Journal of the Association for Information Systems
JAIS

Research Article

Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances

Heng Xu
The Pennsylvania State University
hxu@ist.psu.edu

Tamara Dinev
Florida Atlantic University
tdinev@fau.edu

Jeff Smith
Miami University
jeff.smith@muohio.edu

Paul Hart
Florida Atlantic University
hart@fau.edu

Abstract

Organizational information practices can result in a variety of privacy problems that can increase consumers' concerns for information privacy. To explore the link between individuals and organizations regarding privacy, we study how institutional privacy assurances such as privacy policies and industry self-regulation can contribute to reducing individual privacy concerns. Drawing on Communication Privacy Management (CPM) theory, we develop a research model suggesting that an individual's privacy concerns form through a cognitive process involving perceived privacy risk, privacy control, and his or her disposition to value privacy. Furthermore, individuals' perceptions of institutional privacy assurances -- namely, perceived effectiveness of privacy policies and perceived effectiveness of industry privacy self-regulation -- are posited to affect the risk-control assessment from information disclosure, thus, being an essential component of privacy concerns. We empirically tested the research model through a survey that was administered to 823 users of four different types of websites: 1) electronic commerce sites, 2) social networking sites, 3) financial sites, and 4) healthcare sites. The results provide support for the majority of the hypothesized relationships. The study reported here is novel to the extent that existing empirical research has not explored the link between individuals' privacy perceptions and institutional privacy assurances. We discuss implications for theory and practice and provide suggestions for future research.

Keywords: *Information Privacy Concerns, Institutional Privacy Assurance, Communication Privacy Management (CPM) Theory, Questionnaire Surveys.*

* Ping Zhang was the accepting senior editor. This article was submitted on 10th February 2010 and went through two revisions.

Volume 12, Issue 12, pp. 798-824, December 2011

1. Introduction

The importance of privacy in contemporary globalized information societies has been widely discussed and is undisputed. It has been 30 years since Laufer and Wolfe (1977) observed that "[i]f we are to understand privacy as a future as well as contemporary issue, we must understand privacy as a concept" (p. 22). Numerous studies in diverse fields have improved our understanding of privacy and privacy management at different levels. However, the picture that emerges is fragmented and usually discipline-specific, with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated. The definitions of privacy vary and depend on the field, ranging from a "right" or "entitlement" in law (e.g., Warren & Brandeis, 1890) to a "state of limited access or isolation" in philosophy and psychology (e.g., Schoeman, 1984) to "control" in social sciences and information systems (Culnan, 1993; Westin, 1967). The wide scope of scholarly interests has resulted in a variety of conceptualizations of privacy, which leads Margulis (1977) to note that "theorists do not agree...on what privacy is or on whether privacy is a behavior, attitude, process, goal, phenomenal state, or what" (p. 17). Privacy has been described as multidimensional, elastic, depending upon context, and dynamic in the sense that it varies with life experience (Altman, 1977; Laufer & Wolfe, 1977). Overlapping cognate concepts such as confidentiality, secrecy, and anonymity have added to the confusion (Margulis, 2003a, 2003b). Therefore, Solove (2006) is not alone (see also Bennett, 1992) in his conclusion that "[p]rivacy as a concept is in disarray. Nobody can articulate what it means" (p. 477).

This prior body of conceptual work has led to efforts to synthesize various perspectives and identify common ground. Toward this end, Solove (2006) developed a taxonomy of information practices and activities, which maps out various types of problems and harms that constitute privacy violations. He does not define privacy, but describes privacy as "a shorthand umbrella term" (Solove, 2007, p.760) for a related web of privacy problems resulting from information collection, processing, dissemination, and invasion activities. Culnan and Williams (2009) argue that these organizational information practices "can potentially threaten an individual's ability to maintain a condition of limited access to his/her personal information" (p.675). According to Solove (2007), the purpose of conceptualizing privacy through advancing such taxonomy of information practices is to "shift away from the rather vague label of *privacy* in order to prevent distinct harms and problems from being conflated or not recognized" (p.759).

Solove's (2007) groundwork for a pluralistic conception of privacy suggests that organizational information practices (or poor organizational privacy programs) can result in a variety of privacy problems that can associate with consumers' concerns for information privacy. However, research examining information practices through an organizational lens is underrepresented in the privacy literature, which is dominated by consumer studies focusing on individual actions (Smith, Dinev, & Xu, 2011). Schwartz (1999) questions whether individuals are able to exercise meaningful control over their information in all situations, given disparities in knowledge in the process of data collection and transfer. The implication is that privacy management is not just a matter for the exercise of individual actions but also an important aspect of institutional structure through industry and organizational practices.

To provide a richer conceptual description of privacy management, this research aims to explore the link between individual privacy perceptions and institutional privacy assurances. We argue that enhancing customers' privacy control perceptions and reducing their risk perceptions could be the products of several aspects of organizational practices that are well within the control of the organizations. Institutional privacy assurances based on fair information practices render companies responsible for protecting personal information and help ensure consumers that efforts have been devoted to that end (Culnan & Williams, 2009). Drawing on the Communication Privacy Management (CPM) theory (Petronio, 2002), we examine how institutional privacy assurances (such as privacy policies and industry self-regulation) can contribute to reducing individual privacy concerns. Specifically, we develop a research model to theorize the effects of institutional privacy assurances on reducing individuals' privacy concerns through the risk-control assessment of their information disclosure at a specific level, i.e. related to a specific website.

In what follows, we first present the literature review of information privacy concerns and describe the overarching theory that guides the development of the research model – Communication Privacy Management (CPM) theory. Then we develop the research hypotheses that identify factors included in the process wherein individuals form information privacy concerns. This is followed by the research methodology and findings. We implemented the research design using the context of an online environment. The paper concludes with a discussion of results, the practical and theoretical implications of the findings, and directions for future research.

2. Theory

2.1. Privacy Concerns

Investigating privacy issues requires researchers to identify the root causes of privacy concerns (Phelps, D'Souza, & Nowak, 2000). Because of the complexity of and inconsistencies in defining and measuring privacy, *per se*, and also because the salient relationships depend more on cognitions and perceptions than on rational assessments, almost all empirical privacy research in the social sciences relies on measurement of a privacy-related proxy of some sort. Although the proxies sometimes travel with monikers such as "beliefs," "attitudes," and "perceptions," over time, especially within the field of Information Systems (IS), there has been movement toward the measurement of privacy "concerns" as the central construct. Appendix A summarizes the studies that have included the construct of privacy concerns. As shown in Appendix A, most studies focus on the consequences/impacts of privacy concerns and have treated the construct of privacy concerns as an antecedent to various behavior-related variables, e.g., willingness to disclose personal information (Chellappa & Sin, 2005), intention to transact (Dinev & Hart, 2006b), and information disclosure behavior (Buchanan, Paine, Joinson, & Reips, 2007). Instead of repeating the link between privacy concerns and behavior-related variables, we focus on explaining how individual privacy concerns can be shaped by institutional privacy assurances. Thus, the dependent variable of our research model is the construct of information privacy concerns, or privacy concerns, for short.

Most of the IS studies have conceptualized privacy concerns as *general concerns* that reflect individuals' inherent worries about possible loss of information privacy (Malhotra, Kim, & Agarwal, 2004; Smith, Milberg, & Burke, 1996), However, legal and social scholars have noted recently that privacy is maybe more situation-specific than dispositional, and thus, it is important to distinguish between *general* concerns for privacy and *situation specific* concerns (Margulis, 2003a; Solove, 2006, 2008). The contextual nature of privacy is also addressed by Bennett (1992) and by the Committee of Privacy in the Information Age at the National Research Council (Waldo, Lin & Millett, 2007) which argued that the concern for privacy in a specific situation is much more understandable than it is in the abstract. Following the call for the contextual emphasis of privacy concerns, we adapt the conceptualization of privacy concerns into a situation-specific context, henceforth defined as consumers' concerns about possible loss of privacy as a result of information disclosure to a specific external agent (e.g., a specific website).

2.2. Privacy Boundary Management

The overarching theory that guides the development of the research model is the CPM theory (Petronio, 2002), which was derived from the work of Altman (1974, 1977) on privacy and social behavior, and that of Derlega and Chaikin (1977) on a dyadic boundary model of self-disclosure. The CPM theory was developed to understand how individuals make decisions on information disclosure within interpersonal relationships. This theory uses the metaphor of boundaries to explain the motivation to reveal or withhold information that is governed by "boundary opening" and "boundary closure" rules (Petronio, 2002). When the boundary is open, information flows freely and when it is closed, the information flow is restricted. The CPM theory elaborates elements to aid in decisions about how the information boundaries in dyadic relationships are developed and maintained. Much of the earlier CPM-based research was conducted in interpersonal situations such as marital and parent-child relationships, and physician-patient relationships (see Petronio, 2002 for a review). Recently, the theory has been applied to explain information privacy concerns generated by new technological platforms, including e-commerce (Metzger, 2007) and social media (Child, Pearson, & Petronio, 2009). Moreover, these recent studies have discussed the applicability of the CPM theory

from the interpersonal context to the online individual-organization context. It has been argued that the mental process involved in determining whether to disclose private information to an individual (e.g., a friend or loved one) should be similar to the decision process that must be performed when deciding whether or not to disclose personal information to an online firm (Child et al., 2009; Metzger, 2007). Therefore, Metzger (2007) concludes that the basic premises of CPM theory endure in online privacy management.

CPM is a rule-based theory that proposes that individuals develop rules to form cognitive information spaces with clearly defined boundaries around themselves. This theory identifies three rule management elements: boundary rule formation, boundary coordination, and turbulence. Below we argue that these main elements of boundary rule management–boundary rule formation, coordination, and turbulence—are evident in online privacy management.

2.2.1. Boundary Rule Formation

The CPM theory presumes people make choices regarding information disclosure based on criteria they perceive as salient at the time the decision must be made (Petronio, 2002). With regard to boundary rule formation, this theory proposes that individuals depend on five criteria to generate privacy rules, including: (1) cost-benefit ratio, (2) context, (3) motivations, (4) gender, and (5) culture. In this research, we exclude the culture criteria because of our focus on exploring the link between individuals and organizations regarding privacy. Thus, we ground our work in the first four criteria.

First, the CPM theory suggests that each individual has a mental calculus that is used to construct rules to determine if and when they will disclose personal information based on a cost-benefit calculation of information disclosure (Petronio, 2002). We argue that risk and control represent two key variables individuals weigh when attempting to balance the costs and benefits involved in privacy disclosure. Specifically, when an individual registers a (potential) flow of information in and out across the boundaries, a personal calculus takes place in which the risks are evaluated, along with an estimation of how much control the individual has over the flow.[1] Based on the outcome from the risk-control assessment, the individual evaluates the information flow across boundaries as acceptable or unacceptable. If the flow is acceptable, the individual is not likely to perceive threats, and this will lead to a lower level of privacy concerns. As a consequence, boundary opening and personal information disclosure will be more likely to take place. However, if the flow is unacceptable, the individual is likely to perceive threats that will lead to a higher level of privacy concerns. This may result in boundary closure to prevent information flow.

Second, the CPM theory proposes that context influences the way privacy rules are established and changed (Petronio, 2002). This theory argues that the privacy implications of specific situations or domains can mean something different to each individual. Li, Sarathy, and Xu (2010) also suggest that the effect of privacy-related perceptions is very likely to be overridden by various situational factors at a specific level, e.g., related to a specific firm. However, most empirical studies (e.g., Dinev & Hart, 2006a) consisting of competing influences of benefits and costs of information disclosure have focused on individuals' *general* beliefs or perceptions about releasing personal information but not in a *specific* information exchange context between a firm and an individual. Following the call for the contextual emphasis of boundary rule formation in CPM, we argue in this research that the rules emerging from an individual's articulation of a personal "calculus" of boundary formation should be influenced by the context in which disclosure is deemed acceptable or unacceptable. The conditions "depend in part upon the status of the relationship between the sender and the audience (individual or institutional) receiving it" (Stanton & Stam, 2003, p. 155) and are context specific. Consequently, we conceptualize the risk-control assessment and the construct of privacy concerns in a situation-specific context, e.g., related to a specific firm.

[1] A typical example of this case is an online chat with friends or an online purchase with a vendor well known and frequently used in the past, so making another purchase is "automatic" as with Amazon's "1-Click® Payment Method." In the case when the flow of information across the boundaries is evaluated as unacceptable, the individual perceives the flow as intrusion. Once intrusion is perceived, the individual makes a second round of risk-control assessment that aims to evaluate: 1) whether that particular intrusion is simply an annoyance or disturbance and, thus, not a cause for heightened privacy concerns (e.g., while chatting with a friend, an unknown person solicits contact, but the individual simply ignores him or her); or 2) whether it threatens the person's privacy and, thus, raises one's privacy concerns.

Third, motivational factors may also contribute to privacy boundary rule formation (Petronio, 2002). The CPM theory suggests that when people are judging whether to open boundaries or keep them closed, their rules are also predicated on their inherent need to maintain the boundary that frames personal informational space (Petronio, 2002). As Petronio (2002) pointed out, some people may be motivated to seek the opportunity to express their feelings ("expressive need," p.49), whereas others may have a greater need to avoid engaging in self-disclosure ("self-defense," p.49). In this research, we focus on examining inherent privacy needs through a construct we call the personal disposition to value privacy (DTVP), which reflects an individual's need to maintain certain boundaries that frame personal space.

Fourth, the CPM theory also acknowledges the important role of gender in the management of opening and closing information boundaries and the resulting disclosure or withholding of information (Metzger, 2004, 2007; Petronio, 2002). It has been suggested in the CPM theory that men and women establish rules based on their own unique perspectives of how to enact or maintain privacy (Petronio, 2002). We include gender and other demographic variables as control variables in the research model.

2.2.2. Boundary Coordination and Boundary Turbulence

After individuals disclose their personal information, the information moves to a collective domain where both data subjects (e.g., consumers) and data recipients (e.g., firms) become co-owners with joint responsibilities for keeping the information private (Petronio, 2002). The result is the boundary coordination process through collective control over the use of personal information by both data subjects and data recipients. The CPM theory has suggested that part of the decision to disclose personal information also involves coordinating expectations about how the disclosed information will be treated and who will have access to the information outside the boundary. In other words, a set of privacy access and protection rules will be negotiated among parties and, thus, collectively held privacy boundaries by both data subjects and data recipients are formed. In the context of our research, we argue that privacy policies are one of the boundary coordination mechanisms ensuring consumers that after they disclose personal information, it will be held in a protective domain wherein the company becomes a custodian of the information and accepts responsibility for keeping the information safe and private (Petronio, 2002). The result is that companies are responsible for protecting the information by implementing privacy policies based on fair information practices (Culnan & Bies, 2003).

Due to the complexity of boundary coordination, sometimes the boundary coordination process fails (Petronio, 2002). When there is an invasion from outside sources, or the boundary coordination mechanism does not work, boundary management may become turbulent (Petronio, 2002). For instance, the recent public outcry that ensued after Apple violated its own privacy policy to allow iPhone applications to transmit a user's data (including age, gender, unique phone ID, and location) to third parties elucidates the potentially turbulent relations that can erupt over shifts in boundary conditions (Thurm & Kane, 2010). When boundary turbulence (e.g., privacy violation) occurs, individuals attempt to seek a means of recourse for the aggrieved. In the context of this research, we argue that industry self-regulation is one such mechanism that provides third-party assurances to individuals based on a voluntary contractual relationship among firms and self-regulating trade groups or associations. For example, to address recent public concerns about smart phone privacy issues, the Mobile Marketing Association (MMA) plans to develop a new set of wireless privacy principles and implementation guidelines for mobile application developers, content , and device manufacturers to safeguard privacy of personal information (Walsh, 2010).

3. Research Model Development

The following conclusions can be drawn regarding the formation of privacy concerns based on our discussion of the CPM theory. First, each individual constructs a personal information space with defined boundaries. Second, the boundaries of this information space depend on a risk-control assessment, on an individual's personal dispositions, and on the context of a given relationship with an external entity with which an exchange of information is solicited. Third, when people disclose information, they consider that the information will be held in a protective domain, wherein the company becomes a custodian of the information and accepts responsibility for keeping the information safe and private per its privacy policies. Fourth, when boundary turbulence (e.g., privacy violation) occurs, individuals attempt to seek recourse by defecting or complaining, e.g., filing a complaint with independent third-party privacy groups.

Figure 1 depicts the research model. Based on the CPM framework described above, this research model specifies that privacy concerns are formed: 1) by an individual's perceived boundary of the information space that depends on a contextual risk-control assessment, as well as on the individual's personal dispositions, and 2) by institutional privacy assurances that enable a person to assess the consequences of information disclosure and coordinate boundary management. In the sections below, we define the constructs in our model and present hypotheses of the relationships.

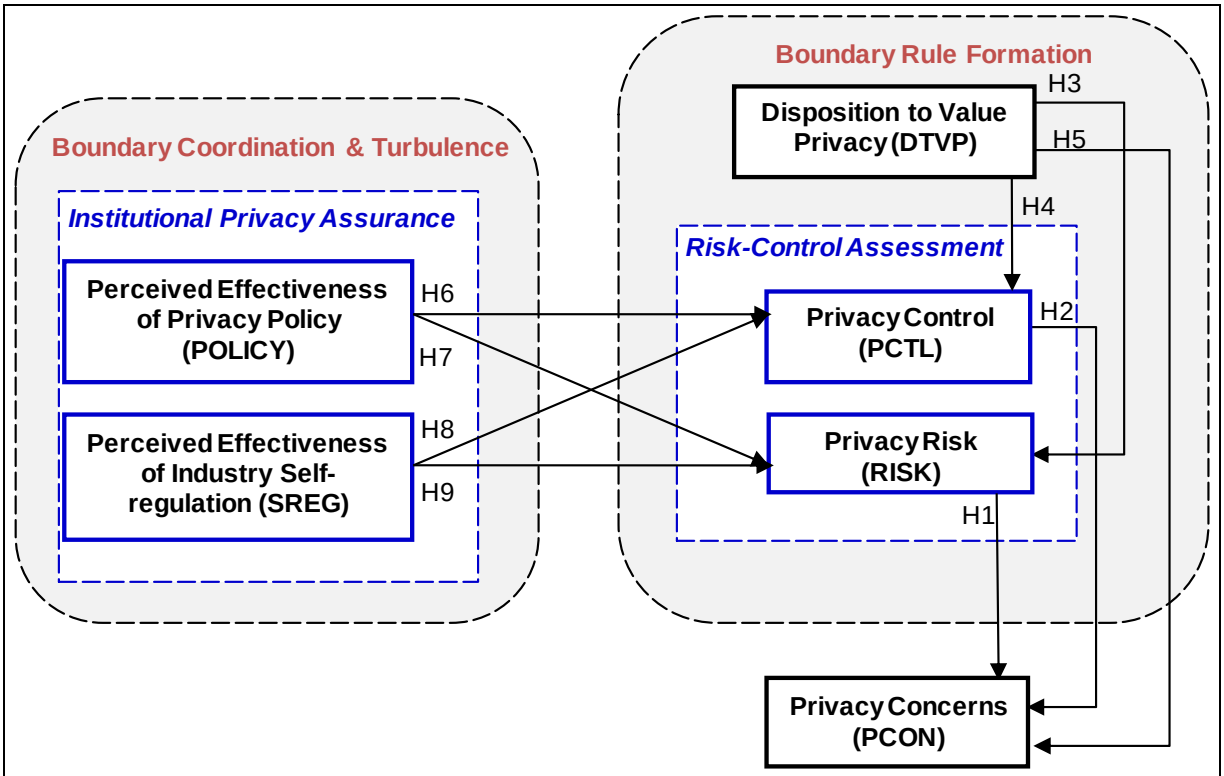

Figure 1. Research Model

3.1. Boundary Rule Formation

According to the CPM theory (Petronio, 2002), information disclosure has both benefits and costs and, thus, involves a contextual risk-control calculation and informed decision making about boundary opening or closing. When people disclose or open their personal space to others, they give away something that they feel belongs to them and, therefore, that they should retain control over it, even after disclosure (Metzger, 2004, 2007). Disclosure renders people vulnerable to opportunistic exploitation because the disclosed personal information becomes co-owned (Petronio, 2002). As such, disclosure always involves some degree of risk (Metzger, 2007). It is this risk that invokes the protective behavior of erecting boundaries that will separate what space/information is considered public and what private. Therefore, these boundaries become the core mechanism for controlling who has access to the personal space/information and how much is revealed or concealed (Metzger, 2007; Petronio, 2002). As we mentioned above, the boundary management rules are also situational and personality dependent, which adds to the complexity and dynamism of privacy and privacy concerns. Below we describe these constructs and their relationships in more details.

3.1.1. Perceived Privacy Risk

Risk has been generally defined as the uncertainty resulting from the potential for a negative outcome (Havlena & DeSarbo, 1991) and the possibility of another party's opportunistic behavior that can result in losses for oneself (Ganesan, 1994). The negative perceptions related to risk may affect an individual emotionally, materially, and physically (Moon, 2000). Sources of opportunistic behavior involving personal information include information collection, processing, dissemination, and invasion activities. Regarding privacy risks, an individual's risk calculation involves an assessment of the

likelihood of negative consequences as well as the perceived severity of these consequences. A number of e-commerce studies empirically verified the negative effect of perceived risks on intentions to conduct transactions (Jarvenpaa & Leidner, 1999; Pavlou & Gefen, 2004). Consistent with prior literature (Malhotra et al., 2004; Norberg & Horne, 2007), we define privacy risk as the expectation of losses associated with the disclosure of personal information.

Along the line of the theory of reasoned action (TRA) (Ajzen, 1991), perceived privacy risk, viewed as the negative antecedent belief, is expected to affect a person's attitude, which is defined as a learned predisposition of human beings (e.g., privacy concerns). Indeed, empirical studies in e-commerce generally support the positive relationship between risk perception and privacy concerns (Dinev & Hart, 2004, 2006a). Accordingly, we expect that the same logic can be applied to our integrative framework. When information flows across a personal boundary, individuals engage in an evaluation about the extent of the uncertainty involved – who has access to the information and how it is or will be used. The higher the uncertainty, the higher individuals perceive the privacy risk. With high risks perceived in disclosing personal information, the individual raises concerns about what may happen to that information (Laufer & Wolfe, 1977). In other words, he or she will raise their privacy concerns. Therefore:

***H1**: Perceived privacy risk positively affects privacy concerns.*

3.1.2. Perceived Privacy Control

As discussed above, more frequently than not, the element of control is embedded in most privacy conceptual arguments and definitions and has been used to operationalize privacy in numerous studies (Culnan, 1993; Malhotra et al., 2004; Sheehan & Hoy, 2000). However, little research has clarified the nature of *control* in the privacy context. For instance, in the privacy literature, control has been used to refer to various *targets* such as social power studies (Kelvin, 1973), procedural fairness of organizational privacy practices (Malhotra et al., 2004), and lack of control over organizational information use (Sheehan & Hoy, 2000). Consequently, Margulis (2003a, 2003b) pointed out that the identification of privacy as a control-related phenomenon has not contributed as much to clarifying the privacy issues as it should have. To fill this gap, Xu and Teo (2004) made one of the first attempts to look into the nature of control in the privacy context through a psychological lens. Following this perspective, "control," interpreted as a perceptual construct with emphasis on personal information as the control target, is conceptualized as a related but distinct variable from privacy concerns. This distinction is consistent with Laufer and Wolfe (1977), who identified control as a mediating variable in a privacy system by arguing that "a situation is not necessarily a privacy situation simply because the individual perceives, experiences, or exercises control" (p. 26). Conversely, an individual may not perceive she has control, yet the environmental and interpersonal elements may create perceptions of privacy (Laufer & Wolfe, 1977). Therefore, we argue that control should be a related but separate variable from privacy concerns.

In this research, we define privacy control as a perceptual construct reflecting an individual's beliefs in his or her ability to manage the release and dissemination of personal information. Empirical evidence in other studies revealed that control is one of the key factors that provides the greatest degree of explanation for privacy concerns (Dinev & Hart, 2004; Phelps et al., 2000). Moreover, consumers' perceptions of control over dissemination of personal information have been found to be negatively related to privacy concerns (Milne & Boza, 1999; Xu, 2007). These considerations suggest that perceived privacy control is a separate construct from privacy concerns and that the two constructs are negatively related. Prior research has shown that, in general, individuals will have fewer privacy concerns when they have a greater sense that they control the release and dissemination of their personal information (Culnan & Armstrong, 1999; Milne & Boza, 1999; Stone & Stone, 1990). In other words, perceived control over personal information is a contrary factor that is weighed against privacy concerns. Therefore:

***H2**: Perceived privacy control negatively affects privacy concerns.*

3.1.3. Disposition to Value Privacy

The CPM framework acknowledges the important role of an individual's inherent need to manage the opening and closing of information boundaries and the resulting disclosure or withholding of

information (Petronio, 2002). The personal nature (self-expression or self-defense) of the boundary management rules is often reflected in the individual's past experiences, demographic characteristics, and personality factors. In the trust literature, a similar construct called propensity to trust (Mayer, Davis, & Schoorman, 1995), or disposition to trust (McKnight, Choudhury, & Kacmar, 2002), has been incorporated in trust theoretical models. Disposition to trust has been defined as "the extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons" (McKnight et al., 2002, p. 339) and has been found to influence trust-related behaviors by framing interpretations of interpersonal relationships (Gefen, 2000; McKnight et al., 2002). Likewise, personal disposition to value privacy (DTVP) is a personality attribute reflecting an individual's inherent need to maintain certain boundaries that frame personal information space. Accordingly, in current research we define DTVP as an individual's general tendency to preserve his or her private information space or to restrain disclosure of personal information across a broad spectrum of situations and contexts.

Following the CPM framework, we posit that personal DTVP will determine boundary opening and closing rules and, thus, will directly affect the risk-control assessment. Individuals who have higher DTVP will inherently cherish their personal boundaries more. Such individuals will need more control over the disclosed information and over the personal information flow, in general. Therefore, they will tend to perceive that they do not have enough control over their own information, as opposed to individuals who, by nature, tend to be more open and sharing of their personal information. The latter group will feel less need for enhanced control; that is, they will have higher perceived control than the former group. Additionally, given the same type of boundary penetration and control, an individual with greater DTVP will have a higher expectation of losses associated with the disclosure of personal information online. For an individual who guards his or her personal space, even a small compromise or opportunistic use of his or her personal information is seen as a big loss of privacy. Thus, such individuals will perceive higher privacy risks associated with information disclosure. Therefore, we hypothesize:

***H3**: DTVP positively affects perceived privacy risk.*

***H4**: DTVP negatively affects perceived privacy control.*

Based on earlier discussions, we can argue that when a boundary penetration is detected, an individual evaluates the status of risk and control associated with potential information disclosure, which informs a possible perception of intrusion into the personal space and, thus, raises privacy concerns. Given the same risk and control assessment of information boundary penetration, an individual who has a higher level of DTVP will be more likely to perceive the boundary penetration as intrusion and, thus, will be concerned about his or her privacy, while an individual who has a lower level of DTVP may be less likely to perceive the same penetration as privacy intrusion. Thus, we further posit that DTVP directly affects privacy concerns. Therefore, we hypothesize:

***H5**: DTVP positively affects privacy concerns.*

3.2. Boundary Coordination and Turbulence: Institutional Privacy Assurance

Situational and environmental factors influence information boundary management rules. Institutional assurance is a salient environmental factor that influences individuals' decisions on information boundary opening or closing. Institutional assurance with respect to privacy concerns is similar to the assurance components of models focusing on trust. The latter assurance components are the institutional dimensions of trust (McKnight et al., 2002). In our model focusing on information privacy, the assurance components are the institutional dimensions of privacy interventions that represent the environmental factors influencing privacy decisions. Following the integrative trust formation model developed by McKnight et al. (2002), we define *institutional privacy assurance* as the interventions that a particular company makes to ensure consumers that efforts have been devoted to protect personal information. These interventions assure consumers that, in terms of information privacy, this company's information practices are reasonable and fair. Previous research (Culnan, 2000; Culnan & Bies, 2003) pointed out two popular types of interventions that organizations can implement and control in their practices – company privacy policy and industry self-regulation, which are examined in this study.

The need for institutional privacy assurances is predicated on the assumption that companies have an incentive to address privacy concerns because if they fail to do so, they will suffer reputational losses (Tang, Hu, & Smith, 2008). Institutional assurances are mechanisms ensuring consumers that when they disclose personal information, it will be held in a protective domain wherein the company becomes a custodian of the information and accepts responsibility for keeping the information safe and private (Petronio, 2002). The result is that companies are responsible for protecting the information by implementing privacy policies based on fair information practices (Culnan & Bies, 2003).

The privacy literature suggests that a firm's collection of personal information is perceived to be fair when the consumer is vested with notice and voice (Culnan & Bies, 2003; Malhotra et al., 2004). A privacy policy is a mechanism through which consumers can be informed about the choices available to them regarding how the collected information is used; the safeguards in place to protect the information from loss, misuse, or alteration; and how consumers can update or correct any inaccurate information. In this research, we define the *perceived effectiveness of privacy policy* as the extent to which a consumer believes that the privacy notice posted online is able to provide accurate and reliable information about the firm's information privacy practices. It has been suggested that the firms' provisions of privacy notice to consumers increase consumers' perceived privacy control (Culnan & Bies, 2003; Milne & Culnan, 2004). Therefore:

> ***H6****: The perceived effectiveness of privacy policy increases consumers' perceived privacy control.*

Interestingly, Culnan and Armstrong (1999) found that for individuals who were informed about information handling procedures by an organization, privacy risk perceptions did not distinguish those who were willing from those who were unwilling to have personal information used for marketing analysis. In other words, privacy risks washed out with the presence of a privacy policy. Previous studies have also shown that businesses that inform consumers about information handling procedures instill greater perceptions of confidence and procedural fairness, thereby lowering consumers' perceived risks of personal information disclosure (Culnan & Armstrong, 1999). Therefore, we hypothesize:

> ***H7****: The perceived effectiveness of privacy policy reduces consumers' perceived privacy risk.*

Industry self-regulatory programs provide another form of institutional privacy assurance. These programs are often established by an industry group or certifying agency (Zwick & Dholakia, 1999). The *perceived effectiveness of industry self-regulation* is defined as the extent to which consumers believe that self-policing industry groups and certifying agencies are able to assist them in protecting their online privacy. Under this self-regulatory approach, industries develop rules and enforcement procedures that substitute for government regulation (Swire, 1997) and often issue certifications in the form of seals of approvals that assure the businesses, indeed, conform to the fair information practices they say they do (Culnan & Bies, 2003). The private sector approach to information privacy regulation consists of industry codes of conduct and the use of self-policing associations to regulate information privacy. For example, as a trade association, the Direct Marketing Association (DMA) has a self-regulatory program for its members, and compliance with its privacy principles is a condition of membership (DMA, 2003). Other examples include privacy seals on e-commerce and e-service websites, such as those given by TRUSTe, whose effectiveness has been examined in prior studies (Hui, Teo, & Lee, 2007; Xu, Teo, Tan, & Agarwal, 2010). Any consumer complaint raised against a licensee will result in reviews and inquiries by the seal program (e.g., TRUSTe). Failure to abide by the terms of the seal program can mean termination as a licensee of TRUSTe and revocation of the trustmark, or referral to the appropriate law authority, which may include the appropriate attorney general's office, the FTC, or the Individual Protection Agency (Benassi, 1999).

The self-regulatory approach to privacy assurance should enhance consumers' perceived control and reduce privacy risk perceptions. Industry self-regulatory programs could limit the firm's ability to behave in negative ways, allowing consumers to form beliefs about expectations of positive outcomes. When a violation occurs, these programs could provide a venue for recourse (Benassi, 1999). These create

strong incentives for firms to refrain from opportunistic behavior. Studies have shown that companies that announce membership in self-regulating trade groups or associations foster consumers' perceptions of privacy control (Culnan & Armstrong, 1999) and mitigate consumers' perceived privacy risks in disclosing personal information (Xu et al., 2010). Therefore, we hypothesize:

> ***H8**: The perceived effectiveness of industry self-regulation increases consumers' perceived privacy control.*
>
> ***H9**: The perceived effectiveness of industry self-regulation reduces consumers' perceived privacy risk.*

3.3. Control Variables

Prior research on information privacy suggests a number of additional factors should be included as control variables because of their potential influence on privacy concerns. Because our primary theoretical focus is not on them, we include them as control variables to eliminate the variance explained by them. They are gender (Sheehan, 1999), age (Culnan, 1995), privacy awareness (Phelps et al., 2000), and previous privacy experience (Smith et al., 1996).

4. Method

4.1. Scale Development

We implemented the research design within the context of the Internet. We empirically tested the research hypotheses using data collected with a survey that included items for the constructs specified in the model. We chose the Internet as the most appropriate context for information privacy research. Because of its development and adoption across the globe, the Internet has become the most relevant and intuitive context for thinking about information privacy. A number of reputable firms such as Google (Hansell, 2008a, 2008b) and Facebook (Stone & Stelter, 2009) have faced privacy-related backlashes in recent years. More and more sites are deploying various tracking tools to clandestinely monitor people's activities online (Vascellaro, 2010). Indeed, all societal entities that deal with personal information, including government, e-commerce, healthcare, finance, and social networks have substantial presence on the web, and the majority of consumers interact with these websites on a daily bases. Thus, we believe respondents will most easily and naturally identify with survey questions about information privacy if they are asked about websites.

Scale development for the constructs (see Appendix B) was based on an extensive survey of the privacy literature. We adapted validated standard scales for use as much as possible. Consistent with recent operationalization of privacy concerns in the literature (e.g., Dinev & Hart, 2006b; Son & Kim, 2008), we measured this construct with seven-point Likert scale items that we directly adapted from Dinev and Hart (2006a). We adapted the language to capture perceptions of specific website privacy practices. We measured perceived privacy risks using four seven-point Likert scale items that were adopted in Dinev and Hart (2006a) and Malhotra et al. (2004) to reflect the potential losses associated with online information disclosure. We measured perceived privacy control using four questions directly taken from Xu (2007). We developed the measurement items for perceived effectiveness of privacy policy and industry self-regulation based on the institutional trust literature (Pavlou & Gefen, 2004), in which the conceptualization of institution-based trust matches our operationalization of institutional privacy assurance. We used TRUSTe as an example of a privacy certifying agency in the context of the Internet. DTVP was measured by three questions that we took from Malhotra et al. (2004).

4.2. Survey Administration

As the CPM theory suggested, the cognitive process with respect to privacy is complex, multifaceted, and context-specific. Individual privacy decision making is a dialectic boundary regulation process conditioned by "individuals' own experiences and social expectations, and by those of others with whom they interact" (Palen & Dourish, 2003, p.129). Accordingly, it seems reasonable to argue that privacy-relevant beliefs should be better related to individuals' own information experiences and social contexts

rather than regarded as a global consequence of technology use per se. To control for the potential effect of information contexts on consumers' reactions, we administered the final survey to Internet users of four different types of websites: 1) electronic commerce sites, 2) social networking sites, 3) financial sites, and 4) healthcare sites. Each participant was randomly assigned to one of the four website contexts.

The survey was administered to undergraduate, graduate, and MBA students at three large universities in the southeastern and northeastern United States. Table 1 provides respondent demographics.

Table 1. Respondent Demographics

Demographic Variables	Category	Frequency (Percent)
Gender	Female Male	365 (44.3%) 458 (55.7%)
Age	18-24 25-29 30-34 35-39 40-49 50 and over	512 (62.2%) 211 (25.6%) 49 (6.0%) 19 (2.3%) 28 (3.4%) 4 (0.5%)
Weekly Web usage: reading newspaper	0-3 hours 4-7 hours 8-13 hours 14+ hours	586 (71.2%) 176 (21.4%) 44 (5.3%) 17 (2.1%)
Weekly Web usage: accessing information about the products/services	0-3 hours 4-7 hours 8-13 hours 14+ hours Missing	353 (42.9%) 301 (36.6%) 123 (14.9%) 38 (4.6%) 8 (1%)
Weekly Web usage: shopping	0-3 hours 4-7 hours 8-13 hours 14+ hours Missing	572 (69.5%) 170 (20.7%) 55 (6.7%) 20 (2.4%) 6 (0.7%)

Participants were asked to recall their experiences in using one website of the assigned context.

We provided definitions and examples of the assigned type of websites in the introduction session of the survey study. Participants were also asked to list the name or URL of a website from the assigned context that they used within the previous six months. There were a total of 918 participants. We removed from the data analysis those responses from participants who said they never used any website of the assigned context. Since participation in the study was completely voluntary, some respondents submitted empty or only partially filled questionnaires that we subsequently eliminated. A total of 823 responses were usable.

While some might argue that the use of student subjects limits the generalizability of the results, we believe that this is an appropriate population to study online privacy. Opponents of the use of student subjects claim that students are inappropriate surrogates for the "real world" when they are asked to imagine themselves as prospective employees in an organizational context. In this study, however, students are naturally a part of the population of interest, and they have experience in using e-commerce, social networking, financial, and healthcare sites. According to the findings of YouthStream Media Networks and Greenfield (2000) as well as Pew Internet & American Life Project (PEW-Internet, 2008), the sample chosen is highly representative of active Internet users (i.e., those between the ages of 18 and 29), making the sample highly appropriate for this context (see also Belanger, Hiller, & Smith, 2002). One recent national survey shows that college students express attitudes toward privacy that are similar to those of older adults (Hoofnagle, King, Li, & Turow, 2010). Moreover, evidence suggests that college students are vulnerable to loss of privacy, with potential information abuse by online crooks, stalkers, hackers and bullies (Gross & Acquisti, 2005).

5. Data Analysis and Results

We used a second-generation causal modeling statistical technique – partial least squares (PLS) -- for data analysis in this research for three reasons. PLS is widely accepted as a method for testing theory in early stages, while LISREL is usually used for theory confirmation (Fornell & Bookstein, 1982). Similar to the cases in prior research (e.g., Ma & Agarwal, 2007), we chose PLS as the statistical technique because of the exploratory nature of this study in the early stage of theoretical development. Additionally, PLS is well suited for highly complex predictive models (Chin, 1998). Prior studies that applied PLS (e.g., Kim & Benbasat, 2006) have found that PLS is best suited for testing complex relationships by avoiding inadmissible solutions and factor indeterminacy. This makes PLS suitable for accommodating the presence of a large number of constructs and relationships in current research. PLS also has the ability to assess the measurement model within the context of the structural model, which allows for a more complete analysis of inter-relationships in the model.

5.1. Measurement Model

Following Gefen, Straub, and Boudreau (2000) and Straub, Boudreau, and Gefen (2004), we evaluated the measurement model by examining the convergent validity and discriminant validity of the research instrument. Convergent validity is the degree to which different attempts to measure the same construct agree (Cook & Campbell, 1979). In PLS, we conducted three tests to determine the convergent validity of measured reflective constructs in a single instrument: reliability of items, composite reliability of constructs, and average variance extracted (AVE) by constructs. We assessed item reliability by examining the loading of each item on the construct and found the reliability score for all the items exceeded the criterion of 0.707 (see Table 2). Thus, the questions measuring each construct in our survey had adequate item reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7 (see Table 3). The average variances extracted (AVE) for the constructs were all above 50 percent, and the Cronbach's alphas were also all higher than 0.7 (see Table 3). As can be seen from the Confirmatory Factor Analysis (CFA) results in Table 2 and the reliability scores in Table 3, these results support the convergent validity of the measurement model.

Table 2. Loadings and Cross-Loadings of Measures

Constructs		PCON	RISK	PCTL	POLICY	SREG	DTVP
Privacy Concerns (PCON)	PCON1	**.830****	.378	-.317	-.265	-.069	.337
	PCON2	**.845****	.410	-.352	-.248	-.053	.306
	PCON3	**.830****	.410	-.288	-.282	-.111	.294
	PCON4	**.866****	.405	-.316	-.295	-.094	.381
Perceived Privacy Risk (Risk)	RISK1	.463	**.882****	-.179	-.290	-.065	.373
	RISK2	.435	**.891****	-.218	-.308	-.066	.292
	RISK3	.370	**.780****	-.269	-.272	-.044	.245
	RISK4	.443	**.825****	-.184	-.329	-.073	.322
Perceived Privacy Control (PCTL)	PCTL1	-.318	-.219	**.858****	.272	.207	-.041
	PCTL2	-.325	-.225	**.892****	.271	.212	-.024
	PCTL3	-.350	-.216	**.884****	.284	.191	-.065
	PCTL4	-.310	-.194	**.825****	.329	.275	-.064
Perceived Effectiveness of Privacy Policy (POLICY)	POLICY1	-.246	-.244	.260	**.879****	.443	.038
	POLICY2	-.356	-.391	.338	**.940****	.446	.067
	POLICY3	-.269	-.312	.313	**.919****	.444	.029
Perceived Effectiveness of Industry Self-regulation (SREG)	SREG1	-.085	-.077	.227	.442	**.866****	.128
	SREG2	-.066	-.049	.225	.419	**.916****	.154
	SREG3	-.114	-.069	.243	.448	**.917****	.123
Disposition to Value Privacy (DTVP)	DTVP1	.349	.338	-.065	-.035	.117	**.891****
	DTVP2	.345	.308	-.047	-.034	.160	**.880****
	DTVP3	.367	.340	-.045	-.020	.123	**.918****

** Significant at the .01 level

Discriminant validity is the degree to which measures of different constructs are distinct (Campbell & Fiske, 1959). Following the procedure to perform CFA suggested by Chin (1998) and applied in Agarwal and Karahanna (2000), we applied two tests to assess discriminant validity. First, all questions were subjected to factor analysis to ensure that questions measuring each construct loaded more highly on their intended construct than on other constructs. As shown in Table 2, all the loadings were higher than cross-loadings.[2] Second, each question should correlate more highly with other questions measuring the same construct than with questions measuring other constructs. This was determined by checking whether the square root of the variance shared between a construct and its measures was greater than the correlation between the construct and any other construct in the model. Table 3 reports the results of discriminant validity, which may be seen by comparing the diagonal to the non-diagonal elements. All items in our study fulfilled the requirement of discriminant validity.

Table 3. Internal Consistency and Discriminant Validity of Constructs

	Composite Reliability	Cronbach's Alpha	Variance Extracted	PCON	RISK	PCTL	POLICY	SREG	DTVP
PCON	0.90	0.87	0.71	0.81					
RISK	0.91	0.87	0.71	0.39	0.84				
PCTL	0.92	0.89	0.74	-0.37	-0.23	0.86			
POLICY	0.94	0.90	0.83	-0.31	-0.32	0.33	0.91		
SREG	0.93	0.88	0.82	-0.09	-0.05	0.25	0.41	0.90	
DTVP	0.92	0.88	0.80	0.39	0.36	-0.06	-0.01	0.14	0.89

Note: PCON = Privacy Concerns; RISK = Perceived Privacy Risk; PCTL = Perceived Privacy Control; POLICY = Perceived Effectiveness of Privacy Policy; SREG = Perceived Effectiveness of Industry Self-regulation; DTVP = Disposition to Value Privacy.

Finally, we addressed the threat of common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Straub et al., 2004). By ensuring anonymity of the respondents, assuring them that there were no right or wrong answers, requesting that each question be answered as honestly as possible, and providing no incentive for participating in the study, we reduced the likelihood of bias caused by social desirability or respondent acquiescence (Podsakoff et al., 2003). Also, we conducted the Harman single-factor test by loading all items to one factor (Podsakoff et al. 2003). No general factor was apparent in the unrotated factor structure, with one factor accounting for 20 percent of the variance, indicating that common method variance is unlikely to be a serious problem in the data. Further, we ran Lindell and Whitney's (2001) test that uses a theoretically unrelated construct (i.e., a marker variable), which was used to adjust the correlations among the principal constructs. We assessed correlation between the marker variable and our research constructs, and the results indicated that the average correlation coefficient was close to 0 ($r = 0.03$, n.s.). Thus, it seems reasonable to argue that our study is relatively robust against common method biases.

5.2. Structural Model

After establishing the validity of the measures, we tested the structural paths in the research model using PLS. We split the dataset into four subsets according to context type and tested the structural models separately for the four different types of websites. Since PLS does not generate any overall goodness of fit indices, predictive validity is assessed primarily by an examination of the explanatory power and significance of the hypothesized paths. Table 4 presents the structural models for the four different contexts as well as for the combined dataset.

As shown in Table 4, the structural models explain 46 percent, 40 percent, 53 percent and 56 percent, of the variance in privacy concerns for the contexts of e-commerce, social networking, finance, and healthcare, respectively. For all four contexts, the direct effects of privacy risk, privacy control, and DTVP on privacy concerns are significant, thus supporting H1, H2, and H5, respectively. As hypothesized, DTVP and perceived effectiveness of privacy policy are found to have significant

[2] To perform CFA in PLS, Chin (1998) suggested the following procedure: Provide the loadings for the construct's own indicators by PLS. Calculate cross-loadings by calculating a factor score for each construct based on the weighted sum of the construct's indicators. Then correlate these factor scores with all other indicators to calculate cross loadings of other indicators on the construct.

impacts on reducing privacy risks, validating H3 and H7. Perceived effectiveness of privacy policy strongly influences privacy control, validating H6.

However, perceived effectiveness of industry self-regulation (H9) does not have a significant impact on privacy risk when the model is run for any of the specific contexts. The influence of DTVP on privacy control (H4) is significant for the social networking context but not for the other three contexts. Finally, the hypothesis for the relationship between perceived effectiveness of industry self-regulation and privacy control (H8) is not supported for the finance context, but it is supported for the other contexts.

Table 4. Structural Model

Hypothesis		Path Estimates				
		Model 1 Combined Dataset (n=823)	Model 2 Electronic Commerce (n=212)	Model 3 Social Networking (n=205)	Model 4 Finance (n=188)	Model 5 Healthcare (n=218)
Theoretical Constructs	H1: RISK →PCON	**0.463***	**0.355***	**0.408***	**0.580***	**0.511***
	H2: PCTL →PCON	**-0.252***	**-0.198***	**-0.251***	**-0.190***	**-0.199***
	H3: DTVP →RISK	**0.341***	**0.334***	**0.346***	**0.324***	**0.373***
	H4: DTVP →PCTL	-0.076	-0.115	**-0.160***	-0.022	-0.083
	H5: DTVP → PCON	**0.189***	**0.232***	**0.169***	**0.164***	**0.177***
	H6: POLICY →PCTL	**0.265***	**0.333***	**0.281***	**0.353***	**0.171***
	H7: POLICY →RISK	**-0.361***	**-0.322***	**-0.242***	**-0.406***	**-0.444***
	H8: SREG →PCTL	**0.182***	**0.204***	**0.217***	0.004	**0.210***
	H9: SREG →RISK	-0.084	-0.075	-0.041	-0.111	-0.051
Covariates	AGE → PCON	0.055	0.062	0.057	-0.021	0.067
	GENDER → PCON	-0.060	-0.120	-0.035	-0.021	-0.051
	AWARE → PCON	-0.005	0.036	-0.125	0.007	0.004
	PEXP → PCON	0.060	0.046	0.052	0.035	**0.156***
	R^2	***46%***	***46%***	***40%***	***42%***	***53%***

**Significant at 5% level*

6. Discussions and Implications

6.1. Discussion of Findings

This study developed and empirically tested a research model that explored the link between individuals' privacy perceptions and institutional privacy assurances. The motivation for this focus was based on the observation that privacy management is not just a matter for the exercise of individual actions, but also an important aspect of institutional structure through industry and organizational practices. We implemented an empirical test of the theoretical model (Figure 1) in the context of online privacy management. Survey respondents were asked to focus on one of four types of websites that they had used. The results showed that the proposed model accounted for between 40 percent and 56 percent of the variance in privacy concerns across different website contexts providing enough explanatory power to make the interpretation of path coefficients meaningful (Table 4). Thus, the results give strong support for the roles of a number of antecedents in influencing the formation of information privacy concerns. These factors can be understood as elements of the CPM theory, which is a useful overarching explanation for an individual's decisions to either reveal or conceal personal information. Moreover, the evidence also supports the notion that a cognitive process involving perceptions of privacy risk and privacy control, along with the DTVP, is important in shaping an individual's privacy concerns. This important finding reveals the institution-individual link related to privacy concerns. That is, privacy concerns are not static, tied to an individual construct, but are highly influenced by institutional factors, such as organizational privacy policies and participation in self-regulatory programs. Our exploration on the link between individuals' privacy perceptions and institutional privacy assurances suggests the need for future studies to understand this link more fully.

A useful interpretation of the results of this study can be made through two analytical lenses. One is based on the paths in the model where the strongest coefficients were found in the results of the combined dataset -- all the respondents for all website contexts -- and the other is based on the variance of the coefficients across the different website contexts.

Overall, our model was validated: the R2 values are high, and most of the hypotheses were supported. Against that backdrop, then, it is useful to drill down by highlighting those paths with relatively higher coefficients (i.e., paths with coefficients > .300): privacy risk to privacy concerns (H1), personal DTVP to privacy risk (H3), and perceived effectiveness of privacy policy to privacy risk (H7). In highlighting these paths, one notes that privacy risk is at the nexis of the antecedent constellation. Both personal DTVP (an internal source) and privacy policy (an external source) directly influence privacy risk. Both internal and external sources are important factors in the cognitive assessment of privacy risk. Understanding privacy has been a difficult scholarly task and one that, as noted early in this paper, has resulted in a range of different definitions. The empirical map of antecedents that influence privacy concerns in this model shows paths that reflect the complexity with which privacy concerns are formed. The study makes a contribution by empirically identifying the salient paths and, at least at this higher level of interpretation, the directions they follow.

The second analytical lens is based on the variance of the coefficients across the different website contexts: e-commerce, social networking, finance, and healthcare sites. Of particular interest are the social networking sites. The results show that DTVP to perceived privacy control was only significant for the social network sites and not the others (H4). A plausible explanation may be a "recency effect": the extensive media coverage about a social networking website in the weeks just prior to the administration of our survey. In early 2008, there was an outcry about a new feature called "Beacon" on Facebook.com. This feature automatically alerted one's friends about the user's Internet purchases. Although users could opt out, doing so was reportedly not intuitive, and there was so much resistance to the feature that Facebook had to remove it. Survey respondents, especially those who subscribed to Facebook, may well have been aware of the privacy issues related to the feature, the ability to control automatic information disclosure on the site, and the degree to which user resistance drove Facebook to eliminate it. Moreover, social networking websites have been rolling out certain features that allow users to control who can access their personal information. For example, Friendster.com embedded privacy control features into various social networking functionalities so that one cannot engage in networking without setting the control features. Thus, it is, perhaps, not surprising that the respondents in the social networking context had a significantly higher mean of perceived privacy control (3.74) than the respondents in the other contexts (i.e., 2.92, 3.30, and 3.14 for e-commerce, financial, and healthcare, respectively). The variation in the results for H4 suggests that the social networking sites may be a unique context that deserves further investigation.

Another observation involves the financial sites. The path from industry self-regulation to perceived privacy control (H8) was not significant. Perhaps the result is not surprising, since the finance industry has its own standards and more strict government regulations for protecting customers' financial information compared to information obtained through other types of business transactions. Thus, industry self-regulation as measured in our investigation seems limited in its influence over individuals' perception of control in the financial context.

The results show that institutional assurance through self-regulation did not mitigate privacy risk for any of the site contexts (H9). This finding suggests that, while organizational intervention through industry self-regulation could enhance individuals' privacy control perceptions, the involvement of a third party is less effective in reducing individuals' privacy risk perceptions. Prior studies have reported similar weak effects of privacy seals on mitigating privacy risk (Hui et al., 2007; Moores, 2005; Moores & Dhillon, 2003). One plausible explanation may be that consumers still have a poor understanding of the role of privacy seals provided by third parties, and hence, their privacy risk perceptions are not affected by them. Thus, there is, indeed, a business incentive for firms to focus more on developing and publicizing their privacy practices, as well as promoting the awareness of industry self-regulation (e.g., privacy seals) among consumers.

We further compare the coefficients across contexts for those hypothesized relationships that were supported by the data (H1, H2, H3, H5, H6, and H7). For each of these six hypotheses, the relationship is stronger for one type of industry than for the others, and these disparities may provide some insights for future research.

For H1 (RISK →PCON), the coefficient of RISK on PCON (b = 0.580) in the finance context is higher than it is in the other three contexts. This suggests that for a given level of risk perception, concerns for privacy are highest among consumers using financial websites. For H2 (PCTL →PCON), the relationship (b = -0.251) is strongest in the social networking context. This suggests that the role of perceived control in alleviating privacy concerns is most significant for consumers using social networking websites. For H3 (DTVP → RISK), the coefficient of DTVP on RISK (b = 0.373) in the healthcare context is higher than it is in the other three contexts. This suggests that for a given level DTVP, consumers using healthcare websites perceived the highest level of risk.

For H5 (DTVP → PCON), the coefficient of DTVP on PCON (b = 0.232) in the e-commerce context is higher than it is in the other three contexts. This suggests that for a given level of personal DTVP, consumers using e-commerce websites perceived the highest level of privacy concerns. For H6 (POLICY → PCTL), the coefficient of POLICY on PCTL (b = 0.353) in the finance context is higher than it is in the other three contexts, which suggests that the role of perceived effectiveness of privacy policy in increasing perceived control is most significant for consumers using financial websites. For H7 (POLICY → RISK) , the coefficient of POLICY on RISK (b = -0.444) in the healthcare context is higher than it is in the other three contexts, which suggests that the role of perceived effectiveness of privacy policy in reducing perceived risk is most significant for consumers using healthcare websites.

Looking across all of these differences among contexts, few obvious patterns emerge. It does appear that consumers using healthcare websites reveal strongest linkages to RISK as a dependent path outcome variable (H3 and H7). It is often argued that health information is, for most data subjects, the most sensitive type of information stored in databases, and this higher sensitivity may be reflected in the model's stronger ability to predict their risk perceptions. (Note, however, that this did not hold for H9, for which results were insignificant in all domains.) Similar logical arguments are not immediately obvious for the other types of websites, however, so we posit the general observation that not only our full model, but also *internal portions* of our model, appear to be stronger in their explanatory power for some websites than for others.

Overall, then, the observations made about the variations across the different web site contexts suggest that there is value in investigating different contexts with respect to understanding privacy concerns. The reported R^2 values across the different sites (Table 4) lend credence to this assertion. Although the reason for these differences is largely conjectural, it does appear that sites utilizing more specific data types are associated with higher percentages of explained variance. For example, there is a 15 percent spread between the finance/healthcare sites and the more general e-commerce site context. The findings reported here suggest that it would be useful to undertake more privacy-related studies that account for specific contexts. This would be consistent with the approach taken by Petronio and her colleagues whose work has covered a range of contexts including healthcare, family, television programs, and so on.

6.2. Limitations

There are several limitations in this study that present useful opportunities for further research. First, although the student subjects in this study comprise a reasonable sample from which to study online privacy (PEW-Internet, 2008), and they are generally concerned about their privacy (Hoofnagle et al., 2010), future research using a more diverse sample could help to further increase the generalizability of this research to the general population. Second, and by design, our work is limited to the examination of how individuals *form* privacy concerns. In this study, we have not extended the nomological network to consider how those concerns are *translated* into intentions and behaviors. In our view, the boundary we have embraced in this study is an appropriate one, as it would be quite unwieldy to derive and test an exhaustive model that also included relationships between privacy concerns and outcome variables. However, as we will discuss below in the "Implications for Research," such an exercise is an obvious extension of this research. Third, while this study did

provide some interesting results across different types of sites, it should be remembered that our objective in embracing this approach was to ensure that any context-specific privacy concerns were being captured. This component of our study should be viewed primarily as an exploratory effort. Indeed, it appears that the results suggest an unanticipated phenomenon: recency effects due to media coverage associated with certain types of websites may impact context-specific perceptions and concerns. This phenomenon deserves additional attention in future studies, as it suggests that domain-specific privacy concerns may be much more dynamic than static in their orientation.

6.3. Contributions and Implications

The study for the first time reveals the organization-individual link regarding privacy: The construct of privacy concerns is not only tied to individual perceptions and attitudes, but it is connected with organizational factors such as privacy policies. This is a very important finding, particularly given the very limited empirical privacy research at the organizational level. This study suggests that several aspects of the organizational practices that are well within the control of firms could enhance customers' privacy control perceptions and reduce their risk perceptions. Institutional privacy assurances based on fair information practices ensure consumers that efforts have been devoted to guard personal information. The result is that businesses that inform consumers about information handling procedures instill greater perceptions of confidence and procedural fairness. That is, organizational privacy practices (such as privacy policies) are linked to individuals' perceptions of these practices, which, in turn, *can* contribute to reducing individual privacy concerns. These findings lead to important implications for both practice and research and should expedite the progress of information privacy research in the IS area and other disciplines as well.

Several theoretical implications follow from our findings. As mentioned above (in "Limitations"), an obvious extension of this study would view privacy concerns as a mediating variable in a much larger nomological network, with privacy concerns leading to intentions and behaviors, likely being informed by both individual and contextual variables. To be sure, some portions of this extended model have already been examined by other researchers (e.g., Chellappa & Sin, 2005; Dinev & Hart, 2006a, 2006b; Phelps et al., 2001; Slyke, Shim, Johnson, & Jiang, 2006). We argue, however, that a larger integrative model that considers not only the antecedents of privacy concerns, but also examines the dependencies derived from them, would make an even larger contribution to the literature. We certainly acknowledge that such an undertaking will be an enormous one, and, in fact, it may require some intermediate studies that consider portions of the supra-model prior to the ultimate test of the entire model.

In this research, great insights have been gained from consideration of individuals' perceptions of various organizational privacy practices. Our initial finding that organizational practices are linked to individuals' perceptions of these practices, which, in turn, raise individuals' privacy concerns, suggests the need for future studies to understand organizational privacy issues more fully. As Culnan and Williams (2009) pointed out, organizations' privacy behaviors have been largely reactive and driven by external pressures. That is, executives rarely take a proactive stance, but rather react to an external event (a threat, security breach, or legislative action) that pressures them to act. Qualitative research methods such as case studies -- which would likely include a set of exhaustive interviews with an organization's members and stakeholders, and some amount of deep "process tracing" -- will certainly produce more insightful results. Such studies will be able to uncover the somewhat subtle organizational dynamics that drive privacy practices and decisions.

It is also worth noting that the DTVP construct in our model had significant relationships with perceptions of privacy risk and privacy concerns in all the domains that we considered in this study. However, this construct is somewhat underdeveloped at this point, and it deserves much additional attention both in the context of instrumentation and also in the context of its role in larger nomological relationships. One can imagine that the DTVP might be related to many other individual traits such as cynicism and paranoia (Smith et al., 1996); it might also serve as a moderating factor in many other relationships, such as the one between intentions and behaviors in privacy-related calculus. We believe that our findings on DTVP may well prove to be fertile ground for additional research on the relationships between privacy concerns and other individual traits.

Another implication for future research and theoretical development is to extend and adapt the model described here to unravel the antecedents of privacy attitudes and behaviors in the context of social media. The variation in the results for H4 suggests that social media may be a unique context that deserves further investigation. In the context of social media marked by active user participation and user-generated content, privacy concerns become particularly salient because users openly and willingly disclose a large volume of personal data and frequently update personal profiles on online social networks (Hoadley, Xu, Lee, & Rosson, 2010; Squicciarini, Xu, & Zhang, 2011; Weiss 2007). Given such contextual differences between social relationship development (in social media) and traditional transaction-oriented systems (in the conventional web), future theoretical development should respond to the urgent call for a privacy paradigm shift in safeguarding privacy for the "social" approach to generating and distributing content in social media.

Finally, we note that one of the fundamental assumptions on which this study rests – that privacy concerns are domain-specific and, thus, must be studied in that context – deserves much additional consideration in terms of confirmation or refutation. To the extent that there is an expectation that an "omnibus" theory of privacy will emerge, this assumption may well prove problematic if confirmed, and the results from this study suggest that it cannot be dismissed. If the assumption does prove robust over time, then this suggests that the theoretical models themselves may also have to be modified to take into account the attributes of various privacy-related domains. One could envision one model for medical data, another for financial data, and so on, with different relationships between constructs (and, even, different constructs themselves) for different domains. Such a situation would deviate somewhat from the extant path in privacy research, but it may well prove to be the most legitimate direction for future research.

From a practical perspective, this study shows that privacy risk and control perceptions are very important factors in determining the level of privacy concerns toward a specific website's information practices. It should be possible to impact both of these perceptions through institutional privacy assurances, as exemplified through privacy policies. Thus, an obvious step in addressing this finding is to review one's privacy policy with an eye toward highlighting the specific areas in which steps are being taken to reduce risk and to empower the data subjects with control. In fact, one reasonable approach might be to provide, within the policy statement, explicit section headings for "risk" and "control." It is currently uncommon to find privacy policies that are organized in this way, and it could well lead data subjects to have improved perceptions.

Of course, such refined policy statements are of scant use if they are not visible to the data subjects. This suggests that websites will need to consider the placement of their privacy policies online as well as their communication of their policies through targeted e-mails, media coverage, etc. Firms will wish to avoid creating the impression that they are hiding their policies, as has been alleged in the case of Google (Hansell, 2008a, 2008b). At a minimum, a website's home page should contain a clear and conspicuous link to the policy – something that Google lacked as of mid-2008 – and an obvious mechanism for asking further questions about the policy. In addition, our results suggest that third party assurances are less effective than privacy policies developed by organizations or companies themselves. This finding should provide additional incentive for businesses to focus on developing their own privacy practices, e.g., developing and enforcing privacy policies, creating an organizational culture of privacy, creating an accountable governance process for privacy, and so forth (see Culnan & Williams, 2009 for a review).

7. Conclusion

This study has provided early empirical support for a model that explains the formation of privacy concerns from the CPM theory perspective. The globalization of economies and information technology and the ubiquitous distributed storage and sharing of data puts the issue of privacy on the forefront of social policies and practices. Drawing on the CPM theory, we developed a model suggesting that privacy concerns form because of an individual's disposition to value privacy, or situational cues that enable one person to assess the consequences of information disclosure. The cognitive process, comprising perceived privacy risk and privacy control, informs individual's information privacy concerns toward websites' privacy practices. We empirically tested the research model through a survey, and the data provide support for the majority of the hypothesized

relationships. The study reported here is novel to the extent that existing empirical research has not explored the link between individuals' privacy perceptions and institutional privacy assurances. We hope that this model will stimulate other scholars to consider the importance of privacy concerns in other contexts.

Acknowledgements

The authors are very grateful to Ping Zhang, Senior Editor, for her encouragement and direction in helping them develop this manuscript. They are also grateful to the reviewers for their constructive advice and very helpful comments on earlier versions of this manuscript. Heng Xu gratefully acknowledges the financial support of the National Science Foundation under grant CNS-0953749.

References

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, 24(4), 665-694.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Altman, I. (1974). Privacy: A conceptual analysis. In D.H. Carson (Ed.), *Man-Environment Interactions: Evaluations and Applications: Part 2* (3-28). Washington, DC.: Environmental Design Research Association.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66-84.

Belanger, F., Hiller, J.S., & Smith, W.J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems*, 11(3-4), 245-270.

Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, 20(5), 313-324.

Benassi, P. (1999). TRUSTe: An online privacy seal program. *Communications of the ACM,* 42(2), 56-59.

Bennett, C.J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology,* 58(2), 157-165.

Campbell, D.T., & Fiske, D.W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, 56(2), 81-105.

Chellappa, R.K., & Sin, R. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2), 181-202.

Child, J.T., Pearson, J.C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology*, 60(10), 2079-2094.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

Cook, M., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston, MA: Houghton Mifflin.

Culnan, M.J. (1993). 'How did they get my name'? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341-363.

Culnan, M.J. (1995). Consumer awareness of name removal procedures: Implication for direct marketing. *Journal of Interactive Marketing*, 9(2), 10-19.

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

Culnan, M.J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science,* 10(1), 104-115.

Culnan, M.J., & Bies, J.R. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323-342.

Culnan, M.J., & Williams, C.C. (2009). How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches. *MIS Quarterly*, 33(4), 673-687.

Derlega, V.J., & Chaikin, A.L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, 33(3), 102-115.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - Measurement validity and a regression model. *Behavior and Information Technology*, 23(6), 413-423.

Dinev, T., & Hart, P. (2006a). An extended privacy calculus model for E-commerce transactions. *Information Systems Research*, 17(1), 61-80.

Dinev, T., & Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29.

Dinev, T., Hart, P., & Mullen, M.R. (2008). Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems*, 17(3), 214-233.

DMA. (2003). *Privacy promise member compliance guide*. Retrieved from http://www.the-dma.org/privacy/privacypromise.shtml

Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-237.

Earp, J.B., & Payton, F.C. (2006). Information privacy in the service sector: An exploratory study of health care and banking professionals. *Journal of Organizational Computing and Electronic Commerce,* 16(2), 105-122.

Fornell, C., & Bookstein, F.L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research,* 19(4), 440-452.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing,* 58(2), 1-19.

Gefen, D. (2000). Lessons learnt from the successful adoption of an ERP: The central role of trust. In S. D. Zanakis, G. Zopounidis and C. Zopounidis (eds.), *Recent Developments and Applications in Decision Making*. Boston, MA: Kluwer Academic.

Gefen, D., Straub, D., & Boudreau, M. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of AIS*, 4(1), 1-78.

Greenfield, Y.M.N.a. (2000). *The Internet is 'Big Man on Campus'—New study from Greenfield online reveals the Web is huge on campus*. Retrieved from http://www8.techmall.com/techdocs/TS000807-2.html.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA.

Hansell, S. (2008a, May 27). Google fights for the right to hide its privacy policy. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2008/05/27/google-fights-for-the-right-to-hide-its-privacy-policy/.

Hansell, S. (2008b, May 30). Is Google violating a California privacy law? *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law/.

Havlena, W.J., & DeSarbo, W.S. (1991). On the measurement of perceived consumer risk. *Decision Sciences*, 22(4), 927-939.

Hoadley, C.M., Xu, H., Lee, J.J., & Rosson, M.B. (2010). Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications,* 9(1), 50-60.

Hoofnagle, C.J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? *SSRN*. Retrieved from http://ssrn.com/abstract=1589864.

Hui, K.-L., Teo, H.H., & Lee, S.-Y.T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, 31(1), 19-33.

Jarvenpaa, S.L., & Leidner, D.E. (1999). Communication and trust in global virtual teams. *Organization Science*, 10(6), 791-815.

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), 203–227.

Kelvin, P. (1973). A social-psychological examination of privacy. *British Journal of Social and Clinical Psychology*, 12(3), 248-261.

Kim, D., & Benbasat, I. (2006). The effects of trust-assuring arguments on consumer trust in Internet stores: application of Toulmin's model of argumentation. *Information Systems Research*, 17(3), 286-300.

Laufer, R.S., & Wolfe, M. (1977). Privacy as a concept and a social issue - Multidimensional developmental theory. *Journal of Social Issues,* 33(3), 22-42.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62-71.

Lindell, M.K., and Whitney, D.J. (2001). "Accounting for common method variance in cross-sectional research designs," *Journal of Applied Psychology,* 86(1), 114-121.

Ma, M., & Agarwal, R. (2007). Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities. *Information Systems Research*, 18(1), 42-67.

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

Margulis, S.T. (1977). Conceptions of privacy: current status and next steps. *Journal of Social Issues*, 33(3), 5-21.
Margulis, S.T. (2003a). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429.
Margulis, S.T. (2003b). Privacy as a social issue and behavioral concept. *Journal of Social Issues,* 59(2), 243-261.
Mayer, R.C., Davis, J.H., & Schoorman, F.D. (1995). An integrative model of organizational trust. *Academy of Management Review,* 20(3), 709-734.
McKnight, D.H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for E-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.
Metzger, M.J. (2004). Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication*, 9(4).
Metzger, M.J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12(2), 335–361.
Milberg, S.J., Burke, S.J., Smith, H.J., & Kallman, E.A. (1995). Values, personal information privacy, and regulatory approaches. *Communications of the ACM,* 38(12), 65-74.
Milne, G.R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5-24.
Milne, G.R., & Culnan, M.J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, 18(3), 15-29.
Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323-339.
Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM*, 48(3), 86-91.
Moores, T.T., & Dhillon, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM*, 46(12), 265-271.
Norberg, P.A., & Horne, D.R. (2007). Privacy attitudes and privacy-related behavior. *Psychology and Marketing*, 24(10), 829-847.
Nunnally, J.C. (1978). *Psychometric Theory*, 2nd ed.. New York: McGraw-Hill.
Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *Proceedings of the SIGCHI conference on human factors in computing systems*, Ft. Lauderdale, Fl., 129-136.
Pavlou, P.A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37-59.
Petronio, S.S. (2002). *Boundaries of privacy: Dialectics of disclosure* (xix,pp. 268). Albany, NY: State University of New York Press.
PEW-Internet. (2008). Pew Internet & American life project: Demographics of Internet users. *PEW,* Retrieved from http://www.pewinternet.org/trends/User_Demo_10%2020%2008.htm.
Phelps, J., D'Souza, G., & Nowak, G.J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.
Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing*, 19(1), 27-41.
Podsakoff, M.P., MacKenzie, B.S., Lee, J.Y., & Podsakoff, N.P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
Schoeman, F.D. (Ed.). (1984). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, UK: Cambridge University Press.
Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review*, 52, 1610-1701.
Sheehan, K.B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4), 24-38.
Sheehan, K.B. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society*, 18(1), 21-32.
Sheehan, K.B., & Hoy, M.G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.
Slyke, C.V., Shim, J.T., Johnson, R., & Jiang, J.J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-444.
Smith, H.J., Milberg, J.S., & Burke, J.S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989-1015.

Solove, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-560.

Solove, D.J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review* (44), 745-772.

Solove, D.J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Son, J.-Y., & Kim, S.S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(3), 503-529.

Squicciarini, C.A., Xu, H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology*, 62(3), 521-534.

Stanton, J.M., & Stam, K. (2003). Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. *Surveillance and Society,* 1(2), 152-190.

Stewart, K.A., & Segars, A.H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.

Stone, B., & Stelter, B. (2009, February 19). Facebook backtracks on use terms. *The New York Times*, B1, B6.

Stone, E.F., & Stone, D.L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management,* 8(3), 349-411.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(1), 380-427.

Swire, P.P. (1997). Markets, self-regulation, and government enforcement in the protection of personal information. In *Privacy and Self-Regulation in the Information Age* (pp. 3-19). Washington, D.C.: Department of Commerce, U.S.A..

Tang, Z., Hu, Y.J., & Smith, M.D. (2008). Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems,* 24(4), 153-173.

Thurm, S., & Kane, Y.I. (2010). Your apps are watching you: A WSJ investigation finds that iPhone and android apps are breaching the privacy of smartphone users. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html#articleTabs%3Darticle.

Vascellaro, E.J. (2010). *Websites rein in tracking tools*. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703957804575602730678670278.html.

Waldo, J., Lin, H., & Millett, L.I. (2007). *Engaging privacy and information technology in a digital age.* Washington, D.C.: National Academies Press.

Walsh, M. (2010). MMA taking on mobile privacy. *MediaPost*. Retrieved from http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=141646&nid=121943.

Warren, S.D., & Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

Weiss, S. (2007). The need for a paradigm shift in addressing privacy risks in social networking applications. In *The Future of Identity in the Information Society* (Vol. 262/2008, pp.161–171). IFIP WG 9.2, Karlstad, Sweden.

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

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *Proceedings of the 28th Annual International Conference on Information Systems*, Montréal, Canada, Paper 125.

Xu, H., and Teo, H.H. (2004). "Alleviating consumer's privacy concern in location-based services: A psychological control perspective," *Proceedings of the 25th Annual International Conference on Information Systems*, Washington, D. C., United States, pp. 793-806.

Xu, H., Teo, H.-H., Tan, B.C.Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 26(3), 135-174.

Yao, M.Z., Rice, R.E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology,* 58(5), 710-722.

Zwick, D., & Dholakia, N. (1999). Models of privacy in the digital age: Implications for marketing and E-commerce. *Research Institute for Telecommunications and Information Marketing (RITIM),* University of Rhode Island.

Appendices

Appendix A. Positivist IS Studies on Privacy

Table A1.

Citation	Theme	Privacy-related concepts	Major Findings
Awad and Krishan (2006)	Examine whether perceived information transparency is associated with consumer willingness to be profiled online	• Previous Online Privacy Invasion • **Privacy concerns** • Privacy Policies • Personal characteristics such as education, income and gender	Customers who desire greater information transparency are less willing to be profiled.
Buchanan et al. (2007)	Measurement development for privacy-related attitudes and behaviors	• Privacy-related attitudes (**privacy concerns**) • Privacy-related behaviors (general caution and technical protection)	Three short Internet-administered scales measuring privacy-related attitudes (privacy concern) and behaviors (General Caution and Technical Protection) are developed and validated.
Bellman, Johnson, Kobrin, and Lohse (2004)	Examine the possible explanations for differences in Internet privacy concerns	• Culture values • Privacy regulatory structure • Government involvement • Internet experience • **Internet privacy concern**	It is found that differences in privacy concerns reflect and are related to differences in cultural values and reflect differences in Internet experience.
Chellappa and Sin (2005)	Predict consumers' usage of online personalization as a result of the tradeoff between their value for personalization and privacy concerns	• Personalization • **Privacy concerns** • Trust • Willingness to share information and use personalization services	The consumers' value for personalization is almost two times more influential than their privacy concerns in determining usage of personalization services.
Culnan (1993)	Identify control as a clear theme in determining individual attitudes toward secondary information use	• **Privacy concerns** • Attitudes toward direct marketing • Demographics • Attitude toward secondary information use	Participants with positive attitudes are less concerned about privacy, perceive shopping by mail as beneficial, and have coping strategies for dealing with unwanted mail.
Dinev and Hart (2004)	Identify perceived vulnerability and perceived control as major antecedents to perceived privacy concerns	• Perceived vulnerability • Perceived ability to control • **Privacy concerns**	Developed and validated an instrument to measure the privacy concerns of individuals who use the Internet and two antecedents, perceived vulnerability and perceived control.
Dinev and Hart (2006b)	Identify social awareness and Internet literacy as major antecedents to perceived privacy concerns	• Social awareness • Internet literacy • **Privacy concerns** • Intention to transact	Social awareness was positively related and Internet literacy was negatively related to Internet Privacy concerns.
Dinev and Hart (2006a)	A theoretical model that incorporated contrary factors representing elements of a privacy calculus was tested and validated.	• Perceived privacy risk • **Privacy concerns** • Trust • Personal internet interest • Willingness to provide personal information to transact on the Internet	Although Internet privacy concerns inhibit e-commerce transactions, the cumulative influence of Internet trust and personal Internet interest are important factors that can outweigh privacy risk perceptions in the decision to disclose personal information.
Dinev, Hart and Mullen (2008)	Test a theoretical model based on a privacy calculus framework and Asymmetric Information Theory	• **Internet privacy concerns** • Perceived need for government surveillance • Government intrusion concerns • Willingness to provide personal information to transact on the Internet	This study found that privacy concerns have an important influence on the willingness to disclose personal information required to transact online. The perceived need for government surveillance was negatively related to privacy concerns and positively related to willingness to disclose personal information. On the other hand, concerns about government intrusion were positively related to privacy concerns.
Earp, Anton, Aiman-Smith, and Stufflebeam (2005)	Compares classes of privacy protection goals and vulnerabilities with consumer privacy values.	• Personalization • Fair Information Practices (Notice, Transfer, Collection, Information Storage and Access) • **Privacy concerns**	Examined Internet users' major expectations about website privacy and revealed a notable discrepancy between what privacy policies are currently stating and what users deem most significant.

Earp and Payton (2006)	Explores employees' privacy orientation in their respective sector, health care or banking	• **Privacy concerns**	Results indicate that healthcare professionals are largely concerned about errors in patient information whereas banking professionals are concerned about improper access of customer information—thereby suggesting differences in perceived privacy practices among these 2 service sectors.
Hui et al. (2007)	Assessed the value of two types of privacy assurance (privacy statements and seals)	• Privacy assurance • Monetary incentive • Information request • Information sensitivity • **Privacy concern** • Information disclosure behavior	This study found that the existence of a privacy statement induced more subjects to disclose their personal information but that of a privacy seal did not; monetary incentive had a positive influence on disclosure; and information request had a negative influence on disclosure.
Jensen , Potts, and Jensen (2005)	Compares users' self-reported with their observed behavior in a simulated e-commerce scenario	• Privacy and security "trust" marks • Existence of privacy policy • Knowledge of, and attitudes toward, privacy-relevant technology • **Privacy concerns** • Privacy reported and actual behavior	This study found that what users said was contrasted with what they did in an experimental e-commerce scenario. Many users have inaccurate perceptions of their own knowledge about privacy technology and vulnerabilities, and that important user groups, like those similar to the Westin "privacy fundamentalists", do not appear to form a cohesive group for privacy-related decision making.
Malhotra et al. (2004)	Develop the dimensionality of Internet Users' Information Privacy Concerns (IUIPC) to reflect internet users' perceptions of fairness/justice	• **Internet Users' Information Privacy Concern (IUIPC)** • Types of information • Trusting beliefs • Risk beliefs • Behavioral intention	The second-order IUIC factor exhibited desirable psychometric properties in the context of online privacy and the structural model including IUIPC explained a large amount of variance in behavioral intention.
Milberg, Burke, Smith, and Kallman (1995)	Examine relationships among nationality, culture values, personal information concerns and information privacy regulation	• Nationality • culture values • regulatory approaches • **Privacy concerns**	Levels of personal information privacy concerns differ across countries.
Sheehan (2002)	Develop a Typology of Internet Users and Online Privacy Concerns	• Awareness • Information use • Information sensitivity • Familiarity • Compensation • **Privacy concerns** • Behaviors	Results indicate that the vast majority of online users are pragmatic when it comes to privacy. This study suggested that online users can be segmented into four distinct groups, representing differing levels of privacy concern: Unconcerned Internet users, Circumspect Internet users, Wary Internet users, and Alarmed Internet users.
Slyke et al. (2006)	Examine the role of Concerns for information privacy (CFIP) in online consumer purchasing	• Risk perception • **Concerns for information privacy** • Trust • Familiarity • Consumers' willingness to transact with web merchant	CFIP affects risk perceptions, trust, and willingness to transact for a well-known merchant, but not for a less well-known merchant. In addition, merchant familiarity does not moderate the relationship between CFIP and risk perceptions or CFIP and trust.
Smith, Milberg, and Burke (1996)	Instrument development to measure privacy concerns about organizational practices	• **Concerns for information privacy** • **(CFIP)**	Developed and validated a 15-item instrument with four subscales tapping into dimensions of CFIP: collection, errors, unauthorized secondary use, and improper access.
Son and Kim (2008)	Develop taxonomy of information privacy-protective responses (IPPR).	• **Concerns for information privacy** • Perceived justice • Societal benefits from complaining • Information privacy-protective responses (IPPR)	The taxonomy of IPPR consists of three categories of behavioral responses: information provision, private action and public action. This study also developed a nomological model and showed how the antecedents of IPPR differentially affect the six types of IPPR. The results indicate that some discernible patterns emerge in the relationships between the antecedents and the three groups of IPPR.
Stewart and Segars (2002)	Examine the factor structure of CFIP posited by Smith et al. (1996)	• **Concerns for information privacy** • **(CFIP)**	CFIP may be more parsimoniously represented as a higher-order factor structure rather than a correlated set of first-order factors.
Yao, Rice, and Wallis (2007)	Examine factors that could potentially influence user concerns about online privacy	• Beliefs in privacy rights • Internet use diversity • Internet use experience • Self-efficacy • Psychological need for privacy • **Privacy concerns**	Beliefs in privacy rights and a psychological need for privacy were the main influences on online privacy concerns.

Appendix B. Measurement Items (measured on seven-point, Likert-type scale)

Table B1.

Privacy Concerns (PCON): Mean = 4.85, Std. Deviation = 1.31

1. I am concerned that the information I submit to this website could be misused.
2. I am concerned that others can find private information about me from this website.
3. I am concerned about providing personal information to this website, because of what others might do with it.
4. I am concerned about providing personal information to this website, because it could be used in a way I did not foresee.

Privacy Risks (RISK): Mean = 4.71, Std. Deviation = 1.27

1. In general, it would be risky to give personal information to this website.
2. There would be high potential for privacy loss associated with giving personal information to this website.
3. Personal information could be inappropriately used by this website.
4. Providing this website with my personal information would involve many unexpected problems.

Privacy Control (PCTL): Mean = 3.27, Std. Deviation = 1.55

1. I believe I have control over who can get access to my personal information collected by this website.
2. I think I have control over what personal information is released by this website.
3. I believe I have control over how personal information is used by this website.
4. I believe I can control my personal information provided to this website.

Perceived Effectiveness of Privacy Policy (POLICY): Mean = 4.27, Std. Deviation = 1.49

Some companies post privacy statements on their Web sites to give information about their information practices, e.g., what information is collected, how your information is used, with whom your information may be shared, and etc. Please indicate the extent to which you agree or disagree with each statement by ticking the appropriate number.

1. I feel confident that these websites' privacy statements reflect their commitments to protect my personal information.
2. With their privacy statements, I believe that my personal information will be kept private and confidential by these websites.
3. I believe that these websites' privacy statements are an effective way to demonstrate their commitments to privacy.

Perceived Effectiveness of Industry Self-Regulation (SREG): Mean = 4.31, Std. Deviation = 1.28

There are third parties such as self-policing trade groups and associations, which prevented companies from using your personal information for any purpose other than processing your request. Groups like TRUSTe have been active as the third party entities policing online privacy interests and promoting trustworthiness to web sites through seals of approval. Please indicate the extent to which you agree or disagree with each statement by ticking the appropriate number.

1. I believe that privacy seal of approval programs such as TRUSTe will impose sanctions for online companies' noncompliance with its privacy policy.
2. Privacy seal of approval programs such as TRUSTe will stand by me if my personal information is misused during and after transactions with online companies.
3. I am confident that privacy seal of approval programs such as TRUSTe is able to address violation of the information I provided to online companies.

Disposition to Value Privacy (DTVP): Mean = 5.63, Std. Deviation = 1.19

1. Compared to others, I am more sensitive about the way companies handle my personal information.
2. To me, it is the most important thing to keep my information privacy.
3. Compared to others, I tend to be more concerned about threats to my information privacy.

Privacy Awareness (AWARE): Mean = 4.79, Std. Deviation = 1.33

1. I am aware of the privacy issues and practices in our society.
2. I follow the news and developments about the privacy issues and privacy violations.
3. I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy.

Previous Privacy Experience (PEXP): Mean = 3.08, Std. Deviation = 1.20

1. How often have you been a victim of what you felt was an improper invasion of privacy?
2. How much have you heard or read during the past year about the use and potential misuse of the information collected from the Internet?
3. How often have you experienced incidents where your personal information was used by a company without your authorization?

About the Authors

Heng XU is an assistant professor of Information Sciences and Technology at The Pennsylvania State University where she is a recipient of the endowed PNC Technologies Career Development Professorship. She received her Ph.D. in Information Systems in 2005. She currently directs the Privacy Assurance Lab, an interdisciplinary research group working on a diverse set of projects related to assuring information privacy. Her ongoing research projects deal with the impacts of novel technologies on individuals' privacy concerns, strategic management of firms' privacy and security practices, and design and empirical evaluations of privacy-enhancing technologies. Her research has appeared in *Decision Support Systems*, *Information & Management, Journal of Management Information Systems*, *Journal of the American Society for Information Science and Technology*, *MIS Quarterly*, and in other journals. In 2010, she was a recipient of the Faculty Early Career Development (CAREER) Award by the National Science Foundation.

Tamara DINEV is an associate professor and chair of the Department of Information Technology and Operations Management (ITOM), College of Business, Florida Atlantic University, Boca Raton, Florida. She received her Ph.D. in Theoretical Physics in 1997. Following several senior positions in information technology companies, her interests migrated to management information systems research, and she joined the Florida Atlantic University ITOM faculty in 2000. Her research interests include information privacy, trust in online vendors, multicultural aspects of information technology usage, and information security. She has published in several journals, including *MIS Quarterly, Information Systems Research, Journal of the AIS, Journal of Strategic Information Systems, Communications of the ACM, International Journal of Electronic Commerce, European Journal of Information Systems, Journal of Global Information Management, e-Service Journal*, and *Behaviour and Information Technology*. She has received numerous best paper awards and nominations at major information system conferences.

Jeff H. SMITH is the George and Mildred Panuska Professor in Business in the Farmer School of Business at Miami University in Oxford, Ohio. His research focuses on ethical, societal, and regulatory issues associated with strategic uses of information technology. His research also examines organizational impediments to successful implementation of information technology applications. His research has appeared in *California Management Review, Communications of the ACM, Harvard Business Review, MIS Quarterly, MIT Sloan Management Review, Organization Science,* and in other journals. He served on the editorial board of *MIS Quarterly* from 2003-2006 and as Chair of the Department of Decision Sciences and Management Information Systems at Miami University (Ohio) from July 2006 until July 2011. He holds B.S. degrees in computer science and math from North Carolina State University; an M.B.A. degree from the University of North Carolina in Chapel Hill; and a D.B.A. degree from Harvard University. He worked for the International Business Machines (IBM) Corporation for several years in the area of software development.

Paul HART is Professor of Information Technology and Operations Management and an Associate Dean in the College of Business at Florida Atlantic University. He received his Ph.D. from the Annenberg School of Communications at the University of Southern California. His research interests include information privacy and security, information technology applications in medical contexts, and information technology-inter-organizational relationships. He has published in a number of journals including *Information Systems Research, Organization Science, Journal of Strategic Information Systems, Decision Sciences, European Journal of Information Systems, Journal of MIS, International Journal of E-Commerce, Management Communications Quarterly*, and *ACM Transactions on Information Systems*. He received numerous best paper awards and nominations at major information system conferences.