019.6	611	2393.6***
Refusal	3101.2	611	1475.2***
Societal Benefits	2445.1	611	819.1***
Information Privacy Concerns	3732.8	611	2106.8***
Interactional Justice	3795.6	611	2169.6***
Procedural Justice	2571.4	611	945.4***
Distributive Justice	2491.5	611	865.5***
Complaining Directly to Online Companies with			
Negative Word-of-Mouth	3072.8	611	1446.8***
Removal	3062.7	611	1436.7***
Misrepresentation	4020.4	611	2394.4***
Refusal	3103.8	611	1477.8***
Societal Benefits	2423.8	611	797.8***
Information Privacy Concerns	3128.1	611	1502.1***
Interactional Justice	3193.4	611	1567.4***
Procedural Justice	2570.5	611	944.5***
Distributive Justice	2493.0	611	867.0***
Negative Word-of-Mouth with			
Removal	3041.5	611	1415.5***
Misrepresentation	4014.8	611	2388.8***
Refusal	3065.7	611	1439.7***
Societal Benefits	2469.3	611	843.3***
Information Privacy Concerns	3711.7	611	2085.7***
Interactional Justice	3780.9	611	2154.9***
Procedural Justice	2573.3	611	947.3***
Distributive Justice	3774.9	611	2148.9***
Removal with			
Misrepresentation	4010.9	611	2384.9***
Refusal	3082.2	611	1456.2***
Societal Benefits	2469.0	611	843.0***
Information Privacy Concerns	3199.4	611	1573.4***
Interactional Justice	3283.4	611	1657.4***
Procedural Justice	2572.4	611	946.4***
Distributive Justice	3259.9	611	1633.9***

Two Factor Combinations for Constrained Measurement Models	χ^2	df	χ^2 Difference
Misrepresentation with			
Refusal	3087.9	611	1461.9***
Societal Benefits	2460.3	611	834.3***
Information Privacy Concerns	4018.5	611	2392.5***
Interactional Justice	3994.5	611	2368.5***
Procedural Justice	3991.9	611	2365.9***
Distributive Justice	4015.8	611	2389.8***
Refusal with			
Societal Benefits	2480.6	611	854.6***
Information Privacy Concerns	3008.0	611	1382.0***
Interactional Justice	3056.1	611	1430.1***
Procedural Justice	3126.9	611	1500.9***
Distributive Justice	3095.0	611	1469.0***
Societal Benefits with			
Information Privacy Concerns	2463.5	611	837.5***
Interactional Justice	2387.4	611	761.4***
Procedural Justice	2365.6	611	739.6***
Distributive Justice	2409.0	611	783.0***
Information Privacy Concerns with			
Interactional Justice	3379.5	611	1753.5***
Procedural Justice	2572.4	611	946.4***
Distributive Justice	2492.2	611	866.2***
Interactional Justice with			
Procedural Justice	2042.9	611	416.9***
Distributive Justice	2219.1	611	593.1***
Procedural Justice with			
Distributive Justice	2165.9	611	539.9***

Notes:
1. The unconstrained measurement model: $\chi^2(610) = 1626.0$
2. ***$p \leq .001$