Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2008 Proceedings

International Conference on Information Systems (ICIS)

2008

Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View

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

Tamara Dinev
Florida Atlantic University, tdinev@fau.edu

H. Jeff Smith
Miami University - Oxford, jeff.smith@muohio.edu

Paul Hart
Florida Atlantic University, hart@fau.edu

EXAMINING THE FORMATION OF INDIVIDUAL'S PRIVACY CONCERNS: TOWARD AN INTEGRATIVE VIEW

Examen de la formation individuelle du souci de protection de la vie privée : vers une vision intégrative

Completed Research Paper

Heng Xu
Pennsylvania State University
University Park, PA 16802
hxu@ist.psu.edu

Tamara Dinev
Florida Atlantic University
Boca Raton, FL 33431
tdinev@fau.edu

H. Jeff Smith
Miami University
Oxford, OH 45056
jeff.smith@muohio.edu

Paul Hart
Florida Atlantic University
Boca Raton, FL 33431
hart@fau.edu

Abstract

Numerous public opinion polls reveal that individuals are quite concerned about threats to their information privacy. However, the current understanding of privacy that emerges is fragmented and usually discipline-dependent. A systematic understanding of individuals' privacy concerns is of increasing importance as information technologies increasingly expand the ability for organizations to store, process, and exploit personal data. Drawing on information boundary theory, we developed an integrative model suggesting that privacy concerns form because of an individual's disposition to privacy or situational cues that enable one person to assess the consequences of information disclosure. Furthermore, a cognitive process, comprising perceived privacy risk, privacy control and privacy intrusion is proposed to shape an individual's privacy concerns toward a specific Web site's privacy practices. We empirically tested the research model through a survey (n=823) that was administered to users of four different types of web sites: 1) electronic commerce sites, 2) social networking sites, 3) financial sites, and 4) healthcare sites. The study reported here is novel to the extent that existing empirical research has not examined this complex set of privacy issues. Implications for theory and practice are discussed, and suggestions for future research along the directions of this study are provided.

Keywords: Privacy concerns, disposition to value privacy, privacy assurance, privacy risk, privacy control, information boundary theory

Résumé

En nous appuyant sur la théorie des frontières d'information, nous développons un modèle intégratif suggérant que le souci de protection de la vie privée se forme du fait de la disposition des individus à la confidentialité ou du fait d'éléments situationnels permettant à une personne d'évaluer les conséquences d'une divulgation d'informations. Nous testons empiriquement le modèle de recherche à travers une enquête (n=823) administrée à des utilisateurs dans différents contextes d'utilisation d'Internet.

Introduction

The importance of privacy in the contemporary globalized, information societies has been widely discussed and is by now undisputed. Numerous works in diverse fields have immensely improved our understanding of privacy at the individual, organizational and societal levels. However, the picture of privacy that emerges is fragmented and usually discipline-dependent. The definitions of privacy vary significantly in different fields, ranging from a *right* or *entitlement* in law (e.g. Warren and Brandeis 1890), to a *state of limited access or isolation* in philosophy and psychology (e.g., Schoeman 1984), and 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 Solove (2006) to note that "[p]rivacy as a concept is in disarray. Nobody can articulate what it means." (p. 477). Privacy has been described as multidimensional, elastic, depending upon context, and dynamic in the sense that it varies with life experience (Altman 1977; Laufer and Wolfe 1977).

Over the past decade, scholars in information systems have examined privacy issues (Malhotra et al. 2004a; Smith et al. 1996; Stewart and Segars 2002) related to the collection and use of personal information from a variety of perspectives. A general observation from this stream of research is that privacy researchers have often used the construct of *privacy concerns* as the proxy to define and measure the concept of *privacy*. Accordingly, the construct of privacy concerns has usually been included and empirically validated as an important factor in various behavioral models (e.g., Chellappa and Sin 2005; Dinev and Hart 2006b).

Little is known, however, on how privacy concerns are formed and developed, and what individual, cultural, institutional, and environmental factors mitigate or influence them in a systematic manner. In general, in complex nomological behavioral models, the construct of privacy concerns has been treated as a psychologically unitary, stand-alone concept (e.g., Slyke et al. 2006). Thus, understanding the nature and formation of privacy concerns, as well as their predictors, is a major issue for researchers and practitioners. Yet, no comprehensive model has been developed in the extant literature to conceptually explore the formation process of privacy concerns as well as to differentiate privacy concerns from other overlapping cognate concepts such as intrusion, privacy risk, privacy control, privacy assurance, and disposition to value privacy. We seek to address this gap in the literature by developing a literature-grounded model that highlights the interrelated factors that contribute to the formation of privacy concerns. By rigorously identifying antecedents of privacy concerns, and by testing our model in different contexts of Internet usage, we are able to conceptually clarify the multiple dimensions of privacy concerns.

Theory

The research model is depicted in Figure 1. The model implies 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. A cognitive process, comprising privacy risk, privacy control and privacy intrusion is proposed to shape an individual's perception of a specific Web site's privacy practices (i.e., privacy concerns).

Information Boundary Theory (IBT)

The overarching theory that guides the development of the research model is the Information Boundary Theory (IBT), which formulates the social aspects of information disclosure. IBT posits that each individual forms a physical or virtual informational space around her with clearly defined boundaries. Depending on the situational and personal conditions, an attempt by an external entity to penetrate these boundaries may be perceived by the individual as intrusion. The motivation to reveal or withhold information is governed by "boundary opening" and "boundary closure" rules (Petronio 2002a). These rules involve dynamic psychological processes that are affected by the nature of the relationship, the expected use of the disclosed information, and the benefits of disclosing the information (Petronio 2002a). Thus, it is important to note that the rules emerge from an individual's articulation of a personal "calculus" of boundary negotiation which is influenced by the conditions 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 and Stam 2003, p. 155); thus they are context specific.

IBT has been applied in employee privacy research (e.g., Stanton and Stam 2003) which provided a reasonable foundation for understanding privacy management in IT intensive organizations. The concept of information

boundary in the information privacy context means that: First, each individual constructs a personal informational space with her own defined boundaries. Second, the boundary of this information space depends on the nature of the information and the individual's own personality and environmental characteristics. Third, when the individual detects a request for information disclosure by an organization (for example, an e-commerce store), the individual initiates a calculus process. The risks of disclosure are evaluated, along with estimation of how much control the individual has over the disclosed information. Based on the outcome of risk-control assessment, the individual deems the disclosure as acceptable or unacceptable. If the disclosure is acceptable, the individual is not likely to perceive privacy intrusion and thus has lower level of privacy concerns. As a consequence, a boundary opening follows and personal information is revealed. In the case the disclosure is evaluated as unacceptable, the individual perceives this outcome as privacy intrusion. Depending on the risk-control assessment, the perception of intrusion may give rise to privacy concerns. Therefore, boundary closing may follow and the information is withheld. Based on the IBT framework described above, below we define each construct in our model and present the hypotheses of the relationships among constructs.

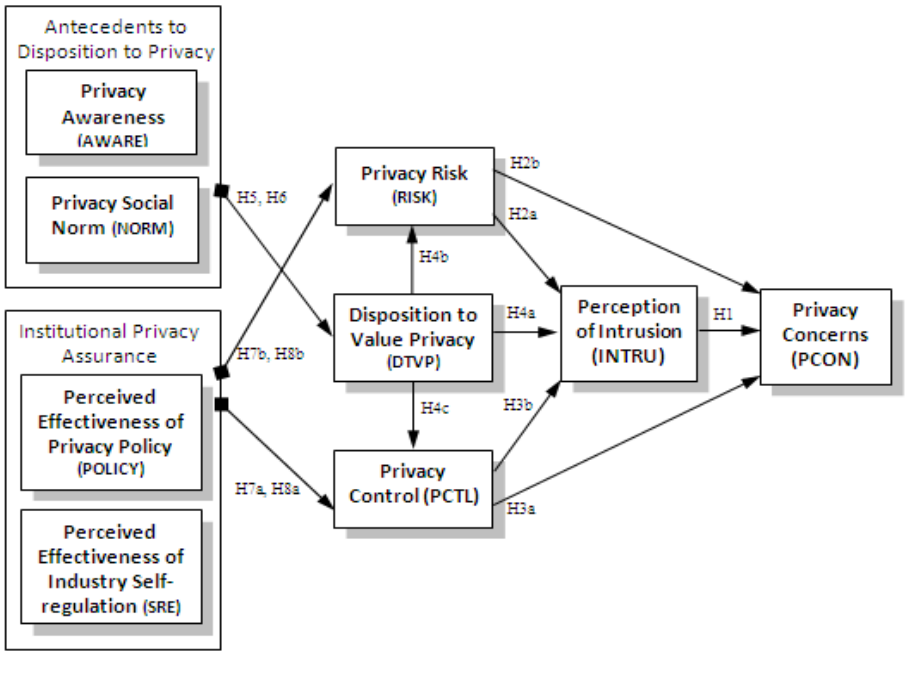

Figure 1. Research Model – Constructs and Nomological Network

Privacy Concerns

Prior research into privacy issues has focused on understanding what motivates Internet users to disclose personal information and what inhibits them from disclosing it. Among various privacy related constructs examined in the literature, the construct of privacy concerns is one of the most widely used variable in the IS research and consistently shown to be one of the strongest predictors of privacy-related behavior (Dinev and Hart 2006b; Malhotra et al. 2004a; Stewart and Segars 2002). In addition, the concept of privacy concerns has been a viable part of the economical privacy models such as privacy calculus which treats individual privacy-related behavior as a result of a situational and context-specific cost-benefit analysis of information disclosure (Acquisti and Grossklags 2005; Culnan and Armstrong 1999; Dinev and Hart 2006b). Several pioneering privacy studies have attempted to conceptualize and operationalize privacy concerns in more detail: The Concern for Information Privacy (CFIP) scale was developed by Smith, Milburg, and Burke (1996) which identified four data-related dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access to information) that have since served as one of the most reliable instrument measuring individuals' concerns toward organizational privacy practices. Recently, Malhotra, Kim, and Agarwal (2004a) operationalized a multidimensional notion of Internet Users Information Privacy Concerns (IUIPC) which adapted the CFIP in the Internet context.

In this study, we avoid repeating the numerous extant studies about the link between privacy concerns and behavior-related variables. Instead, we focus on explaining how privacy concerns are formed. Thus, the dependent variable of our research model is the construct of privacy concerns which is defined as concerns about possible loss of privacy as a result of information disclosure to an online business.

Perception of Intrusion

The concept of intrusion has always been related to the concept of personal space (Solove 2004; Solove 2007; Tolchinsky et al. 1981; Westin 1967), which particularly well matches with our IBT framework. Based on a comprehensive review of scholarly work and courts' interpretations of privacy and intrusion, Solove (2006) defines intrusion as "invasive acts that disturb one's tranquility or solitude" (p.491) and "involves the unwanted general incursion of another's presence or activities" (p.555). Solove (2006) further argues that intrusion disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Protection against intrusion involves protecting the individual from unwanted social invasions, affording people what Warren and Brandeis called "the right to be let alone" (1890, p. 193). According to Solove (2006), intrusion can create discomfort and harm and requires protection even if the information is barely disseminated. Thus, intrusion has always been identified as an event harmful to the individual, and with this, it bears negative connotation (see also Tolchinsky et al. 1981; Westin 1967).

However, we argue that not every penetration of the personal space is deemed as harmful by the individual. Examples of personal space's boundaries penetrations that are not perceived or labeled as intrusion are abundant: 911 teams breaking in a house to save a person's life from a health, fire, or crime threats; consented personal information and habit gathering to received special offers and coupons; sensitive medical information request to select the best medical treatment; installation of security monitoring systems in private spaces, etc. Therefore, perception of boundary penetration and perception of intrusion are two different perceptions and the latter obviously involves a specific set of beliefs, to be perceived of causing harm and labeled as intrusion.

Intrusion was identified as a component of privacy by the tort scholar Prosser (1960) who synthesized the cases that emerged from Warren and Brandeis's famous law review article *The Right to Privacy* (1890). Prosser categorized four types of harmful activities under the rubric of privacy, namely: 1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; 2) Public disclosure of embarrassing private facts about the plaintiff; 3) Publicity which places the plaintiff in a false light in the public eye; 4) Appropriation, for the defendant's advantage, of the plaintiff's name or like-ness. Likewise, Westin (1967) defined reserve as "the creation of a psychological barrier against unwanted intrusion" as a component of his four states of individual privacy. And Tochinsky et al. (1981) developed the Invasion of Privacy Score (IPS) that captures the perception of intrusion into the personal information space. As one can see, intrusion can certainly raise privacy concerns, but intrusion is not the only condition that informs individual's privacy concerns. In other words, intrusion perception is not identical with privacy concerns. The items 2, 3, and 4 from Rosser's categorization above also inform privacy concerns but they can occur without any form of intrusion into the personal space. Therefore, we conclude that perceived intrusion is a distinctly different construct from privacy concerns. Seeing that perceived intrusion involves harmful incursion into the personal information space, we propose it as an important predictor to privacy concerns:

H1: Perception of intrusion positively affects privacy concerns.

Determinants to Perception of Intrusion

Prior research on information disclosure within the framework of IBT points to the following important components of boundary management: risk and control, personal and environmental factors. According to the IBT and its adaptive form of Communications Privacy Management Theory (Petronio 2002b), disclosure has both benefits and risks and thus involves a complex calculation and informed decision making about boundary opening or closure. When people disclose or open their personal space to the others, they give over something they feel belongs to them and thus "they feel they should retain the right to control it and not be harmed, even after disclosure" (Metzger 2004; Metzger 2007). Disclosure renders people vulnerable to opportunistic exploitation because the disclosed private information becomes co-owned by other parties (Petronio 2002b). As such, disclosure always involves some degree of risk (Metzger 2007). It is the risk that invokes the protective behavior of erecting boundaries that will separate what space/information we consider public and private. Therefore, these boundaries become the core mechanism of

controlling who and how much has access to the personal space/information (Metzger 2007; Petronio 2002b). Therefore, the boundary management rules are developed to help people maximize the benefits from disclosure while minimizing the risks. As we mentioned above, these rules are situational and personality dependent and may change very dynamically. The benefits include self-expression, to relationship development, to social control, while the risks include loss of dignity, status, control (Metzger 2007; Petronio 2002b).

We propose that, when a boundary penetration has been detected by an individual, she develops a perception of intrusion into her personal space after the evaluation of risks and control involved in the penetration. In other words, perceived risk and perceived control are major determinants of perception of intrusion. The personal nature (self-expression) of the boundary management rules and of the perception of intrusion are reflected in the individual's cultural and personality characteristics which we call disposition to value privacy, much like the development of disposition to trust in the trust literature (e.g. McKnight et al. 2002). Furthermore, the situational and environmental factors on which the boundary management rules develop are reflected in the "perception of the environment" through a set of organizational privacy assurance variables, much like the structure assurance in the trust literature (e.g. McKnight et al. 2002). Below we describe these construct and their relationships with more details.

Perceived Privacy Risk

Risk has been generally defined as uncertainty resulting from the potential for a negative outcome (Havlena and DeSarbo 1991) and the possibility of the other party's opportunistic behavior that can result in losses (Ganesan 1994; Yates and Stone 1992). Sources of opportunistic behavior with personal data include selling to, or sharing information with third parties, financial institutions (Budnitz 1998) or government agencies (Preston and 2004; Wald 2004). Privacy risk could also include the misuse of personal information, such as insider disclosure or unauthorized access and theft (Rindfleisch 1997). A number of e-commerce studies empirically verified the negative effect of perceived risk on intentions to conduct transactions (Jarvenpaa et al. 2000; Norberg et al. 2007; Pavlou and Gefen 2004). Consistent with prior literature (Malhotra et al. 2004a; McKnight et al. 2002), we define perceived privacy risk as the expectation of losses associated with the disclosure of personal information online. Early conceptual work has suggested that the potential negative consequences of information disclosure are related to perceived invasion of privacy (Fusilier and Hoyer 1980; Petronio 1991; Petronio 2002b). Therefore, the higher the perceived risk from a penetration into the personal information space, the higher the likelihood that it will be perceived as intrusion.

H2a. Perceived privacy risk positively affects perceptions of intrusion.

Along the line of the theory of reasoned action (TRA) (Ajzen 1991), privacy risk perception, viewed as the negative antecedent belief, is expected to affect a person's attitude that is defined as a learned predisposition of human beings (e.g., privacy concerns). Empirical studies in e-commerce generally supported this expectation of the negative relationship between risk perception and privacy concerns (Dinev and Hart 2004; Dinev and Hart 2006b). Accordingly, we expect that the same logic can be applied to our integrative framework.

H2b. Perceived privacy risk positively affects privacy concerns.

Perceived Privacy Control

The element of *control* is embedded in most privacy conceptual arguments and definitions and has been used to operationalize privacy in numerous measurement instruments (Altman 1975; Culnan 1993; Kelvin 1973; Margulis 1977; Smith et al. 1996; Westin 1967). Privacy scholars have often linked the concept of privacy with control by either defining privacy as control *per se*, or positioning control as a key factor shaping privacy. In this research, "control" – interpreted as perceived control over disclosure and subsequent use of personal information – is conceptualized as a related but separate variable from privacy concerns. Such conceptualization has been supported by Laufer and Wolfe (1977), who positioned control as a mediating variable in the 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, the individual may not perceive she has a control, yet the environmental and interpersonal elements may create perceptions of privacy (Laufer and Wolfe 1977). These considerations suggest that perceived privacy control is a separate construct from privacy concerns and that the two constructs are negatively related. Empirical evidence revealed that control is one of the key factors which provide the greatest degree of explanation for privacy concern (Phelps et al. 2000; Sheehan and Hoy 2000; Xu 2007). In other words,

perceived control over disclosure and subsequent use of personal information is a contrary factor that is weighed against privacy concerns.

H3a. Perceived privacy control negatively affects privacy concerns.

Prior literature has generally supported the relationship between perceived control and perceived privacy invasion (Fusilier and Hoyer 1980). It has been found that individuals who perceived they had control over the use of the information to be disclosed, experienced less privacy invasion than did those who believed they had no control over their personal information (Fusilier and Hoyer 1980). Culnan and Armstrong (1999) also argue that individuals perceive information disclosure to be less privacy-invasive when they believe that they are able to control future use of the information. Conversely, using personal information without permission is viewed as a privacy invasion and unethical behavior (Cespedes and Smith. 1993), which may result in angry and disloyal customers who are more likely to defect (Morgan and Hunt 1994; Nowak 1995). Therefore, we hypothesize that:

H3b. Perceived privacy control negatively affects perceptions of intrusion.

Disposition to Value Privacy

The IBT theory suggests that the privacy management of opening and closing the boundaries of the personal space and the resulted in disclosure or withholding of information is dependent on the individual's personal characteristics. In the trust literature, a similar construct reflecting the personal trusting tendencies has been identified and named propensity to trust (Mayer et al. 1995) or disposition to trust (McKnight et al. 2002) which has been shown to influence trusting beliefs in the literature. Likewise, personal disposition to value privacy reflects the individual's inherent needs and attitudes towards marinating a personal space. Patil and Kobsa (2005) define and measure the personal disposition towards privacy as how much individuals "value privacy" (Patil and Kobsa 2005) and have found that it is a major determinant to privacy concerns. Similarly, we define disposition to value privacy as the extent to which a person displays a willingness to preserve his or her private space or to disallow disclosure of personal information to others across a broad spectrum of situations and persons. In the IBT framework, given that personal characteristics such as self-expression (Metzger 2004; Metzger 2007; Petronio 2002b) determine the boundary opening/closure rules, we posit that disposition to value privacy, as a personal characteristics, affects directly the perception of intrusion, and indirectly, through the latter, privacy concerns. Thus, given the same risk and control assessment of a certain personal space penetration or information gathering, an individual who has a higher value to privacy will perceive the penetration as intrusion, while an individual who tends to be more "open" and more likely to share "his or her space or information", will not perceive the same penetration as intrusion. Additionally, given the same type of privacy penetration, an individual with greater disposition to value privacy will perceive higher risk of and lower control over his or her personal space and information. Therefore, we hypothesize:

H4a. Disposition to value privacy positively affects perception of intrusion.

H4b. Disposition to value privacy positively affects perceived privacy risk.

H4c. Disposition to value privacy negatively affects perceived privacy control.

We consider two subconstructs to disposition to value privacy, namely privacy awareness and privacy social norms. Both have been related to the individual's innate characteristics of privacy in the literature and both have been shown to be important factors.

Privacy Awareness

Privacy awareness reflects the extent to which an individual is informed about privacy practices and policies, about how disclosed information is used, and is cognizant about their impact over the individual's ability to preserve her private space (Donaldson 1989; Donaldson and Dunfee 1994; Dunfee et al. 1999; Phelps et al. 2000). Dinev and Hart (2006b) developed social awareness as a predictor to privacy concerns. According to them, individuals with high social (privacy) awareness will in general closely follow privacy issues, the possible consequences of a loss of privacy due to accidental, malicious, or intentional leakage of personal information, and the development of privacy policies. Media news and highly publicized cases will heighten their acquaintance with possible breaches of privacy and security, and the risks. These individuals will have a stronger awareness and will appreciate more the importance of privacy in social life. Therefore, privacy awareness is an antecedent to the personal disposition to

value privacy, which in our model is the very factor that reflects the *personal* characteristics of the privacy management and information disclosure, per IBT:

H5. Privacy awareness positively affects disposition to value privacy.

Privacy Social Norm

As Laufer and Wolfe (1977) argue, the "mores of a community transmitted through language, tradition, and values constitute boundaries of consciousness about privacy" (p. 28). Patterns and forms of privacy has long been related to the cultural characteristics of the social group an individual lives in (Altman 1977; Roberts and Gregor 1971). Several MIS studies have found that there are differences in information privacy concerns across cultures (Bellman et al. 2004; Dinev et al. 2006a; Dinev et al. 2006b; Milberg et al. 2000), the cultural dimension of individualism (Hofstede 1980; Hofstede 2003) being the most responsible factor for these differences. The concept of privacy is related to the extent that individualism is sought after and reinforced in a culture (Etzioni 1999). In the U.S., a highly individualistic society, legal precedent and public opinion highly value privacy as an expression and a safeguard of personal dignity (Laufer and Wolfe 1977) and individual right (Etzioni 1999; Westin 1967). Additionally, per IBT, the perception of space is also associated with the notion of privacy (see also Laufer and Wolfe 1977). What is private versus public space, as well as how much physical distance between people is considered normal are all distinct characteristics of cultures, and all are related to perceptions of privacy (Hall and Hall 1990). We posit that, the social norm about privacy determines an individual's disposition to value privacy and thus influences the boundary management in the IBT framework:

H6. Privacy social norm positively affects disposition to value privacy.

Institutional Privacy Assurance

Situational and environmental factors influence information boundary management rules. Institutional assurance is a salient environmental factor that influences information boundary opening or closing. Institutional assurance with respect to privacy concerns is similar to the assurance components of models focusing on trust. In the latter the assurance components are the institutional dimensions of trust (McKnight et al. 2002). In our model focusing on privacy, the assurance components are the institutional dimensions of risk and control and represent the environmental factors that influence information boundary management 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 is safe. This study focuses two types of interventions: (a) company privacy policy and (b) industry self-regulation.

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. 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 co-owner 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 and 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 and Bies 2003; Malhotra et al. 2004b). In other words, consumers want to influence changes in firms' polices that they find to be objectionable (Malhotra et al. 2004b). Privacy policy is a mechanism where 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. The prescription of notification of and consent by consumers effectively exemplifies procedural fairness and thus increases consumers' perceived control over their personal information (Culnan and Bies 2003; Milne and Culnan 2004). Therefore:

H7a: 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 concerns did not distinguish individuals 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 and Armstrong 1999). Therefore, we hypothesize:

H7b: The perceived effectiveness of privacy policy reduces consumers' perceived privacy risk.

Frequently, institutional privacy assurance is reinforced by the industry self-regulatory initiatives. These involve standards established by an industry group or certifying agency which are then voluntarily adopted by industry members or associates (Zwick and Dholakia 1999). 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 which assure that the businesses indeed conform to the fair information practices they purport to (Culnan and Bies 2003). The private sector approach to information privacy regulation consists of industry codes of conduct and the use of self-policing trade groups and associations to regulate information privacy. An examples of an industry self-regulator is the Direct Marketing Association (DMA) that made compliance with its privacy principles as a condition of membership (DMA 2003). Other examples include privacy seals on e-commerce and e-service web sites such as those given by Online Privacy Alliance or TRUSTe, and whose effectiveness has been examined in prior MIS studies (Xu and Teo 2004; Xu et al. 2005). In this situation, consumers and businesses collectively control personal information, with the industry self regulator acting as a facilitator for resolving any conflicts that may arise (Xu 2007). Studies have shown that companies that announce membership in self-regulating trade groups or associations foster consumers' perceptions of control over their personal information (Culnan and Armstrong 1999) and mitigate consumers' perceived privacy risks in disclosing personal information (Xu et al. 2005). Therefore, we hypothesize:

H8a: The perceived effectiveness of industry self-regulation increases consumers' perceived privacy control.

H8b: The perceived effectiveness of industry self-regulation reduces consumers' perceived privacy risk.

Method

Scale Development

The research hypotheses were empirically tested using data collected with a survey that included items for the constructs specified in the model. Scale development for the constructs was based on an extensive survey of the privacy literature. Validated standard scales were adapted for use as far as possible. Privacy concerns were measured by seven-point Likert scale items that were directly taken from the measurement of concern for information privacy (CFIP) outlined in Smith et al. (1996): collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. However, wordings were adapted to capture perceptions of a specific web site's privacy practices. In our search for rigorously validated empirical measures for perception of intrusion, we explored the literature in social sciences, political economy, sociology, and organizational sciences, and contacted leading researchers in these fields. We were not able to find any previously developed and rigorously validated instruments that measure perception of intrusion as a separate construct. In previous studies, perceptions of intrusion items were included in general privacy-related instruments (Tolchinsky et al. 1981, Stone et al. 1983). Consistent with the current best practices in scale development, we relied on theoretical developments of the construct and its meaning (Westin 1967, Solove 2006, Mael et al 1996); and we cast a wide net in identifying candidate items. We constructed an initial set of items reflecting the underlying theory while observing the trends in general survey research (refer to Appendix A for the items).

We measured perceived privacy risks using four seven-point Likert scale items that were adopted in Dinev and Hart (2006a) and Malhotra et al. (2004a) to reflect the potential losses associated with the information disclosure. Perceived privacy control was measured using four questions directly taken from Xu (2007). The measurement items for perceived effectiveness of privacy policy and industry self-regulation were developed based on institutional trust literature (Pavlou and Gefen 2004) in which the conceptualization of institution-based trust matches our operationalization of institutional privacy assurance. We used TRUSTe as an example of privacy seal in the context of Internet. Disposition to value privacy was measured by three questions that were directly taken from Malhotra et al. (2004a). Awareness to privacy was measured by three questions that were directly taken from Dinev

and Hart (2005). Drawing on technology adoption literature (Venkatesh et al. 2003), social norm was measured with three questions that addressed the importance of social influence on individual privacy perceptions.

Survey Administration

The initial questionnaire was reviewed by four Information Systems (IS) faculty members for clarity. Next, a pilot study involving 51 undergraduate students was conducted using the improved questionnaire. The main objectives of the pilot study were to assess the clarity and conciseness of the survey instructions and questions, evaluate the measurement model, and gauge the duration of the survey. The respondents were also contacted for a face-to-face interview so that their opinions on the survey instructions and questions could be gathered. Following their feedback and analysis of measurement model, a number of revisions were made: some items were dropped, wording changes were made, and instructions that the respondents found confusing were clarified. All measurement items were included in Appendix A.

Due to the context-specific nature of privacy (Altman 1975), parameter estimates in the model (e.g., factor mean levels, path coefficients) may not necessarily be the same among different contexts. As such, the final survey was administered to users of four different types of web sites: 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 Internet usage contexts. The final survey was administered to undergraduate, graduate and MBA students at three large universities in the United States. Participants were asked to recall their experiences in using one website of the assigned context. They were also asked to list the name or URL of the assigned context within last 6 months. The responses from those participants who never used any website of assigned context were dropped from data analysis. There were 1015 subjects participated; 823 responses were usable.

Data Analysis and Results

Partial least squares (PLS), a second-generation causal modeling statistical technique, was used for data analysis. PLS possesses many advantages over traditional statistical methods such as factor analysis, MANOVA and regression. First, PLS is well suited for highly complex predictive models (Chin 1998b). This makes PLS suitable for handling large number of constructs. Second, PLS has the ability to assess the measurement model within the context of the structural model, which allows a more complete analysis of inter-relationships in the model. Third, PLS is generally more appropriate for testing theories in the early stages of development (Fornell and Bookstein 1982). Given the large number of constructs being tested as well as the exploratory nature of this study in the early stage of theoretical development, PLS is more suitable than other methods.

Measurement Model

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 and Campbell 1979). In PLS, three tests are used to determine the convergent validity of measured reflective constructs in a single instrument: reliability of items, composite reliability of constructs, and average variance extracted by constructs. Appendix A presents the assessment of the measurement model. 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. Thus, the questions measuring each construct in our experiment had adequate item reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7. The average variances extracted for the constructs were all above 50 percent, and the Cronbach's alphas were also all higher than 0.7. These results support the convergent validity of the measurement model (see Appendix A).

Discriminant validity is the degree to which measures of different constructs are distinct (Campbell and Fiske 1959). To test discriminant validity, the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model. Table 1 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 1. Discriminant Validity									
	PCON	**INTRU**	**RISK**	**PCTL**	**POLICY**	**SEAL**	**DTVP**	**AWARE**	**NORM**
PCON	0.805								
INTRU	0.604	0.863							
RISK	0.604	0.515	0.841						
PCTL	-0.371	-0.343	-0.232	0.861					
POLICY	-0.306	-0.315	-0.321	0.328	0.913				
SEAL	-0.084	-0.085	-0.051	0.246	0.506	0.903			
DTVP	0.398	0.337	0.356	-0.061	-0.008	0.142	0.894		
AWARE	0.107	0.089	0.127	0.063	0.024	0.110	0.315	0.889	
NORM	0.220	0.203	0.207	0.013	0.102	0.169	0.458	0.323	0.834

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 the type of contexts and the structural models were tested separately for four different types of websites. We conducted hypothesis tests by examining the sign and significance of the path coefficients. A bootstrapping technique was applied to estimate the significance of the path coefficients. Since PLS does not generate any overall goodness of fit indices, predictive validity is assessed primarily through an examination of the explanatory power and significance of the hypothesized paths. The explanatory power of the structural model is assessed based on the amount of variance explained in the endogenous construct (i.e., privacy concerns). We conducted the statistical tests at a five-percent level of significance using one-tailed t-tests.

Table 2 presents the structural models for four different contexts. The structural models explain 37%, 49%, 57% and 59%, of the variance in privacy concerns in the contexts of e-commerce, social networking, finance and healthcare respectively. As shown in Table 2, for all the four contexts, the direct effect of perception of intrusion, privacy risk, and privacy control are significant, thus supporting H1, H2b, and H3a, respectively. As hypothesized, privacy risk and privacy control strongly influence perception of intrusion, thus validating H2a and H3b. Disposition to privacy and perceived effectiveness of privacy policy are found to have significant impacts on reducing privacy risks, validating H4b and H7b. Privacy social norm is a significant predictor of disposition to value privacy, supporting H6. Perceived effectiveness of privacy policy strongly influences privacy control, validating H7a.

Table 2. Results of Hypotheses Testing

Hypothesis	E-Commerce (n=212)		Social Networking (n=205)		Finance (n=188)		Healthcare (n=218)	
	Path Estimate	Supported	Path Estimate	Supported	Path Estimate	Supported	Path Estimate	Supported
H1: INTRU →PCON (+)	**0.330***	Yes	**0.349***	Yes	**0.367***	Yes	**0.374***	Yes
H2a: RISK →INTRU (+)	**0.477***	Yes	**0.197***	Yes	**0.568***	Yes	**0.514***	Yes
H2b: RISK →PCON (+)	**0.280***	Yes	**0.396***	Yes	**0.405***	Yes	**0.419***	Yes
H3a: PCTL →PCON (-)	**-0.139***	Yes	**-0.187***	Yes	**-0.130***	Yes	**-0.144***	Yes
H3b: PCTL →INTRU (-)	**-0.176***	Yes	**-0.256***	Yes	**-0.160***	Yes	**-0.179***	Yes
H4a: DTVP →INTRU (+)	**0.223***	Yes	**0.241***	Yes	**0.180***	Yes	0.077	**No**
H4b: DTVP →RISK (+)	**0.335***	Yes	**0.346***	Yes	**0.323***	Yes	**0.372***	Yes
H4c: DTVP →PCTL (-)	-0.111	**No**	**-0.160***	Yes	-0.023	**No**	-0.081	**No**
H5: AWARE →DTVP (+)	**0.238***	Yes	0.024	**No**	**0.246***	Yes	**0.194***	Yes
H6: NORM →DTVP (+)	**0.421***	Yes	**0.477***	Yes	**0.390***	Yes	**0.366***	Yes
H7a: POLICY →PCTL (+)	**0.274***	Yes	**0.280***	Yes	**0.352***	Yes	**0.171***	Yes
H7b: POLICY →RISK (-)	**-0.301***	Yes	**-0.242***	Yes	**-0.405***	Yes	**-0.446***	Yes
H8a: SEAL →PCTL (+)	**0.145***	Yes	**0.159***	Yes	0.004	**No**	**0.210***	Yes
H8b: SEAL →RISK (-)	-0.095	**No**	-0.039	**No**	-0.051	**No**	-0.051	**No**
R^2	***37%***		***49%***		***57%***		***59%***	

*Significant at 5% level of significance.

However, perceived effectiveness of privacy (H8b) does not have any significant impact on perceived privacy risk. For the hypothesis on the relationship between disposition to value privacy and perception of instruction (H4a), it is not significant for the healthcare context but significant for the rest contexts. Regarding the impact of disposition to value privacy on privacy control (H4c), it is significant for the social networking context but this is not the case for the rest three contexts. Privacy awareness has been found to be a significant predictor of disposition to value privacy (H5) in the e-commerce, finance and healthcare contexts but such relationship is not supported in the social networking context. For the hypothesis on the relationship between perceived effectiveness of privacy seal and privacy control (H8a), it is not significant for the finance context but significant for the rest of contexts.

Discussion and Conclusion

Discussion of Findings

This study developed and empirically tested an integrative model to investigate the formation process of privacy concerns. Our proposed model is able to account for 37% ~ 59% of the variance in privacy concerns across different Internet usage context, which possesses enough explanatory power to make the interpretation of path coefficients meaningful. The evidence from this study provided empirical support 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. A cognitive process of assessing the information boundary, comprising privacy risk, privacy control and privacy intrusion, is shown important to shape an individual's privacy concerns towards a specific Web site's privacy practices.

More than previous empirical privacy studies, this research shows that privacy constructs relate to each other in organized, meaningful ways. This is important because definitions of privacy and relationships among privacy-related constructs are inconsistent and not fully developed or empirically validated in current literature. Having an integrative research framework with consistent set of constructs should enable privacy research to progress more quickly by having systematic understandings.

The findings empirically validate the cognitive process of privacy concerns. Perception of instruction, perceived privacy risk and perceived privacy control are shown to be important in affecting privacy concerns across different context in e-commerce, social networking, finance and healthcare. The results also show that individuals' control perceptions over their personal information could help reduce their perceptions of intrusion; and their privacy risk perceptions significantly lead to perceptions of intrusion. For all the four Internet usage contexts, disposition to value privacy is shown to be an important predictor of perceived privacy risk; and privacy social norm is found to be a significant predictor of disposition to value privacy. Furthermore, this study shows that the organizational privacy assurance intervention through privacy policy could increase individuals' perceived privacy control and mitigate their privacy risk perceptions across different contexts.

However, the proposed organizational intervention through privacy seals did not have a direct impact on perceived privacy risk in any of the four contexts (H8b). One plausible explanation for this unexpected finding is that the participants did not trust these privacy seals provided by third parties, and hence their privacy risk perceptions were not affected by the privacy seals. This finding is not surprising as prior studies have shown the weak effects of privacy seals on mitigating privacy risks (Hui et al. 2007). In fact, Edelman (2006) recently found that TRUSTe-certified sites are more than twice as likely to be untrustworthy as uncertified sites. Hence, privacy interventions involving a third party appear less effective than those interventions directly from web sites (e.g., privacy policy). This result suggests that there is indeed a business incentive for websites to focus more on enhancing their privacy policies.

The insignificant effect of industry self-regulation (i.e., operationalized as privacy seals in this study) on privacy risk prompts a question about the role it plays in alleviating privacy concerns. The results show that, although privacy seals were ineffective in mitigating privacy risk, it did enhance individuals' privacy control perceptions for the usage of e-commerce, social networking, and healthcare sites. Hence, it seems that privacy seals can only influence perception of intrusion and privacy concerns indirectly through the privacy control. However, such effect of privacy seals cannot be applied to the usage of financial sites. Our result showed that perceived effectiveness of privacy seals did not affect privacy control perception for the finance context (H8a). There is perhaps nothing surprising in this finding since the finance industry has its own standards and more strict government regulations for protecting

customers' financial information. Thus, it seems that the market for privacy seals in the financial sector is very limited. In fact, none of the finance sites used by our participants has a privacy seal.

Another context-specific difference in the hypothesized relationships is the lack of statistical significance for the path between disposition to value privacy and perception of intrusion (H4a) in the healthcare context. Perhaps many individuals who use healthcare sites have urgent needs and want to benefit from information they can acquire through them. They understand that submitting detailed personal information is required in order to obtain precise and accurate medical information or services. They may feel that they have to adjust their privacy preferences and disposition which might otherwise lead them to withhold information submission in other contexts. An adjustment would reflect an evaluation of the risk and control factors in the privacy calculus that would result in a different information boundary decision than the one an individual might make in other contexts.

As for the relationship between DTVP and perceived privacy control (H4c), the results show that it was statistically significant only for the social networking context. In addition, the context of social networking differs from the other three in another hypothesized relationship. For the effect of privacy awareness on DTVP (H5), it was insignificant for the social networking context but significant for the other three. Regarding such interesting pattern of results for the social networking context, a plausible explanation is that these results may to some degree be a function of extensive media exposure in the weeks prior to the administration of our survey. In early 2008, there was a privacy outcry regarding news feed features and the web beacon at social networking sites (e.g., Facebook.com). Thus, users of social networking sites may well have been more aware of privacy issues associated with such sites, which leads to the insignificant relationship between privacy awareness and DTVP. In addition, social networking companies have been rolling out features that allow users to control who can access their personal information. Some social networking sites (e.g., Friendster.com) even embedded the privacy control features into the very use of various social networking functions and thus integrated privacy control as part of social networking functionality. Accordingly, it is perhaps not surprising to see that our respondents from the social networking context had a significantly higher mean of perceived privacy control (3.74) than the respondents from the other contexts (2.92, 3.30, and 3.14 for e-commerce, financial, and healthcare, respectively). These interesting results indicate that there is possibly a set of other factors that are unique for the users of the social networking sites but probably less important for the other three contexts. Future research could be directed to further explore the social networking context.

Implication and Conclusion

Our research model is strongly rooted in a general conceptual framework drawing on IBT and our model is likely to be applicable to a variety of privacy-related contexts. Our posited predictors explain 37% ~ 59% of the variance in the construct of privacy concerns in different context, suggesting that the IBT serves as a useful theoretical foundation in the information privacy context. Additionally, the present study highlights the roles of personal characteristics and organizational interventions in increasing privacy control and mitigating privacy risk, which have important implications for the Web vendors in diverse sectors.

From a practical perspective, this study shows that a privacy cognitive process involving calculating privacy risk and control perceptions as well as perception of invasion are the important factors in determining the level of privacy concerns toward a specific website's information practices. In this aspect, this study provides some insights into the different approaches that could be employed by a website. First, this study shows that incorporating organizational privacy structural assurances through privacy policy is one of the important ways of increasing individuals' privacy control perceptions and reducing their privacy risk perceptions. Second, although organizational intervention through privacy seals could enhance individuals' privacy control perceptions (with exception of social networking sites), such involvement with a third party is less effective in reducing individuals' privacy risk perceptions. Thus, there is indeed a business incentive for websites to focus more on enhancing their privacy policies and communicating them to their customers.

In conclusion, this study provides preliminary empirical support to understand the formation of privacy concerns from the information boundary theory perspective. Using the groundwork laid down in this study, future research along various possible directions could contribute significantly to extending our theoretical understanding and practical ability to tackle the Internet privacy issues.

Appendix A. Psychometric Properties of the Measurement Model

Construct Indicators (measured on seven-point, Likert-type scale)	Factor Loadings	Composite Reliability	Cronbach's Alpha	Variance Extracted
Privacy Concerns (PCON)				
It bothers me when these websites ask me for this much personal information.	0.716	0.902	0.873	0.648
I am concerned that these websites are collecting too much personal information about me.	0.835			
I am concerned that unauthorized people may access my personal information.	0.818			
I am concerned that these websites may keep my personal information in a non-accurate manner.	0.794			
I am concerned about submitting information to websites.	0.854			
Privacy Intrusion (INTRU)				
I feel that as a result of my using these websites, others know about me more than I am comfortable with.	0.867	0.921	0.889	0.744
I believe that as a result of my using these websites, the information about me that I consider private is now more readily available to others than I would want to.	0.894			
I feel that as a result of my using these websites, the information about me is out there that, if used, will invade my privacy.	0.827			
I feel that as a result of my using these websites, my privacy has been invaded by the others that collect all the data about me.	0.861			
Privacy Risks (RISK)				
In general, it would be risky to give personal information to websites.	0.880	0.906	0.867	0.707
There would be high potential for privacy loss associated with giving personal information to websites.	0.885			
Personal information could be inappropriately used by websites.	0.777			
Providing websites with my personal information would involve many unexpected problems.	0.816			
Privacy Control (PCTL)				
I believe I have control over who can get access to my personal information collected by these websites.	0.857	0.920	0.886	0.742
I think I have control over what personal information is released by these websites.	0.888			
I believe I have control over how personal information is used by these websites.	0.882			
I believe I can control my personal information provided to these websites.	0.819			
Perceived Effectiveness of Privacy Policy (POLICY)				
I feel confident that these websites' privacy statements reflect their commitments to protect my personal information.	0.882	0.937	0.899	0.833
With their privacy statements, I believe that my personal information will be kept private and confidential by these websites.	0.938			
I believe that these websites' privacy statements are an effective way to demonstrate their commitments to privacy.	0.917			
Perceived Effectiveness of Privacy Seal (SEAL)				
I believe that privacy seal of approval programs such as TRUSTe will impose sanctions for online companies' noncompliance with its privacy policy.	0.872	0.930	0.881	0.816
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.	0.918			
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.	0.920			
Disposition to Value Privacy (DTVP)				
Compared to others, I am more sensitive about the way online companies handle my personal information.	0.889	0.923	0.878	0.800
To me, it is the most important thing to keep my online privacy.	0.879			
Compared to others, I tend to be more concerned about threats to my personal privacy.	0.915			
Awareness to Privacy (AWARE)				
I am aware of the privacy issues and practices in our society.	0.818	0.919	0.865	0.791
I follow the news and developments about the privacy issues and privacy	0.934			

violations.				
I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy.	0.911			
Social Norm (NORM)				
People who influence my behavior think that keeping personal information private is very important.	0.780	0.872	0.780	0.695
My friends believe I should care about my privacy.	0.868			
People who are important to me think I should be careful when revealing personal information online.	0.851			

References

Acquisti, A., and Grossklags, J. "Privacy and Rationality in Individual Decision Making.," *IEEE Security & Privacy* (3) 2005, pp 26-33.

Ajzen, I. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50) 1991, pp 179-211.

Altman, I. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Brooks/Cole Publishing, Monterey, CA, 1975.

Altman, I. "Privacy Regulation: Culturally Universal or Culturally Specific?," *Journal of Social Issues* (33:3) 1977, pp 66-84.

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

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

Campbell, D.T., and Fiske, D.W. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:1) 1959, pp 81-105.

Cespedes, F.V., and Smith., H.J. "Database Marketing: New Rules for Policy and Practice," *Sloan Management Review* (34:Summer) 1993, pp 7-22.

Chellappa, R.K., and Sin, R. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2) 2005, pp 181-202.

Chin, W.W. "The Partial Least Squares Approach to Structural Equation Modeling," in: *Modern Methods for Business Research,* G.A. Marcoulides (ed.), London, 1998b, pp. 295-336.

Cook, M., and Campbell, D.T. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Houghton Mifflin, Boston, 1979.

Culnan, M.J. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3) 1993, pp 341-364.

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

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

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. "Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States," *Journal of Global Information Management* (14:4), Oct-Dec 2006a, pp 57-93.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. "Privacy calculus model in e-commerce - a study of Italy and the United States," *European Journal of Information Systems* (15:4), Aug 2006b, pp 389-402.

Dinev, T., and Hart, P. "Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model," *Behavior and Information Technology* (23:6) 2004, pp 413-423.

Dinev, T., and Hart, P. "Internet privacy concerns and social awareness as determinants of intention to transact," *International Journal of Electronic Commerce* (10:2), Win 2005, pp 7-29.

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

DMA. Privacy Promise Member Compliance Guide. *Direct Marketing Association*. 2003, http://www.the-dma.org/privacy/privacypromise.shtml

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

Donaldson, T., and Dunfee, W.T. "Towards a Unified Conception of Business Ethics: Integrative Social Contracts Theory," *Academy of Management Review* (19), April 1994, pp 252-284.

Dunfee, W.T., Smith, N.C., and Ross, T.W.J. "Social Contracts and Marketing Ethics," *Journal of Marketing* (63), July 1999, pp 14-32.

Edelman, B. "Adverse Selection in Online "Trust" Certifications," Harvard University, 2006.

Etzioni, A. *The limits of privacy*, Basic Books, New York, 1999, pp. vii, 280 p.

Fornell, C., and Bookstein, F.L. "Two Structrual Equation Models: LISREL and PLS Applied to Customer Exit-Voice Theory," *Journal of Marketing Research* (19:11) 1982, pp 440-452.

Fusilier, M.R., and Hoyer, W.D. "Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation," *Journal of Applied Psychology* (65:5) 1980, pp 623-626.

Ganesan, S. "Determinants of Long-Term Orientation in Buyer-Seller Relationships," *Journal of Marketing* (58), April 1994, pp 1-19.

Hall, E., and Hall, M. *Understanding cultural differences*, Intercultural Press, Yarmouth, ME, 1990.

Havlena, W.J., and DeSarbo, W.S. "On the Measurement of Perceived Consumer Risk " *Decision Sciences* (22:4) 1991, pp 927-939.

Hofstede, G. *Culture's consequences*, Sage, Beverly Hills, CA, 1980.

Hofstede, G. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*, Sage, Longdon, 2003.

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

Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:12) 2000, pp 45-71.

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

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

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

Margulis, S.T. "Conceptions of Privacy - Current Status and Next Steps," *Journal of Social Issues* (33:3) 1977, pp 5-21.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. "An integrative model of organizational trust," *Academy. Management Review* (20:3) 1995, pp 709-734.

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

Metzger, M.J. "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce," *Journal of Computer-Mediated Communication* (9) 2004.

Metzger, M.J. "Communication Privacy Management in Electronic Commerce" *Journal of Computer-Mediated Communication* (12:2) 2007, pp 335–361.

Milberg, S.J., Smith, H.J., and Burke, S.J. "Information privacy: Corporate management and national regulation," *Organization Science* (11:1), Jan-Feb 2000, pp 35-57.

Milne, G.R., and Culnan, M.J. "Strategies for reducing online privacy risks: Why consumers read(or don't read) online privacy notices," *Journal of Interactive Marketing* (18:3) 2004, pp 15-29.

Morgan, R.M., and Hunt, S.D. "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing* (58:3) 1994, pp 20-38.

Norberg, P.A., Horne, D.R., and Horne, D.A. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs* (41:1), Sum 2007, pp 100-126.

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

Nunnally, J.C. *Psychometric Theory*, (2nd ed.) McGraw-Hill, New York, 1978.

Patil, S., and Kobsa, A. "Uncovering privacy attitudes and practices in instant messaging," in: *Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work*, ACM, Sanibel Island, Florida, USA, 2005.

Pavlou, P.A., and Gefen, D. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1) 2004, pp 37-59.

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

Petronio, S.S. "Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples," *Communication Theory* (1) 1991, pp 311–335.

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

Preston, J., and "Judge strikes down section of patriot act allowing secret subpoenas of internet data," in: *The New York Times, September 30*, 2004.

Prosser, W.L. "Privacy, a legal analysis," *California Law Review* (48:3) 1960, pp 338-423.

Rindfleisch, T.C. "Privacy, information technology, and health care," *Communications of the Acm* (40:8), Aug 1997, pp 92-100.

Roberts, J.M., and Gregor, I. "Privacy: A Cultural View," in: *Privacy,* J. Penncock and J. Chapman (eds.), Atherton Press, New York, 1971, pp. 199-225.

Schoeman, F.D. *Philosophical Dimensions of Privacy: an Anthology*, Cambridge University Press, Cambridge; New York, 1984.

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

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

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

Solove, D.J. *The digital person : technology and privacy in the information age*, New York University Press, New York, 2004, pp. xii, 283 p.

Solove, D.J. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3) 2006, pp 477-560.

Solove, D.J. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Yale University Press, New Haven, CT, 2007.

Stanton, J.M., and Stam, K. "Information Technology, Privacy, and Power within Organizations: A Merger of Boundary Theory and Social Exchange Perspectives," *Surveillance and Society* (2:Spring) 2003, pp 152-190.

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

Swire, P.P. "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in: *Privacy and Self-Regulation in the Information Age*, Department of Commerce, U.S.A., Washington, D.C., 1997, pp. 3-19.

Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W., and Fromkin, H.L. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology* (66:3) 1981, pp 308-313.

Venkatesh, V., Morris, G.M., Davis, B.G., and Davis, F.D. "User Acceptance of Information Technology: Toward A Unified View," *MIS Quarterly* (27:3) 2003, pp 425-478.

Wald, M. "Airline Gave Government Information on Passengers," in: *New York Times, January 18*, 2004.

Warren, S.D., and Brandeis, L.D. "The Right to Privacy," *Harvard Law Review* (4:5) 1890, pp 193-220.

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

Xu, H. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," *Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007)*, Montréal, Canada, 2007.

Xu, H., and Teo, H.H. "Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective," *Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004)*, Washington, D. C., United States, 2004, pp. 793-806.

Xu, H., Teo, H.H., and Tan, B.C.Y. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," *Proceedings of 26th Annual International Conference on Information Systems (ICIS 2005)*, Las Vegas, NV, 2005, pp. 897-910.

Yates, J.F., and Stone, E.R. "Risk appraisal," in: *Risk-taking behavior,* J.F. Yates (ed.), John Wiley & Sons, Chichester, England, 1992, pp. 49-85.

Zwick, D., and Dholakia, N. "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.