European Journal of Information Systems (2013) 22, 295–316
© 2013 Operational Research Society Ltd. All rights reserved 0960-085X/13
www.palgrave-journals.com/ejis/

RESEARCH ARTICLE

Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts

Tamara Dinev[1],
Heng Xu[2],
Jeff H. Smith[3] and
Paul Hart[1]

[1]Department of Information Technology & Operations Management, College of Business, Florida Atlantic University, Boca Raton, USA; [2]College of Information Sciences and Technology, Pennsylvania State University, University Park, USA; [3]Department of Decision Sciences and Management Information Systems, Farmer School of Business, Miami University, Oxford, USA

**Correspondence: Tamara Dinev
Department of Information Technology & Operations Management, College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA.
Tel: +1 (561) 297-3181;
Fax: +1 (561) 297-3043**

Abstract

Privacy is one of the few concepts that has been studied across many disciplines, but is still difficult to grasp. The current understanding of privacy is largely fragmented and discipline-dependent. This study develops and tests a framework of information privacy and its correlates, the latter often being confused with or built into definitions of information privacy *per se*. Our framework development was based on the privacy theories of Westin and Altman, the economic view of the privacy calculus, and the identity management framework of Zwick and Dholakia. The dependent variable of the model is perceived information privacy. The particularly relevant correlates to information privacy are anonymity, secrecy, confidentiality, and control. We posit that the first three are tactics for information control; perceived information control and perceived risk are salient determinants of perceived information privacy; and perceived risk is a function of perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations. The research model was empirically tested and validated in the Web 2.0 context, using a survey of Web 2.0 users. Our study enhances the theoretical understanding of information privacy and is useful for privacy advocates, and legal, management information systems, marketing, and social science scholars.

European Journal of Information Systems (2013) **22,** 295–316.
doi:10.1057/ejis.2012.23; published online 29 May 2012

Keywords: privacy; anonymity; secrecy; confidentiality; control; risk

**Received: 21 November 2009
Revised: 31 January 2011
2nd Revision: 27 September 2011
3rd Revision: 6 March 2012
Accepted: 10 March 2012**

Introduction

Privacy has been studied for more than 100 years in almost all spheres of social science, most notably law, economics, psychology, management, marketing, and management information systems. Amazingly, however, it is also a concept that 'is in disarray [and n]obody can articulate what it means' (Solove, 2006, p. 477). Margulis (1977) noted the variety of conceptualizations of privacy and the disagreement among scholars on what privacy is. The lack of a clear, concrete, measurable, and empirically testable conceptualization of privacy affects many aspects of the society – the vagueness of the concept fails to guide adjudication and lawmaking (Bennett, 1992; Solove, 2006), as well as formation of government and organizational management policies and practices regarding the privacy and security of employees, consumers and clients, and citizens.

Numerous attempts have been made by scholars to define and develop a coherent understanding of privacy and to integrate the different perspectives from different fields. The picture of privacy that emerges is fragmented and usually discipline-specific. The concepts, definitions, and relationships are inconsistent and neither fully developed nor empirically validated. In Law, many scholars defined privacy as a 'right' or 'entitlement' (e.g., Warren & Brandeis, 1890); others from other disciplines, including philosophy and psychology, define it as a 'state of limited access or isolation' (e.g., Schoeman, 1984); and yet another group of scholars, particularly from the social sciences and information systems used 'control' as a definition of privacy (Westin, 1967; Culnan, 1993). Privacy 'has been described as multidimensional, elastic, depending upon context, and dynamic in the sense that it varies with life experience' (Xu *et al*, 2011, p. 799). And yet, 'much of the work … has come from groups with a single point of view (e.g., civil liberties advocates, trade associations) and/or a mission that is associated with a point of view (e.g., regulatory agencies)' (Waldo *et al*, 2007, p. vii). Many overlapping concepts, such as intrusion, deception, secrecy, anonymity, have been built into the definition of privacy and have added to the confusion (Margulis, 2003a, b). Moreover, very few have been empirically measured or tested. As Solove (2006, p. 479) notes, 'privacy seems to be about everything, and therefore it appears to be about nothing'. In its report on the status of privacy research, the Committee of Privacy in the Information Age at the National Research Council of the National Academy of Sciences notes that it was 'struck by the extraordinary complexity associated with the subject of privacy', and that 'the notion of privacy is fraught with multiple meanings, interpretations, and value judgments' (Waldo *et al*, 2007, p. x). Solove (2006) also notes that many discussions about privacy are targeted toward people's fears and anxiety to the extent that the expression 'this violates my privacy' or 'my privacy should be protected' has become more a product of instinctive recoil void of meaning rather than a well-articulated statement carrying reason and a specific relevance. The difficulty in articulating what constitutes privacy, and thus what constitutes harm to privacy, translates into policymaker's and the courts' difficulty in defending privacy interests. This further leads to dismissing cases and disregarding organizational and government problems (Solove, 2006).

Given these challenges and murky conceptual waters, our study attempts to build a more rigorous, empirically testable framework of privacy and its correlates, which have often been confused with or built into the definitions of privacy *per se*. The specific research goals of our study are to (i) identify the appropriate conceptualization of privacy and the correlates that previously have been closely associated or confused with privacy; and (ii) develop empirical measures and test a nomological model of these correlates to examine their relationship to privacy and their distinctness from it.

We believe that our study is timely and needed. The dynamic globalization of the economy and information technology (IT), and the ubiquitous distributed storage and sharing of data puts the issue of information privacy at the forefront of society policies and practices. This development contributes to the urgency and need for finding a better and common framework for privacy, and information privacy in particular, that can be used across multiple areas that affect social life.

The focus of our paper is information privacy, although we found that in public and political discourse, as well as in various research streams, a clear distinction between physical and information privacy is not made. For example, polls and surveys ask about 'privacy' rather than 'information privacy'. In many disciplines, including law, marketing, management information systems and economics, physical privacy concepts and definitions are directly applied to information privacy, providing continuity in the nomological models associated with information privacy (Smith *et al*, 2011). Analogously, we will use earlier, general privacy concepts to derive and analyze information privacy-specific concepts. In an attempt to be as clear as possible in our framework, throughout the remainder of this paper we will use the term 'privacy' to refer to 'information privacy'. We will refer to 'general privacy' when we use previous studies and theories that are relevant to information privacy, but did not specify whether the term 'privacy' concerns physical or information privacy.

The overarching models guiding this process are the general privacy theories of Altman (1974, 1975), Westin (1967), and Margulis (1977, 2003a, b; see Margulis, 2003a for a review) and the general privacy taxonomy developed by Solove (2006). Each of these identifies a set of privacy dimensions but to the best of our knowledge have not been empirically validated. In addition, we employ the Zwick & Dholakia's (2004) conceptualization of identity management that will help us rigorously define and operationalize the tactics of information control we will identify in the study. We conducted a survey study to test the research model.

In what follows, we first describe the literature review for our research, presenting the overarching theories and privacy definitions that guide the development of the research model. Then we develop the logic underlying the research model that presents the process through which individuals form privacy perceptions. This is followed by a description of the research methodology, choice of context to empirically test our model, and our findings. The paper concludes with a discussion of the results and implications of the findings.

The theory – how information control and risk affect privacy

The concept of privacy – literature review

Scholars in different fields have examined the concept of general privacy including psychology (e.g., Altman, 1975; Laufer & Wolfe, 1977), human resources (Tolchinsky *et al*, 1981; Stone & Stone, 1990), sociology (e.g., Etzioni, 1999), law (e.g., Rosen, 2000), political science (e.g., Westin, 1967), marketing (e.g., Goodwin, 1991), and management information systems (e.g., Mason, 1986; Smith, 1994; Culnan & Armstrong, 1999). Such rich theoretical ground has led to the observation that there is a lack of consensus on what general privacy means: 'theorists do not agree … on what privacy is or on whether privacy is a behavior, attitude, process, goal, phenomenal state, or what' (Margulis, 2003b, p. 17). Indeed, there is a stream of research for each of these perspectives. Perhaps, the most famous and the oldest is the general 'privacy as a right' concept, first defined by Warren & Brandeis (1890) as the 'the right to be left alone'. This definition has been central to legal interpretations and court decisions, as well in the political discourse, where the term 'privacy' has been used to refer to 'physical privacy in the home or office, the ability to make personal reproductive decisions without interference from the government, freedom from surveillance, or the ability to keep electronic communications and personal information confidential' (Waldo *et al*, 2007, p. 1). Congressional law committees have taken the defeatist approach to legally defining general privacy (Young, 1978) and concluded that the concept of general privacy cannot be satisfactorily defined. The need was felt, however, to elaborate on the 'right to (general) privacy' concept introduced by Warren & Brandeis (1890). Thus, in subsequent treatments, general privacy was regarded as a 'right' but has been expanded to include a number of so-called (general) 'privacy interests' (Flaherty, 1979; Milberg *et al*, 2000). These privacy interests include control, confidentiality, solitude, anonymity, and secrecy and in an empirical sense, can be considered dimensions or antecedents of privacy. However, as we will point out later, in many studies any of these dimensions have been equated with privacy, from which the main current confusion arises.

Psychologist's view of general privacy is that of a feeling, an emotion (Young, 1978) rather than 'right'. They argue that often there appears to be no logical reason why a person should feel that his or her general privacy has been violated and yet that is his or her perception. Thus, psychologists conclude that 'privacy and gregariousness are both human instincts and relate to all the higher forms of animal behavior' (Young, 1978, p. 3; see also Altman, 1974).

Economists, by contrast, have defined privacy as a value, in economic terms, 'both in its role in the information needed for efficient markets and as a piece of property' (Waldo *et al*, 2007, p. 1). Sociology researchers approach privacy from the perspective of the collection and use of personal information in the context of 'power and influence between individuals, groups, and institutions within society' (Waldo *et al*, 2007, p. 1). Thus, the sociology produced the control-centered definitions of general privacy (Westin, 1967; Altman, 1974; Margulis, 1977). From this perspective, general privacy is a struggle for control between the individual and society (Cate, 1997). Philosophers interpreted general privacy as a 'state' (of limited access or isolation) (Schoeman, 1984). Each of these definitions carries a set of dimensions that point to the multidimensional nature of general privacy.

Westin (1967) sees general privacy as 'the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity and reserve'. There are four 'states' of general privacy posited in Westin's theory: *solitude, intimacy, anonymity, and reserve* (it is important to note that, in the end, Westin's definition does arrive at the 'state' interpretation of general privacy). Several researchers developed measurements and empirically examined Westin's states of general privacy (Marshall, 1974; Pedersen, 1997), whereas others developed more specialized general privacy scales. Some of these scales measure the above mentioned states of general privacy and through their values attempt to assess general privacy itself (e.g., the concealment scale of Cramer & Barry (1999)). Difficulties, however, arise because of a lack of a clear concept about what general privacy is in the first place. For example, Pedersen (1997) developed measures for Solitude, Isolation, Anonymity, Reserve, Intimacy with Friends, and Intimacy with Family. The researcher then introduced these constructs as 'types of privacy' (p. 147) interchangeably equating them with 'types of privacy behaviors' and 'psychological functions of privacy'.

The problem is not merely confusion in terminology but reflects the scholars' struggle to fundamentally understand what exactly general privacy is – behavior, state, function, or feeling – and evidently these cannot be confused or interchanged. Several other difficulties arose with the above measures when other scholars argued that these states are actually distinct factors that are more antecedents than direct measures of general privacy. Underlining the normative element of general privacy that distinguishes it from these states, they argue that general privacy is not synonymous with solitude, secrecy, and autonomy (Cate, 1997). More factors were added to describing the states of general privacy, such as secrecy (embedded in Westin's theory but not defined, Tefft, 1980; McLean, 1995; Margulis, 2003a; Solove, 2004), transparency (Brin, 1998), and confidentiality (Young, 1978; Solove, 2006).

Altman's (1975, p. 24) theory of general privacy revolves around the concept of control; general privacy is defined as 'the selective control of access to the self'. Altman also distinguishes between actual and desired general privacy. The first indication of general privacy perception in a given situation depends on the individual's desires (expectations). He thus introduces levels of general privacy: optimal (desired = actual), crowding (desired < actual), and isolation (desired > actual) (see Margulis, 2003a).

Each discipline has argued its angle on the concept of general privacy, but most developed verbose descriptions without quantitative measurement. Management information systems research undertook the task of developing privacy construct measurements that can be used in quantitative models to test relationships (Smith *et al*, 2011). Following Altman (1974, 1975), many management and management information systems studies equated privacy with control. However, recent empirical evidence has shown that while control is a major factor in forming individual's privacy concerns, it is not identical to privacy (Dinev & Hart, 2004, 2006; Xu, 2007). Schoeman (1984) and Laufer & Wolfe (1977) also described a number of counterexamples that pose difficulties in equating privacy with control.

Due to the inconsistencies in conceptualizing and measuring privacy *per se*, much behavioral research on privacy uses *privacy concerns* as a proxy for *privacy*. An extensive body of literature examines privacy concerns (for references, see, e.g., Dinev & Hart, 2006 or Smith *et al*, 2011) because these are also the proxy used to measure privacy attitudes in opinion polls and by consumer research firms and provide a good connection with individuals' feelings about privacy. Important studies that have contributed to our understanding of privacy concerns and their implications for individual's behavior include those of Culnan (1993), Smith *et al* (1996), Culnan & Armstrong (1999), Milberg *et al* (2000), Malhotra *et al* (2004), Dinev & Hart (2006) and many others. Smith *et al* (1996) developed an instrument, Concerns For Information Privacy, to measure individuals' concerns toward organizational privacy practices, including four dimensions: collection, errors, secondary use, and unauthorized access to information.

The two main characteristics that distinguish MIS research are the conceptualization of privacy concerns rather than privacy, and the quantitative approach to measuring and modeling privacy concerns (for a comparative matrix of the MIS research on privacy, see Xu *et al*, 2011). These include the organizational information practice aspect of privacy concerns (Smith *et al*, 1996) and the individual privacy concerns (among MIS studies, see, e.g., Culnan & Armstrong, 1999; Belanger *et al*, 2002; Culnan & Bies, 2003; Malhotra *et al*, 2004; Dinev & Hart, 2005, 2006; Liu *et al*, 2005; Awad & Krishnan, 2006; Poindexter *et al*, 2006; Hui *et al*, 2007; Chellappa, 2008; Dinev *et al*, 2008; Son & Kim, 2008).

In this study, however, we will consciously stay away from privacy concerns as the commonly adopted proxy to privacy. Instead, we will attempt to seek a rigorous definition of and antecedents to privacy. We do this for three reasons: first, while a good proxy for privacy, we believe that privacy concerns are not identical to privacy – indeed, one may have high concerns about his or her privacy and yet it may be that his or her privacy may have not been violated, and vice versa. Although we do not yet have a rigorous definition of privacy, it is clear that it is distinct from privacy concerns. The second reason to avoid privacy concerns as a construct in our study is that we did not find it in the aforementioned privacy theories (and these are leading social theories of privacy), nor did we find concerns as a possible dimension of privacy *per se*. The lack of connection of the 'privacy concerns' – focused MIS privacy research with leading theories from other disciplines contributes to the problem of the fragmentary understanding of privacy. Finally, we share Young's (1978) observation that privacy concerns carry a negative connotation of the concept of information and general privacy, and thus may be inadequate if general privacy should be regarded as potentially valuable to any human being and society as a whole.

Theoretical model of privacy and its correlates – integrative approach

Perceived privacy as a dependent variable. As shown in Figure 1, the dependent variable (DV) of our research model is perceived privacy. First, we note that in most of the aforementioned theories, the most common theme that emerges is that privacy is a *state* in which an individual is found in a given situation at a given moment of time. This consensus emerges regardless of how the authors begin their conceptualization of privacy or whether basic assumptions varied. For example, Westin (1967) refers to 'states of privacy' and both Altman (1974, 1975) and Westin (1967) discuss 'state of control' and 'state of limited access' (Margulis, 2003a, b). Also, Warren and Brandeis's (1890) definition of general privacy as a 'right to be left alone' implicitly refers to a state – of being left alone. Similarly, MIS researchers have referred to privacy as a state. For example, Dhillon & Moores (2001, p. 2) defined Internet privacy as 'the seclusion and freedom from unauthorized intrusion', and Di Pietro & Mancini (2003, p. 78) defined privacy as 'the freedom of not having someone or something to interfere in our life without our permission'. At some point, it seems, and sometimes unintentionally, most researchers reach the need to use the word 'state' to describe privacy. This latter observation aligns well with the dictionary definition of 'state', namely 'the condition of a person or

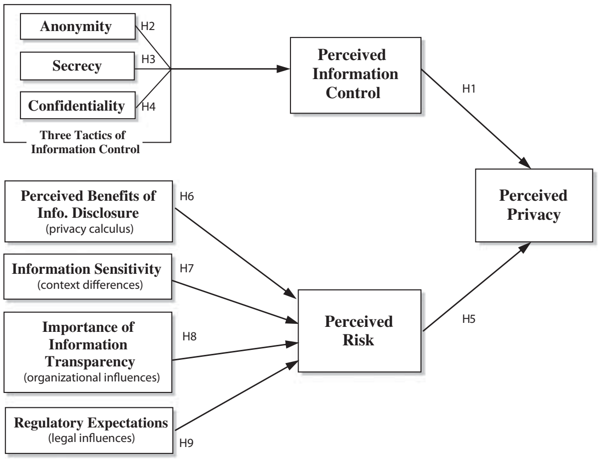

Figure 1 Research model.

thing, as with respect to circumstances or attributes', 'particular condition of mind or feeling'.

Since, per definition, perception is the process of attaining awareness or understanding of mental and sensory information, an individual's evaluation of his or her own mental and or/physical state of being is carried through his or her perceptions (Sternberg, 2003). Thus, if we assume that, in most general terms, privacy can be considered as a *state,* the empirically testable definition of privacy will be the 'perceived (state of) privacy'. We thus adapt the Schoeman's (1984) conceptual definition of privacy in general to information privacy: perceived privacy is an individual's self-assessed state in which external agents have limited access to information about him or her.

Research Model. While each of the prior theories reviewed above focuses on different theoretical aspects of the same underlying phenomenon, in our attempt to clarify the intertwining concepts of privacy and its related factors, we see opportunities for consolidation and integration. Evaluating evidence from the perspective of a single theory may lead to falsification of that theory and creates a major scientific challenge (Cote, 2002). The goal of theory integration is to identify the commonalities in multiple theories about the focal phenomenon and produce a synthesis that is superior to any of the component theories (Akers, 2001). However, exactly how the theories should be integrated seamlessly into a better theory is far from clear and we do not claim to have found the exclusive, unique solution. Rather, we rely on the research advances and further scholarly contributions for our model to be further developed, clarified, and enhanced.

The literature review of MIS and other disciplines leads us to propose a research model that integrates three conceptual frameworks. At its core lies the calculus framework of privacy incorporating the risk-control interplay (Culnan & Armstrong, 1999; Dinev & Hart, 2006). The calculus perspective of privacy has been described as 'the most useful framework for analyzing contemporary consumer privacy concerns' (Culnan & Bies, 2003, p. 326). The implicit understanding is that privacy is not absolute (Klopfer & Rubenstein, 1977), but based on a cost-benefit analysis, that is, a 'calculus of behavior' (Laufer & Wolfe, 1977, p. 36). We integrate this core with recently advanced control and risk theories that aim to explain how perceptions of risk and control are formed in individuals regarding their personal information. For the control aspect, we build on Zwick & Dholakia's (2004) conceptualization of identity management and identify three different tactics that consumers apply to control the flow of their personal information: anonymity, secrecy, and confidentiality. For the risk aspect, we base our framework mainly on Fusilier & Hoyer (1980), Petronio (2002), and Culnan (e.g., Culnan & Armstrong, 1999; Culnan & Bies, 2003). All of these studies address the individual's sense of risk when considering the consequences of information disclosure; each of them develops a set of risk factors although none offers an integrated, comprehensive treatment of risk. We have integrated the most salient risk factors shown to affect perception of risk and propose that an individual's perceived risk is a function of the expected outcomes of information disclosure, together with considerations for context (i.e., information sensitivity), organizational (i.e., importance of information transparency), and legal (i.e., regulatory expectations) influences. Figure 1 presents the research model.

Information control and risk – the backbone of privacy The level of privacy concerns an individual develops has been shown to lead to decision making whether to disclose personal information (among MIS studies, see, e.g., Culnan & Armstrong, 1999; Belanger *et al*, 2002; Culnan & Bies, 2003; Malhotra *et al*, 2004; Dinev & Hart, 2005; Liu *et al*, 2005; Awad & Krishnan, 2006; Dinev & Hart, 2006; Dinev *et al*, 2006, 2008; Poindexter *et al*, 2006; Hui *et al*, 2007; Chellappa, 2008; Son & Kim, 2008). In comparing the work of Westin and Altman and those whose research is based on their theories from a range of disciplines, Margulis (2003b, p. 415) identified common core elements: (general) '[p]rivacy involves control over transactions (interactions, communications) that regulate access to self and that, as a consequence, reduce vulnerability and increase decisional and behavioral options'. This definition reflects the view of privacy as a complex construct, that is, the dichotomy between the individual and others (Kelvin, 1973) and captures the two most important factors of privacy: (i) control over disclosure of personal information, and (ii) the notion of privacy risk. Furthermore, the calculus framework of general privacy (e.g., Dinev & Hart, 2004, 2006) also underscores the risk-control interplay. Both risk and control have been shown to operate as privacy-borne beliefs related to the potential consequences of information disclosure. Thus, based on the literature, we identify the two major factors that directly account for the perceived privacy: perceived information control and perceived risk. Below, we present the theoretical foundation for the control and risk constructs, and their relationship with perceived privacy, and the corresponding hypotheses.

Perceived information control As discussed above, the element of control has been identified as an important factor of privacy. Laufer & Wolfe (1977, p. 39) made one of the strongest arguments for separating control from the concept of privacy: 'the dimensions of the privacy phenomenon are conceptually distinct from control/choice, which is a mediating variable'. Therefore, control should be a related but separate construct from privacy, and control and privacy should be positively related (see also Dinev & Hart, 2006).

In this research, we conceptualize information control as a perception and define it as an individual's beliefs in one's ability to determine to what extent information about the self will be released onto the Web 2.0-related sites. Prior literature differentiates between two types of control important for the privacy context: control over information disclosure and control over information use once the information has been obtained (Culnan & Armstrong, 1999; Spiekermann, 2005). Mostly, Web 2.0 operators address the first dimension by offering granular privacy settings (Hoadley *et al*, 2010), which allow limiting accessibility of one's personal information with regard to other members and third parties. For example, Facebook users can specify their privacy preferences on who can see their profiles and personal information, who can search for them, how they can be contacted, what stories about them get published to their profiles and so on. It has been suggested that individuals tend to have a lower level of privacy concerns when they have a sense of information control (Culnan & Armstrong, 1999). Several privacy studies suggest that the loss of information control is central to the perception of privacy invasion (Milne & Boza, 1999; Phelps *et al*, 2000; Sheehan & Hoy, 2000). Accordingly, we hypothesize that perceived information control is strongly related to perceived privacy.

H1: *Perceived information control positively affects perceived privacy.*

Tactics of information control Zwick & Dholakia (2004) propose a theoretical framework on identity management, wherein digital representation of an individual is determined by the *amount* and *accuracy* of the personal information collected. They further argue that attempts to regain control over one's identity require tactics that limit accessibility to one's personal information with regard to other members and third parties. That is, 'as the law of the place becomes dominated by companies' data collection strategies, consumers try to devise tactics that allow them to control either the amount or the accuracy (or both) of personal information that ends up in electronic databases' (Zwick & Dholakia, 2004, p. 35).

Zwick & Dholakia's (2004) conceptual framework identifies three different tactics that consumers apply to manage the externalization of their personal information: anonymity, secrecy, and confidentiality (Table 1). On the basis of the proposed definitions and the direct relationship between perceived information control and perceived privacy, we posit that these tactics of information control are actually mechanisms for maintaining the desired state of privacy which is achieved through control over the information exchange between the individual and the world outside his or her information boundaries (Margulis, 2003a). Thus, we propose that these tactics of information control (i.e., anonymity, secrecy, and confidentiality) will positively influence control perceptions in our model.

Anonymity. Using the framework in Table 1, anonymity of (Cell 1) is the tactic to conceal a person's identity (Camp, 1999; Marx, 1999; Zwick & Dholakia, 2004; Rensel *et al*, 2006; Qian & Scott, 2007) and it exists when an individual is acting in a way that limits the availability of identifiers to others. In the IT context, anonymity is often shaped by the features and affordances of the privacy enhancing technologies (Qian & Scott, 2007). Technical anonymization mechanisms offer different degrees of anonymity (Kobsa & Schreck, 2003) with the options for individuals to be totally anonymous, pseudonymous, or identifiable (Nissenbaum, 1999; Qian & Scott, 2007). Users' ability to stay anonymous can be expected to lead to more extensive and frank interaction, hence to more and better data disclosure about themselves, and thus to better personalization and aggregate data collection since they feel more information control. Anonymity, therefore, is defined in our study as the ability to carry out an externalization tactic that can conceal an individual's real identity (Turkle, 1995; Zwick & Dholakia, 2004).

In Web 2.0 and social networks such as Facebook or Linkedin, users are participating to connect with colleagues, friends, classmates or fans, and thus, they reveal their true identities. However, users on these sites are more often performing than revealing their genuine thoughts and feelings (Turkle, 2011). To participate fully and contribute genuine thoughts and ideas in the social reality of Web 2.0 communications (blogging, tagging, user-driven ratings and reviews, etc.), they would need to stay anonymous. Anonymity will often be regarded as necessary if the real identity is to be protected

Table 1 Tactics of information control

	Accuracy of personal information	
	Low	*High*
Amount of personal information externalized		
Low	SECRECY 2 Sharing of little and potentially inaccurate information Avoid digital representations of the real self	CONFIDENTIALITY 3 Externalization of restricted but highly accurate information
High	ANONYMITY 1 Sharing of personal information with concealing a consumer's real identity	NO CONTROL 4 Disclose large amount of personal information Reveal an accurate representation of the self

Source: Zwick and Dholakia (2004).

from unwarranted and biased profiling (Clarke, 1988; Zwick & Dholakia, 2004). In other words, the individual creates 'a multiplication of consumer identities as a form of camouflage against the strategy of surveillance of the proprietary powers' (Zwick & Dholakia, 2004, p. 36). Therefore, when consumers are provided with the means to conceal their identities in various Web 2.0 communications, their perceptions of information control are likely to increase. Hence, we hypothesize:

H2: *Anonymity positively affects perceived information control.*

Secrecy. Cell 2 is secrecy, which has been defined as intentional concealment of information (Tefft, 1980; Bok, 1989). Secrecy usually expresses the intention 'toward the sharing of little and potentially inaccurate information' (Zwick & Dholakia, 2004, p. 35). Secretive withholding of personal information is then 'regarded as an attempt to block any digital representation from emerging in the network' (Zwick & Dholakia, 2004, p. 35). Secretive consumers do not actively share information and 'seek to avoid digital representations of the real self, accurate or not' (Zwick & Dholakia, 2004, p. 36). People keep some information secret because the information may have the potential to result in a high level of risk if known by others. Consequently, people are likely to desire the means to conceal the secret information. As Bok (1989) states:

> To keep a secret from someone … is to block information about it or evidence of it from reaching that person, and to do so intentionally; to prevent him [or her] from learning it, and thus, from processing it, making use of it or revealing it. (p. 5)

We thus define secrecy as the ability to carry out an externalization tactic that involves concealment of information, which enables individuals to manipulate and control environments by denying outsiders vital information about themselves (Tefft, 1980). When consumers do not allow much accessibility to certain personal information, they maintain high levels of control over this information. Thus, secrecy is directly related to control.

H3: *Secrecy positively affects perceived information control.*

Confidentiality. Cell 3 is confidentiality and mainly concerns 'the externalization of restricted but highly accurate information to a specific company' (Zwick & Dholakia, 2004, p. 35). It connects to the security aspect of private information that is stored in databases (Camp, 1999), which 'restricts the information flow in terms of what is externalized and who gets to see it' (Zwick & Dholakia, 2004, p. 35). Concerns for confidentiality usually occur at the stage in which private data has been disclosed and stored in database. Research has shown that threats to data confidentiality include: (i) accidental disclosures, (ii) insider curiosity, (iii) insider subordination, and (iv) unauthorized access (Rindfleisch, 1997; Earp & Payton, 2006). Therefore, by necessity, confidentiality involves the recipient of the private information, as well as third parties to a greater extent than anonymity and secrecy do. That is, the individual has to rely on these other parties to keep personal information confidential more so than in the case of anonymity and secrecy tactics. Camp (1999) has noted that confidentiality implies that the data and the information they represent must be protected and their use confined to authorized purposes by authorized people. We thus define confidentiality as the perceived ability to carry out an externalization tactic that restricts the information flow in terms of what is disclosed and who gets to see it (Zwick & Dholakia, 2004). When confidentiality is assured by preventing unauthorized access, consumers may perceive higher levels of control over their personal information. Thus, we hypothesize that confidentiality is positively related to perceived information control.

H4: *Confidentiality positively affects perceived information control.*

Perceived risk enters a decision-making process when situations of that process create a sense of uncertainty, discomfort, and/or anxiety (Dowling & Staelin, 1994), such as when psychological discomfort triggers feelings of uncertainty (Moorman *et al*, 1993), anxiety causes pain (Taylor, 1974), or when there is cognitive dissonance (Festinger, 1957). The notion of risk is related to privacy and shares some of the latter's complexity. Introduced separately from privacy, risk has been described as the perceived potential risk that occurs when personal information is revealed (Raab & Bennett, 1998; Pavlou, 2002). However, it has also been described as a possible consequence of concealing information, when disclosure would be important for attaining a positive outcome (Petronio, 2002). Fusilier & Hoyer (1980) and Petronio (2002) have argued that the perceived state of privacy is determined by an individual's sense of risk, and recently Krasnova *et al* (2009) have identified perceived privacy risk as a main factor predicting personal information disclosure in online social networks. Applying their findings to the context of this research, we define the perception of risk as the user's perceived expectation of suffering a negative outcome as a consequence of online disclosure of personal information.

Users may perceive two kinds of risks if their personal information is not used fairly or responsibly (Goodwin, 1991; Culnan, 1993; Smith *et al*, 1996). First, a user may perceive that her privacy is invaded if unauthorized access is made to her personal information in the absence of appropriate controls. Second, as computerized information may be easily distributed and reused, a user may perceive a relatively high risk that the information she has provided is being put into secondary use for unrelated purposes without her knowledge or consent (Culnan & Armstrong, 1999). In the context of Web 2.0, improper information practices would result in the mining and mapping of personal data to make an individual's behavior more visible. Furthermore, users who often reveal their true identities on some Web 2.0 sites (e.g., social networking sites) expose their personal information to potential misuse (Gross & Acquisti, 2005). Therefore, when individuals perceive that there will be uncertainty or negative consequences of their information disclosure, they will be feeling that they have less privacy overall. Hence, we hypothesize:

H5: *Perceived risk negatively affects perceived privacy.*

Predictors of perceived risk The literature is abundant with studies of factors that affect perceived risk (e.g., Fusilier & Hoyer, 1980; Culnan & Armstrong, 1999; Pavlou, 2002; Petronio, 2002; Culnan & Bies, 2003). For example, in a recent study about the effect of interactivity of an e-service on perceived risk, Featherman *et al* (2011) suggest that richer media with instant feedback and multiple cues better convey performance efficacy and promised benefits helping consumers improve their understanding of an online service through an interactive preview. Thus, the perceived risk of utilizing the e-service should be lessened. In another study, Luo *et al* (2010) used Featherman *et al*'s (2011) multifaceted risk model and found that perceived risk predictors include trust, self-efficacy, and structural assurances. Each of the studies explores a set of risk factors, but none offers an integrated, comprehensive treatment of risk. On the basis of our literature review, we have identified the most salient risk factors to affect perceptions of risk. We integrate these factors in our model and propose that an individual's perceived risk is a function of perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations.

Perceived Benefits of Information Disclosure. The notion of privacy calculus assumes that there is a consequential tradeoff of costs and benefits salient in an individual's privacy decision making. Overall, the calculus perspective of privacy suggests that when asked to provide personal information to service providers or companies, consumers perform a cost-benefit analysis (Culnan, 1993; Milne & Gordon, 1993; Sheehan & Hoy, 2000; Dinev & Hart, 2006) and they 'are assumed to behave in ways that they believe will result in the most favorable net level of outcomes' (Stone & Stone, 1990, p. 363). Consequently, we argue that consumers are more likely to accept the potential risks that accompany the disclosure of personal information as long as they perceive that they can achieve a positive net outcome (i.e., benefits exceed the costs of disclosure) (Culnan & Bies, 2003). Hence, when a positive outcome of information disclosure is anticipated, risk beliefs are hypothesized to decrease:

H6: *Perceived benefits of information disclosure negatively affect perceived risk.*

It is important to note that privacy decisions involve more than a cost-benefit analysis as discussed above. Information disclosure entails considerable uncertainties, which are also subject to the opportunistic behaviors of online companies or Web sites. In this research, we further propose that the perception of risk is also a function of the level of information sensitivity, importance of information transparency, and regulatory expectations.

Information Sensitivity. Support for individuals having different information-related beliefs as a consequence of different information experiences or interacting with the external environment is suggested by prior general and information privacy literature (Stone *et al*, 1983). It has been shown that the levels of privacy needs and concerns are dependent on the type of information collected and used by an organization (Milne & Gordon, 1993; Phelps *et al*, 2000; Sheehan & Hoy, 2000; Malhotra *et al*, 2004). Malhotra *et al* (2004) refer to this information attribute as 'information sensitivity' (see also Phelps *et al*, 2000). For example, it was reported that consumers found information such as medical data, financial information, and personal identifiers (e.g., social security numbers) to be much more sensitive than demographic information, lifestyle habits, and purchase behavior (Vidmar & Flaherty, 1985; Phelps *et al*, 2000; Sheehan & Hoy, 2000; Metzger, 2004; Dinev & Hart, 2007). On the basis of Malhotra *et al* (2004), we define information sensitivity as a personal information attribute that informs the level of discomfort an individual perceives when disclosing specific personal information to a specific external agent (in our case, a Web site). We believe this definition is in accordance with the dictionary connotation of 'sensitive': when pertaining to an object, it means requiring tact or caution; delicate; touchy, like in 'sensitive topic', that is, having potential to invoke a certain level of discomfort in people.

Since certain domains of life are considered more private than others (Phelps *et al*, 2000), all things being equal, individuals will perceive a higher level of risk for their disclosure of more sensitive information than they do for their disclosure of less sensitive information (Li *et al*, 2011). Malhotra *et al* (2004) found that more sensitive information has a more negative effect on consumer's attitudes and intentions toward revealing personal information. In particular, they found that it will increase the consumer's risk beliefs. In the context of Web 2.0, it has been shown that the majority of users are selective in terms of the type of personal information they disclose online (Acquisti & Gross, 2006). For example, for the online social networks, most would publish their sexual orientation, political views, and birthday but conceal address, phone numbers, and class schedules (Acquisti & Gross, 2006). Thus, when the information requested is perceived as sensitive, risk perceptions are hypothesized to increase:

H7: *Information sensitivity positively affects perceived risk.*

Importance of Information Transparency. More and more users demand to know what type and how much information is collected about them, how is it stored, and to whom it is distributed or sold. Company's transparency about the usage, storage, and sharing of the personal data inform an individual's 'reasonable expectation of privacy' (Waldo *et al*, 2007) (i.e., the expectation of how the information will be collected and handled by the organizations). On the basis of the Utility Maximization Theory, Awad & Krishnan (2006) showed the importance of a company's information transparency. The results of their study indicated that customers who desire greater transparency for information handling are less willing to be identified. In this research, the importance of information transparency is defined as the consumer-rated importance of notifying the consumers what types of information a firm has collected about them, and how that information is going to be used (Stone *et al*, 1983; Awad & Krishnan, 2006). The hypothesized relationship between the importance of information transparency and perceived risk is supported by Awad & Krishnan (2006), who found that privacy beliefs were significantly related with individuals' expectations of the organization's information-handling practices. Customers who desire greater information handling transparency perceive greater risk, and thus are less willing to be profiled (Awad & Krishnan, 2006). That is to say, users who rate information transparency as important are more aware of risk in disclosing personal information:

H8 *Importance of information transparency positively affects perceived risk.*

Regulatory Expectations. As Smith *et al* (2011, p. 1001) pointed out, 'skepticism about the effectiveness of industry self-regulation in protecting consumer privacy has resulted in privacy advocates and consumers clamoring for strong and effective legislation to curtail rampant abuses of information by firms'. In the context of privacy, the regulatory approaches can decree the type of personal information merchants are allowed to collect from individuals, sometimes with their consent, as well as the ways with which stored personal information should be protected against misuse (Swire, 1997). Through enforcement agencies, the government can catch offenders and determine penalties for merchants when violations occur. Such punishments can also deter attempts to misuse stored personal information (Culnan & Bies, 2003; Xu *et al*, 2010). It follows that users who expect more restrictive privacy regulations are likely to be more concerned about the risk of information disclosure. Thus, we hypothesize that user expectations of privacy laws will be positively associated with perceptions of risk.

H9: *Regulatory expectations positively affect perceived risk.*

Control variables

Prior research on privacy suggests that a number of additional factors should be included as control variables because of their potential influence on our research model. Because our primary theoretical focus is not on them or there is no sufficient theoretical argument we can make to include them in our model as actionable variables, we include them as control variables, to eliminate the variance explained by them. They are gender, age, and weekly Web usage.

Research method

All social research involves creating a theory, which we did in the previous section and then designing a method to test the hypotheses involving actual collection of data. The methods can be observations or controlled experiment. The observation method can be interpretive in nature (choosing one or more specific case studies) or positivist involving quantitative approaches of statistical testing (Straub *et al*, 2004). The former is an appropriate method when processes and policies are described. The latter is the best approach when behavior and attitudes are explored from large general populations. It also involves operationalization (measurement of variables) and statistical validation of the relationships. Since our study is about behaviors and attitudes, we adopted the survey approach.

Choosing a context for testing the theoretical model

In contrast to most privacy research which was conducted in the conventional Web context (e.g., Rust *et al*, 2002; Stewart & Segars, 2002; Malhotra *et al*, 2004; Dinev & Hart, 2006), we empirically test the research model in an understudied Web 2.0 context. Prominent Web 2.0 features that support the creation and consumption of user-generated contents, such as blogging (e.g., Blogger), tagging (e.g., del.icio.us and Flickr), user-driven ratings (e.g., Digg), and social networking (e.g., Facebook and MySpace) have a number of characteristics that make them particularly suitable for examining the research model. First, Web 2.0 represents a shift from a World Wide Web that is 'read only' to a Web that has been described as the 'Read Write Web' (Gillmor, 2007). Consequently, Web 2.0 provides user-centered platforms for information sharing, information publishing, collective editing and collaboration, is becoming a prevalent phenomenon globally (eMarketer, 2007). The explosion of Web 2.0 technologies creates the opportunity for a plethora of niche markets within the media landscape that were expected to generate US$4.3 billion by 2011, more than four times what Web 2.0-related sites generated in 2007 with more than 70 million users (eMarketer, 2007). Second, despite the presence of some privacy norms and regulations, there are relatively few well-established institutional rules and contracts governing Web 2.0 technologies, and this give rise to opportunism.

Third, in a context characterized by active user participation and user generated content, privacy concerns are particularly salient because a larger volume of user digital footprints could be potentially accessible to the public. As one recent PEW survey pointed out, the vast array of data that makes up 'personal information' in the age of Web 2.0 are nearly impossible to quantify or neatly define (Madden *et al*, 2007). Users of Web 2.0 applications often act in a way that the application can observe and record, the potential knowledge in that action can be released onto the Web, and made available to everyone. Web 2.0 brought the voluntary disclosure of personal information to the mainstream, and thus increases privacy risks (Gross & Acquisti, 2005). Therefore, understanding the underlying antecedents to privacy has become much more important in the Web 2.0 age.

Scale development

To test research hypotheses, data were collected through a survey that included scales for the constructs specified in the research model. Scale development was based on an extensive survey of the privacy literature. All construct measures were reflective measures, where a change in the construct affects the underlying measures (Petter *et al*, 2007). Perceived privacy was measured by three questions adapted from Chellappa (2008) (see also Chellappa, 2001a, b and Frye & Dornischa, 2010). Drawing on Featherman & Pavlou (2003) and Dinev & Hart (2006), we measured perceived privacy risk using four items to reflect the potential losses associated with the information disclosure. Our items, while more tailored for Web sites, are also well aligned with two of the three items of the instrument for privacy risk developed and validated by Featherman & Pavlou, 2003. Items measuring perceived information control were measured by four questions that were directly taken from Xu (2007). Anonymity was measured by three items developed from Teich *et al* (1999) and secrecy was measured by three items adapted from Bok (1989) and Tefft (1980). Information sensitivity was measured by three items based on prior literature (Milne & Gordon, 1993; Phelps *et al*, 2000; Sheehan & Hoy, 2000), perceived benefits of information disclosure was measured by three items adapted from Stone *et al* (1983), and importance of information transparency was measured by three items taken from Awad & Krishnan (2006). Confidentiality was measured by three items based on Camp (1999), and Zwick & Dholakia (2004). Measures for regulatory expectations were developed based on prior privacy studies (Milberg *et al*, 1995; Milberg *et al*, 2000; Bellman *et al*, 2004). All measurement items are included in the Appendix A.

Survey administration

The initial questionnaire was reviewed by external researchers and a pilot study was conducted involving 31 undergraduate students. The respondents' opinions on the clarity of the survey instructions and questions were also gathered. Following their feedback and analysis of measurement model, some changes were made to the instrument, including dropping certain items, wording of items, and editing the instructions. The survey was administered to undergraduate, graduate, and M.B.A. students at two large universities in the United States. Respondents were asked to recall their experiences in using Web 2.0-related sites such as blogging sites (e.g., Blogger), tagging sites (e.g., del.icio.us and Flickr), user-driven rating sites (e.g., Digg), and social networking sites (e.g., Facebook and MySpace). They were also asked to list the name or URL of the Web site that they used within the last 6 months. The 10 most frequently used Web 2.0 sites were http://www.Google.com, http://www.Amazon.com, www.facebook.com, www.myspace.com, www.hi5.com, www.youtube.com, www.4chan.org, www.flickr.com, www.friendster.com, www.linkedin.com, www.orkut.com, and www.groups.yahoo.com. A total of 192 responses were used in the empirical testing. Table 2 provides respondent demographics.

Non-response bias was assessed by verifying that early and late respondents were not significantly different (Armstrong & Overton, 1977). Early respondents were those who responded within the first week (48%). The two groups of early and late respondents were compared based on their demographics (age, gender, and Web usage experience). All *t*-test comparisons between the means of the two groups showed insignificant differences.

The use of student subjects has been questioned before on grounds of external validity and generalizability. However, multiple reasons suggest that, in this case, the use of student subjects does not present a significant threat in our study. First, study participants were online customers and Internet users and students are among the most active users. On the basis of the latest survey conducted by the Pew Internet & American Life Project (2011), the sample chosen is highly representative of active Internet users (i.e., those between the ages of 18 and 29), making the sample highly relevant for this context. Second, we investigated correlations between age and individual construct's sub-scales, and all of them are relatively small and insignificant. We also ran age as a control variable in our structural model and there was no significant effect. Third, prior empirical research in MIS and marketing suggests that where online behavior is concerned, a random sample of the general population of online consumers may not always be better than a student sample. For all the reasons above, many MIS studies related to internet use and online behavior have used students as subjects (see, e.g., McKnight *et al*, 2002; Komiak & Benbasat, 2006; Strite & Karahanna, 2006; Tam & Ho, 2006; Webster & Ahuja, 2006; Jiang & Benbasat, 2007a, b; McElroy *et al*, 2007.)

Table 2 Respondent demographics

Demographic variables	*Category*	*Percentage (%)*
Gender	Female	46.3
	Male	53.7
Age	18–24	80.0
	25–29	10.2
	30–34	3.4
	35–39	2.9
	40–49	2.0
	50 and over	1.5
Weekly Web usage: reading newspaper	0–3 h	73.7
	4–7 h	19.0
	8–13 h	4.9
	14+ h	2.4
Weekly Web usage: accessing information about the products/services	0–3 h	43.9
	4–7 h	33.7
	8–13 h	17.1
	14+ h	5.4
Weekly Web usage: shopping	0–3 h	70.2
	4–7 h	21.0
	8–13 h	5.4
	14+ h	3.4

Data analysis and results

A second-generation causal modeling statistical technique, partial least squares (PLS), was used for data analysis in this research. For a detailed rationale about using PLS as one of the best methods for empirical testing of structural models, see Xu *et al* (2011). To analyze the measurement quality and the path model for hypothesis testing, we used SmartPLS (Ringle *et al*, 2005) as the primary statistical tool. Following the literature tradition of structural equation modeling, we first assessed the quality of the measurement model to ensure the validity of constructs and reliability of the measurements. This was followed by structural modeling, to test the research hypothesis and the overall quality of the proposed model.

Measurement model

The quality of the measurement model is usually assessed in terms of its content validity, construct validity, and reliability (Straub *et al*, 2004). Content validity is defined as the degree to which the items represent the construct being measured. Content validity is usually assessed by the domain experts and literature review (Straub *et al*, 2004). In this case, the content validity is primarily assured by adopting the previously published measurement items for the construct and an item-by-item review by the research team before and after the pilot study.

Construct validity can be assessed using convergent validity and discriminant validity. Convergent validity is defined as the degree to which the measurement items are related to the construct they are theoretically predicted to be related (Straub *et al*, 2004). Statistical evidence of convergent validity was confirmed by the high factor loadings and their statistical significance, as shown by their corresponding *t*-values (all greater than 2.576). As seen from Table 3, no items exhibit either low factor loadings (<0.7) or high cross-loadings indicating good convergent validity.

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 & Karahanna (2000), we applied two tests to assess discriminant validity. First, per Table 3, the confirmatory factor analysis showed low cross loadings ensuring that the items of each construct loaded more highly on their intended construct than other constructs. Second, each item should correlate more highly with other items measuring the same construct than with items measuring other constructs. This was determined by checking whether the square root of the average variance extracted (AVE) shared between a construct and its items were greater than the correlations between the construct and any other items in the model. Table 4 shows the correlations and each construct's AVE. The diagonal values are the square roots of the AVEs and are all higher than the correlations. Thus, all items in our study fulfilled the requirement of discriminant validity.

The reliability of the measurement addresses the concern of how well the items for one construct correlate or move together (Straub *et al*, 2004). Reliability is usually assessed by two indicators – Cronbach's α and composite reliability. Cronbach's α is a measure of internal consistency among all items used for one construct. Composite reliability addresses a similar concept, but is considered a more rigorous reliability measure in the context of

Table 3 Loadings* and cross-loadings of measures

	PRV	*PCTL*	*ANYT*	*CFDT*	*SCRT*	*RISK*	*BEN*	*IS*	*TR*	*LAW*
PRV1	**0.933**	0.505	0.244	0.107	0.226	−0.280	0.177	−0.334	−0.073	−0.025
PRV2	**0.938**	0.523	0.220	0.106	0.231	−0.268	0.192	−0.314	−0.087	−0.027
PRV3	**0.890**	0.585	0.276	0.080	0.202	−0.279	0.223	−0.288	−0.075	−0.011
PCTL1	0.470	**0.803**	0.229	0.306	0.307	−0.103	0.119	−0.327	0.087	0.015
PCTL2	0.590	**0.899**	0.256	0.248	0.301	−0.108	0.150	−0.237	0.043	0.008
PCTL3	0.573	**0.892**	0.264	0.209	0.313	−0.093	0.121	−0.209	0.053	0.065
PCTL4	0.503	**0.791**	0.366	0.314	0.428	−0.073	0.106	−0.276	0.086	0.049
ANYT1	0.218	0.251	**0.858**	0.109	0.209	−0.079	0.064	−0.224	0.005	0.013
ANYT2	0.220	0.276	**0.929**	0.102	0.206	−0.143	0.126	−0.183	0.029	0.015
ANYT3	0.279	0.371	**0.930**	0.094	0.249	−0.160	0.120	−0.278	0.010	0.011
CFDT1	0.101	0.224	0.150	**0.760**	0.306	−0.063	0.095	−0.161	0.183	194
CFDT2	0.105	0.284	0.104	**0.899**	0.318	−0.103	0.091	−0.152	0.361	0.338
CFDT3	0.110	0.293	0.106	**0.864**	0.316	−0.084	0.049	−0.157	0.284	0.222
SCRT1	0.204	0.458	0.292	0.326	**0.857**	−0.036	0.045	−0.218	0.187	0.201
SCRT2	0.213	0.291	0.243	0.295	**0.784**	−0.077	0.073	−0.155	0.177	0.152
SCRT3	0.222	0.295	0.272	0.316	**0.841**	−0.028	0.079	−0.262	0.157	0.195
RISK1	−0.232	−148	−0.177	−0.108	−0.021	**0.858**	−0.312	0.250	0.227	0.194
RISK2	−0.202	−0.151	−0.185	−0.091	−0.038	**0.890**	−0.263	0.226	0.339	0.229
RISK3	−0.303	−0.155	−0.153	−0.149	−0.132	**0.784**	−0.246	0.241	0.297	0.297
RISK4	−0.232	−0.183	−0.172	−0.110	−0.043	**0.788**	−0.217	0.304	0.154	0.265
BEN1	0.152	0.096	0.072	0.107	0.023	−0.204	**0.715**	−0.155	−0.024	0.014
BEN2	0.186	0.098	0.059	0.103	0.111	−0.234	**0.859**	−0.128	−0.006	0.013
BEN3	0.219	0.114	0.138	0.091	0.027	−0.219	**0.874**	−0.207	−0.034	0.020
IS1	−0.154	−0.315	−0.235	−0.093	−0.209	0.242	−0.124	**0.920**	0.186	0.099
IS2	−0.158	−0.234	−0.154	−0.060	−0.130	0.177	−0.146	**0.707**	0.195	0.058
IS3	−0.187	−0.240	−0.197	−0.040	−0.250	0.207	−0.125	**0.756**	0.138	0.094
TR1	−0.044	0.118	0.001	0.261	0.252	0.296	−0.043	0.165	**0.937**	0.350
TR2	−0.111	0.064	0.024	0.193	0.172	0.278	−0.008	0.213	**0.963**	0.375
TR3	−0.083	0.052	0.011	0.172	0.170	0.244	−0.006	0.200	**0.885**	0.313
LAW1	−0.058	0.097	0.030	0.331	0.197	0.228	0.017	0.056	0.308	**0.909**
LAW2	−0.010	0.074	0.019	0.267	0.251	0.301	0.037	0.082	0.389	**0.933**
LAW3	−0.089	0.049	0.022	0.226	0.161	0.247	0.035	0.094	0.376	**0.890**

*All loadings (denoted in bold) were statistically significant at level $P<0.01$.

Table 4 Internal consistency and discriminant validity of constructs

	Composite reliability	*Cronbach's α*	*AVE*	*ANYT*	*CFDT*	*SCRT*	*RISK*	*PRIV*	*IS*	*BEN*	*TR*	*LAW*	*PCTL*
ANYT	0.93	0.87	0.82	0.91									
CFDT	0.88	0.84	0.71	−0.01	0.84								
SCRT	0.87	0.77	0.69	0.37	0.48	0.83							
RISK	0.90	0.87	0.70	−0.19	0.23	0.09	0.84						
PRIV	0.95	0.90	0.85	0.36	−0.01	0.29	−0.31	0.92					
IS	0.86	0.80	0.67	−0.23	0.05	−0.19	0.31	−0.42	0.82				
BEN	0.86	0.76	0.68	0.13	−0.10	−0.08	−0.32	0.21	−0.09	0.82			
TR	0.95	0.92	0.87	−0.04	0.43	0.22	0.35	−0.18	0.32	−0.03	0.93		
LAW	0.93	0.89	0.82	0.04	0.38	0.28	−0.08	−0.06	0.11	−0.03	0.41	0.91	
PCTL	0.92	0.89	0.74	0.27	0.04	0.31	−0.23	0.51	−0.38	0.19	−0.11	−0.05	0.86

structural equation modeling (Chin, 1998). The reliability indicators of the constructs in this study are shown in Table 4. All values are higher than the recommended minimum value of 0.70 (Gefen *et al*, 2000; Nunnally's, 1978) indicating good reliability of the measurement for each constructs.

Putting all indicators together, we can conclude that the measurement model has satisfactory quality in terms construct validity, discriminant validity, and reliability.

Finally, we addressed the threat of common method bias (Podsakoff *et al*, 2003; Straub *et al*, 2004). Burton-Jones (2009) proposes a more comprehensive approach to common method bias and provides a clear definition: It is the 'difference between the measured score of a trait and the trait score that stems from the rater, instrument, and/or procedure used to obtain the score.' (Burton-Jones, 2009, p. 448). He proposed two fundamental sources of method bias: knowledge bias and rating bias. An example of a knowledge bias would be a bias due to a rater's lack of knowledge of the trait score that would cause self-rating *vs* observers' rating of the trait. An example of a rating bias would be the bias from the rater's unwillingness to provide a best estimate of the trait score, or a bias from the instrument or procedure influencing the rater to give a different score. Both result in providing an inaccurate response because it is socially desirable or because the rater has privacy concerns.

We thoroughly examined our survey instrument and its administration against the criteria listed by Burton-Jones (2009) and we concluded that neither suffered knowledge or rater bias. By ensuring anonymity to 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% 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 (termed a marker variable), which was used to adjust the correlations among the principal constructs (Malhotra *et al*, 2006). Following Malhotra *et al* (2006), the correlation between the marker variable and our research constructs was assessed and were assumed to have no relationships. The results indicated that the average correlation coefficient was close to 0 ($r = 0.02$, NS). Thus, we argue that this research is relatively robust against common method biases.

Structural model

After establishing the validity of the measures, we tested the structural paths in the research model using PLS by examining the sign and significance of the path coefficients. Predictive validity is assessed with PLS 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., perceived privacy in our study). We conducted the statistical tests at a 5% level of significance. Control variables were included in the model. None of them had a statistically significant effect on the DV. Figure 2 presents the structural models.

The structural models explain 52.2% of the variance in perceived privacy. As hypothesized, perceived control and perceived risk strongly influence perception of privacy, thus validating H1 and H5. Anonymity, secrecy, and confidentiality are found to be the significant mechanisms to information control, validating H2, H3, and H4. Perceived benefits of information disclosure, information sensitivity, importance of information transparency, and regulatory expectations all have significant impacts on perceived risk, validating H6, H7, H8, and H9.

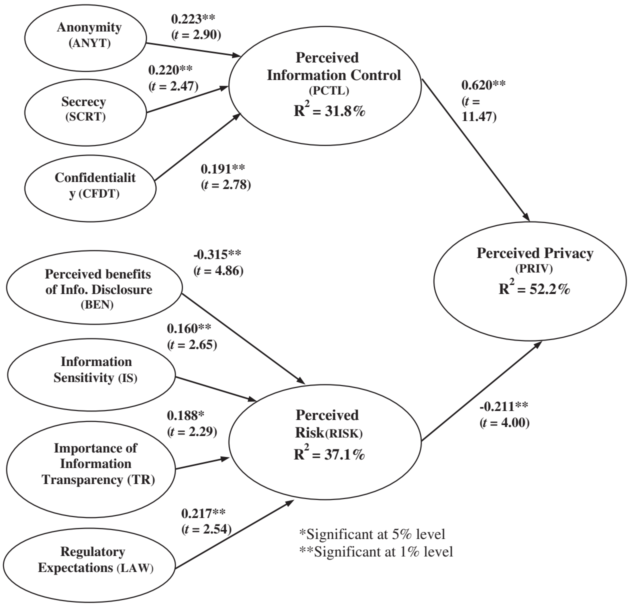

Figure 2 The structural model.

Discussion and conclusion

We want to begin this section by emphasizing that this study is far from conclusive and should be treated as merely an *attempt* to empirically address the confusion in the literature among privacy and its other conceptually close correlates such as anonymity, secrecy, confidentiality and so on. We believe that more than one study is needed in order to resolve the present ambiguity, lack of rigorous definitions, and consistent empirical treatment of these correlates. Thus more research ideas should spring out in the near future. The dynamics of the research dialogue and the evolution of the theoretical and conceptual thinking include subsequent clarifications, finding of weaknesses, deficiencies, corrections to definitions, and relationships that are present in our study. So, our study should be treated as laying the groundwork for a further stream of conceptualizations and models that will contribute to clarification of what privacy and its correlates actually mean, and more importantly, does their meaning change with evolution of technology and enrichment of contexts.

This study developed and empirically tested a research model to investigate privacy perceptions in Web 2.0-related sites. The results of our hypotheses testing are presented in Table 5. Our proposed model is able to

Table 5 Results from the hypotheses testing

Hypothesis number	*Relationship*	*Support*
1	Perceived information control (+)→Perceived privacy	Yes, level 0.01
2	Anonymity perceived (+)→Information control	Yes, level 0.01
3	Secrecy perceived (+)→Information control	Yes, level 0.01
4	Confidentiality (+)→Perceived information control	Yes, level 0.01
5	Perceived risk (−)→Perceived privacy	Yes, level 0.01
6	Perceived benefits of information disclosure (−)→Perceived risk	Yes, level 0.01
7	Information sensitivity (+)→Perceived risk	Yes, level 0.01
8	Importance of information transparency (+)→Perceived risk	Yes, level 0.05
9	Regulatory expectations (+)→Perceived risk	Yes, level 0.01

account for 52.2% of the variance in perceived privacy, and thus possesses adequate explanatory power to make the interpretation of path coefficients meaningful. The evidence from this study provided empirical support that a cognitive process of assessing perceived information control and perceived risk is shown to be important in shaping an individual's privacy perception. We confirm that privacy risk attitudes are grounded in an individual's values in terms of information sensitivity, assessment of perceived benefits of information disclosure, importance of information transparency, and regulatory expectations that enable a person to assess the risks of information disclosure. Anonymity, secrecy, and confidentiality were shown to be the important tactics of information control.

We also conducted extensive mediation tests with various methodologies. We provide a detailed report in Appendix B. The tests validated our theoretical model and showed that the relationships on our structural model are the most significant.

Limitations and future research

Although the data generally supported the proposed model, we note several limitations to our work. First, and by design, our work is limited to the examination of how individuals *form* privacy perceptions. In this study, we have not extended the nomological network to consider how those perceptions are *translated* into outcome variables such as information disclosure 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 perceived privacy and outcome variables. Future research could move beyond the examination of the formation of privacy perceptions to the examination of such as trust and information disclosure behaviors (Krasnova *et al*, 2009).

Second, while our model explains a substantial percent of variance in the perceived privacy, there are several factors investigated in prior research and missing in our model, namely the context, culture, personality characteristics, and possibly personal and institutional trust-related factors. All of these missing from our model factors may additionally strengthen the privacy model and provide additional explained variance. Due to the contextual nature of privacy (Milberg *et al*, 1995; Milberg *et al*, 2000), the current research framework would need to be expanded in the future. While information sensitivity partially captures the nature of context (see also Bansal *et al*, 2010), a much richer context can be explored in future studies (Acquisti, 2004; Bansal *et al*, 2008). The dynamics of the ITs and the new opportunities of communication such as social networking and Web 2.0, introduce new and more complex factors that have to be included in future models. For example, the fact that online participants in social networking sites voluntarily disclose their personal information should be taken into account and possibly a new context-specific construct such as Voluntariness should be included in the nomological interplay of control, privacy, and risk. If we explore other Web sites, where users do not voluntarily submit their personal information, we may find a different picture. Clearly, there is opportunity for future research and establishing the generalizability of our current model.

In addition, there is substantial evidence that personality factors are also playing role in formation of privacy perceptions. Personality differences such as introversion *vs* extroversion (Lu *et al*, 2004), independent-self *vs* interdependent-self (Xu, 2007), and 'Big-Five' personality traits (Bansal *et al*, 2010) have been found to affect individual privacy concerns. None of these are present in our model and definitely warrant future research.

There is urgent need of a separate research to rigorously and systematically argue about the extent to which physical and information privacy can be directly used interchangeably and under one umbrella. As we mentioned in the beginning of our study, the information privacy research has adopted earlier concepts that pertained to physical privacy directly and seamlessly to the information privacy. No questions were asked at that stage about the applicability of this direct borrowing of theories and concepts. As the importance of information privacy and the ubiquity of electronic data grow, the need of this clarification becomes more and more pressing.

Finally, our study suffers the inherent disadvantages and flaws of every positivist, survey-based empirical study – the precision, control, and thoroughness that is lost when we focus only on realism (McGrath, 1982; Dennis & Valacich, 2001). The more intricate nuances of the constructs are lost when we try to frame them into measurable items, and with this suffer the richness of the context as well as the cultural and period specifics.

Theoretical and practical implications

This research presents a model linking privacy and its various correlates together, which 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 have been inconsistent and not fully developed in the extant literature. Our model has drawn upon and brought together multitude of concepts, definitions, and visions about privacy that have been discussed throughout the decades of privacy research in such a diverse manner that prompted Solove (2006, p. 477) to declare that general privacy is 'a concept is in disarray'. We believe our study brings researchers closer to the so much needed conceptual and operational clarity of privacy.

This research has also shown that the conventional understanding of privacy from a calculus perspective can be extended: on one hand, consumers may assess the outcomes of information disclosure; on the other hand, they may also attend to evaluate the sensitivity of requested information, organization's information-handling practices, and the regulatory environment that enable them to assess the risks of information disclosure.

Further, the work theoretically differentiates three tactics of information control and empirically tests their effects on influencing privacy perceptions. On the basis of the Zwick & Dholakia's (2004) conceptualization of identity management, we identify three different tactics consumers apply to manage the externalization of their personal information: anonymity, secrecy, and confidentiality. In the past, these were argued to be privacy 'interests' or 'dimensions', while, through a consistently built and empirically validated integrated model, we showed that they have to be viewed as control tactics that influence privacy perceptions through the control construct.

Similarly to the works of Chellappa (2001a, b), the study above examines perceptions of privacy as a state rather than privacy as a concern as most of MIS studies have done. By centering our privacy model around perceptions of privacy, we eliminated the need to rely on the privacy concerns as a proxy that may bring a negative connotation to the notion of privacy, if the latter is to be regarded as a human and societal well-cherished value.

From a practical perspective, this study shows that risk beliefs and perceived information control are the important factors in users' privacy perceptions with Web 2.0-related sites. In this respect, this study provides some insights into the approaches that could be used by a Web 2.0 site operator to address privacy issues by reducing risk beliefs and enhancing control perceptions. To the extent that perceived information control is an important factor influencing privacy perception, it is important for Web 2.0 site operators to develop privacy control features with user-friendly interfaces for ensuring individual's capability to maintain the anonymity, secrecy, and confidentiality of their personal information. From a privacy risk reduction perspective, Web 2.0 site operators should be aware that perceived risk does decrease user privacy perception.

This study shows that the user's assessment of perceived benefits of information disclosure significantly decreases perceived risk, while information sensitivity increases perceived risk. It follows that additional incentives (e.g., more functions or customized features) and limited collection of sensitive information need to be considered to mitigate the user's perceived risk of information disclosure. Our study shows that importance of information transparency can help decrease user risk beliefs. This, in turn, suggests that Web 2.0 site operators should not keep privacy practice in the backroom of their Web sites. Instead, details on how and what information is collected and stored should be integrated into customer relationship management campaigns, and information on the regulations to which Web 2.0 site operators comply should be communicated to users.

Beyond the Web 2.0 context, the main practical implication is in creating public and organizational policies and rules that are better aligned with the more intricate understanding of what drives individuals' perception of less or more privacy. Our results show that citizens expect more regulations from their government or from the private sector regarding gathering of personal information, and that has an effect on their perceived risk. The regulations can cover both the amount and the type of information, with respect to how sensitive the information is, which can be gathered, and the extent of the user's control on the collection and distribution of the personal information. Many goals can be achieved with smarter, better regulation. Both increased user control and decreased perceived risk can be managed by policies and regulations, and they both affect the perceived privacy.

In this study, we developed a framework that includes privacy and constructs, such as anonymity, secrecy, and confidentiality that have often been regarded as dimensions of privacy and sometimes even equated with privacy. We showed that these three constructs are actually tactics of information control and affect the users' perceived information control, which, along with perceived risk, directly affect the perceived privacy. We also showed that perceived risk can be decreased by perceived benefits from information disclosure, and substantially increased by the sensitivity of the disclosed information, the regulatory expectations the users have, and the importance of information transparency. Users' information control and risk perceptions could play primary roles in addressing privacy issues pertaining to

Web 2.0-related sites, especially in the absence of well-established legal resources. This study provides a preliminary understanding of the privacy issues in Web 2.0-related sites by integrating privacy and its correlates into a theoretical framework. Using the groundwork laid down in this study, further work could contribute to extending our theoretical understanding and practical ability to foster the diffusion of Web 2.0 features.

About the authors

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.

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.

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 to 2006 and as Chair of the Department of Decision Sciences and Management Information Systems at Miami University (Ohio) from July 2006 til 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 a 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.

References

Acquisti A (2004) Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM Electronic Commerce Conference*, p 21, ACM Press, New York.

Acquisti A and Gross R (2006) Imagined communities: awareness information sharing and privacy on the facebook. In *Proceedings of the 6th Privacy Enhancing Technologies Symposium*, p 36, Cambridge, United Kingdom.

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

Akers R (2001) *Criminological Theories: Introduction, Evaluations, and Application*. Roxbury, Los Angeles, CA.

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

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

Armstrong JS and Overton TS (1977) Estimating non-response bias in mail surveys. *Journal of Marketing Research* **14(3)**, 396–402.

Awad NF and Krishnan MS (2006) The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* **30(1),** 13–28.

Bansal G, Zahedi F and Gefen D (2008) The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: a multiple-context investigation. In *Proceedings of 29th Annual International Conference on Information Systems (ICIS 2008)*. Paris, France.

Bansal G, Zahedi FM and Gefen D (2010) The impact of personal dispositions on information sensitivity privacy concern and trust in disclosing health information online. *Decision Support Systems* **49(2),** 138–150.

Baron RM and Kenny DA (1986) The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations. *Journal of Personality and Social Psychology* **51,** 1173–1182.

Belanger F, Hiller JS and Smith WJ (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 EJ, Kobrin SJ and Lohse GL (2004) International differences in information privacy concerns: a global survey of consumers. *Information Society* **20(5),** 313–324.

Bennett CJ (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press, Ithaca, NY.

Bok S (1989) *Secrets: On the Ethics of Concealment and Revelation*. Random House Digital, Inc., New York.

Brin D (1998) *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Perseus Books Group, Reading, MA.

Burton-Jones A (2009) Minimizing method bias through programmatic research. *MIS Quarterly* **33(3),** 445–471.

Burton-Jones A and Straub D (2006) Reconceptualizing system usage: An approach and empirical test. *Information Systems Research* **17(3),** 220–246.

Camp LJ (1999) Web security and privacy: an American perspective. *Information Society* **15(4),** 249–256.

Campbell DT and Fiske DW (1959) Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin* **56(2),** 81–105.

Cate FH (1997) *Privacy in the Information Age*. Brookings Institution Press, Washington DC.

Chellappa RK (2001a) The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. PhD Thesis, University of South California, Los Angeles, CA.

Chellappa RK (2001b) Contrasting expert assessment of privacy with perceived privacy: implications for public policy. In *Proceedings of the National Conference on Digital Government Research*, p 147, Redondo Beach, CA.

Chellappa RK (2008) Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security. Working paper. [WWW document] http://www.bus.emory.edu/ram/Papers/sec-priv.pdf (accessed 6 March 2012).

Chin WW (1998) The partial least squares approach to structural equation modeling. In *Modern Methods for Business Research* (Marcoulides GA, Ed.) Mahwah, NJ, Lawrence Erlbaum Associates. pp 295–336.

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* **31(5),** 498–512.

Cote S (2002) *Introduction in Criminological Theories – Bridging the Past to the Future*. Sage Publications, Thousand Oaks, CA.

Cramer KM and Barry JE (1999) Psychometric properties and confirmatory factor analysis of the self-concealment scale. *Personality and Individual Differences* **27(4),** 629–637.

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

Culnan MJ and Armstrong PK (1999) Information privacy concerns procedural fairness and impersonal trust: an empirical investigation. *Organization Science* **10(1),** 104–115.

Culnan MJ and Bies RJ (2003) Consumer privacy: balancing economic and justice considerations. *Journal of Social Issues* **59(2),** 323–342.

Dennis A and Valacich J (2001) Conducting research in information systems. *Communications of the AIS* **7(5),** 1–41.

Dhillon GS and Moores T (2001) Internet privacy: interpreting key issues. *Information Resources Management Journal* **14(4),** 33.

Di Pietro R and Mancini LV (2003) Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM* **46(9),** 74–79.

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

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

Dinev T and Hart P (2007) Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *E-Service Journal* **4(3),** 25–61.

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

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

Dowling G and Staelin RA (1994) Model of perceived risk and intended risk-handling activity. *Journal of Consumer Research* **21(1),** 119–134.

Earp JB and Payton FC (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.

eMarketer (2007) User-generated content: will web 2.0 pay its way? [WWW document] http://www.emarketer.com/Products/Explore/ReportList.aspx?dsNav = Rpp:25,Nrc:id-1047,N:879,Nr:Type%3AReport (accessed 6 March 2012).

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

Featherman M, Wright RT, Thatcher JB, Zimmer J and Pak R (2011) The Influence of interactivity on e-service offerings: an empirical examination of benefits and risks. *AIS Transactions on Human-Computer Interaction* **3(1),** 1–25.

Featherman MS and Pavlou PA (2003) Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies* **59(4),** 451–474.

Festinger LA (1957) *Theory of Cognitive Dissonance*. Stanford University Press, Stanford, CA.

Flaherty DH (1979) *Privacy and Government Data Banks: An International Perspective*. Mansell, London.

Frye NE and Dornischa MM (2010) When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior* **26(5),** 1120–1127.

Fusilier MR and Hoyer WD (1980) Variables affecting perceptions of invasion of privacy in a personnel selection situation. *Journal of Applied Psychology* **65(5),** 623–626.

Gefen D, Rigdon E and Straub DW (2011) An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly* **35(2),** iii–xiv.

Gefen D, Straub DW and Boudreau MC (2000) Structural equation modeling and regression: guidelines for research practice. *Communications of AIS* **4(1),** 1–78.

Gillmor D (2007) The read-write web: technology that makes we the media possible. [WWW document] http://www.authorama.com/we-the-media-3.html (accessed 6 March 2012).

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

Gross R and Acquisti A (2005) Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. Alexandria, VA.

Hoadley CM, Xu H, Lee JJ and Rosson MB (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.

Hui K-L, Teo H-H and Lee TSY (2007) The value of privacy assurance: an exploratory field experiment. *MIS Quarterly* **31(1),** 19–33.

Jiang Z and Benbasat I (2007a) Investigating the influence of the functional mechanisms of online product presentations. *Information Systems Research* **18(4),** 454–470.

Jiang Z and Benbasat I (2007b) The effects of presentation methods and task complexity on online consumers' product understanding. *MIS Quarterly* **31(3)**, 475–500.

Kelvin P (1973) A social-psychological examination of privacy. *British Journal of Social Clinical Psychology* **12(2)**, 248–261.

Klopfer PH and Rubenstein DI (1977) The concept privacy and its biological basis. *Journal of Social Issues* **33(3)**, 52–65.

Kobsa A and Schreck J (2003) Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology* **3(2)**, 149–183.

Komiak XS and Benbasat I (2006) The effects of personalization and familiarity on trust in and adoption of recommendation agents. *MIS Quarterly* **30(4)**, 941–960.

Krasnova H, Spiekermann S, Koroleva K and Hildebrand T (2009) Online social networks: why we disclose. *Journal of Information Technology* **25(2)**, 109–125.

Laufer RS and 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 and Xu H (2011) The role of affect and cognition on online consumers' willingness to disclose personal information. *Decision Support Systems* **51(3)**, 434–445.

Lindell MK and Whitney DJ (2001) Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology* **86(1)**, 114–121.

Liu C, Marchewka JT, Lu J and Yu CS (2005) Beyond concern – a privacy-trust-behavioral intention model of electronic commerce. *Information & Management* **42(2)**, 289–304.

Luo X, Li H, Zhang J and Shim JP (2010) Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services. *Decision Support Systems* **49(2)**, 222–234.

Madden M, Fox S, Smith A and Vitak J (2007) Digital footprints: online identity management and search in the age of transparency. PEW Internet & American Life Project. [WWW document] http://pewresearch.org/pubs/663/digital-footprints (accessed 6 March 2012).

Malhotra NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (IUIPC): the construct the scale and a causal model. *Information Systems Research* **15(4)**, 336–355.

Malhotra NK, Kim SS and Patil A (2006) Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science* **52(12)**, 1865–1883.

Margulis ST (1977) Conceptions of privacy: current status and next steps. *Journal of Social Issues* **33(3)**, 5–21.

Margulis ST (2003a) On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* **59(2)**, 411–429.

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

Marshall NJ (1974) Dimensions of privacy preferences. *Multivariate Behavioral Research* **9(3)**, 255–271.

Marx GT (1999) What's in a name? Some reflections on the sociology of anonymity. *Information Society* **15(2)**, 99–112.

Mason RO (1986) Four ethical issues of the information age. *MIS Quarterly* **10(1)**, 4–12.

McElroy JC, Hendrickson AR, Townsend AM and Demarie SM (2007) Dispositional factors in internet use: personality versus cognitive style. *MIS Quarterly* **31(4)**, 809–820.

McGrath JE (1982) Dilemmatics: the study of research choices and dilemmas. In *Judgment Calls in Research* (McGrath JE, Martin J and Kulka RA, Eds), pp 69–102, Sage, Beverly Hills, CA.

McKnight DH, Choudhury V and Kacmar C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research* **13(3)**, 334–359.

McLean D (1995) *Privacy and Its Invasion*. Praeger, Westport, CT.

Metzger MJ (2004) Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* **9(4)**, 114–121.

Milberg SJ, Burke JS, Smith HJ and Kallman AE (1995) Values personal information privacy concerns and regulatory approaches. *Communication of the ACM* **38(12)**, 65–74.

Milberg SJ, Smith HJ and Burke SJ (2000) Information privacy: corporate management and national regulation. *Organization Science* **11(1)**, 35–57.

Milne GR and Boza M-E (1999) Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing* **13(1)**, 5–24.

Milne GR and Gordon EM (1993) Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy and Marketing* **12(2)**, 206–215.

Moorman C, Desphande R and Zaltman G (1993) Factors affecting trust in market research relationships. *Journal of Marketing* **57(1)**, 81–101.

Nissenbaum H (1999) The meaning of anonymity in an information age. *The Information Society* **15(2)**, 141–144.

Nunnally JC (1978) *Psychometric Theory*. McGraw-Hill, New York.

Pavlou PA (2002) Institution-based trust in inter organizational exchange relationships: the role of online B2B marketplaces on trust formation. *Journal of Strategic Information Systems* **11(3–4)**, 215–243.

Pedersen DM (1997) Psychological Functions of Privacy. *Journal of Environmental Psychology* **17(2)**, 147–156.

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

Petter S, Straub DW and Rai A (2007) Specifying formative constructs in information systems research. *MIS Quarterly* **31(4)**, 623–656.

Pew Internet & American Life Project (2011) Demographics of internet users. [WWW document] http://www.pewinternet.org/Trend-Data/Whos-Online.aspx (accessed 6 March 2012).

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

Podsakoff MP, Mackenzie BS, Lee JY and Podsakoff NP (2003) Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* **88(5)**, 879–903.

Poindexter JC, Earp JB and Baumer DL (2006) An experimental economics approach toward quantifying online privacy choices. *Information Systems Frontiers* **8(5)**, 363–374.

Qian H and Scott CR (2007) Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication* **12(4)**, 1428–1451.

Raab CD and Bennett CJ (1998) The distribution of privacy risks: who needs protection? *Information Society* **14(4)**, 263–274.

Rensel AD, Abbas JM and Rao HR (2006) Private transactions in public places: an exploration of the impact of the computer environment on public transactional web site use. *Journal of the Association for Information Systems* **7(1)**, 19–50.

Rindfleisch TC (1997) Privacy information technology and health care. *Communications of the ACM* **40(8)**, 92–100.

Ringle CM, Wende S and Will A (2005) SmartPLS, 2.0. University of Hamburg, Hamburg, Germany. [WWW document] http://www.smartpls.de (accessed 14 April 2012).

Rosen J (2000) *The Unwanted Gaze: The Destruction of Privacy in America*. Random House, New York.

Rust R, Kannan PK and Peng N (2002) The customer economics of internet privacy. *Journal of the Academy of Marketing Science* **30(4)**, 455–464.

Schoeman FD (Ed) (1984) *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, Cambridge, UK.

Sheehan KB and Hoy MG (2000) Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing* **19(1)**, 62–73.

Smith HJ (1994) *Managing Privacy: Information Technology and Corporate America*. University of North Carolina Press, Chapel Hill, NC.

Smith HJ, Dinev T and Xu H (2011) Information privacy research: an interdisciplinary review. *MIS Quarterly* **35(4)**, 989–1015.

Smith HJ, Milberg JS and Burke JS (1996) Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly* **20(2)**, 167–196.

Solove DJ (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York University Press, New York.

Solove DJA (2006) Taxonomy of privacy. *University of Pennsylvania Law Review* **154(3)**, 477–560.

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

Spiekermann S (2005) Perceived control: scales for privacy in ubiquitous computing environments. In *Proceedings of the 10th International Conference on User Modeling*. Edinburgh, Scotland.

Sternberg R (2003) *Cognitive Psychology*. Thomson Wadsworth, Belmont, CA.

Stewart KA and Segars AH (2002) An empirical examination of the concern for information privacy instrument. *Information Systems Research* **13(1)**, 36–49.

Stone EF and Stone DL (1990) Privacy in organizations: theoretical issues research findings and protection mechanisms. *Research in Personnel and Human Resources Management* **8(3)**, 349–411.

Stone EF, Gueutal GH, Gardner DG and Mcclure S A (1983) Field experiment comparing information-privacy values beliefs and attitudes across several types of organizations. *Journal of Applied Psychology* **68(3)**, 459–468.

Straub DW, Boudreau M-C and Gefen D (2004) Validation guidelines for IS positivist research. *Communications of AIS* **13(1)**, 380–427.

Strite M and Karahanna E (2006) The role of espoused national cultural values in technology acceptance. *MIS Quarterly* **30(3)**, 679–704.

Swire PP (1997) Markets self-regulation and government enforcement in the protection of personal information. In *Privacy and Self-Regulation in the Information Age* (Daley WM and Irving L, Eds), pp 3–19, Department of Commerce, Washington DC.

Tam KY and Ho SY (2006) Understanding the impact of web personalization on user information processing behavior and judgment. *MIS Quarterly* **30(4)**, 865–890.

Taylor J (1974) The role of risk in consumer behavior. *Journal of Marketing* **38(2)**, 54–60.

Tefft SK (1980) *Secrecy a Cross-Cultural Perspective*. Human Sciences Press, New York.

Teich A, Frankel MS, Kling R and Lee YC (1999) Anonymous communication policies for the Internet: results and recommendations of the AAAS conference. *Information Society* **15(2)**, 71–77.

Tolchinsky PD, McCuddy M, Adams J, Ganster DC, Woodman R and Fromkin HL (1981) Employee perceptions of invasion of privacy: a field simulation experiment. *Journal of Applied Psychology* **66(3)**, 308–313.

Turkle S (1995) *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster New York.

Turkle S (2011) *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books, New York.

Vidmar N and Flaherty D (1985) Concern for personal privacy in an electronic age. *Journal of Communication* **35(1)**, 91–103.

Waldo J, Lin H and Millett LI (2007) *Engaging Privacy and Information Technology in a Digital Age*. Washington DC, National Academies Press.

Warren SD and Brandeis DL (1890) The right to privacy. *Harvard Law Review* **4(5)**, 193–220.

Webster J and Ahuja JS (2006) Enhancing the design of Web navigation systems: the influence of user disorientation on engagement and performance. *MIS Quarterly* **30(3)**, 661–678.

Westin AF (1967) *Privacy and Freedom*. Atheneum, New York.

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

Xu H, Dinev T, Smith HJ and Hart P (2011) Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* **12(12)**, 798–824.

Xu H, Teo HH, Tan BCY and 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.

Young JB (1978) *Privacy*. Wiley, Chichester, UK.

Zwick D and Dholakia N (2004) Whose identity is it anyway? Consumer representation in the age of database marketing. *Journal of Macromarketing* **24(1)**, 31–43.

Appendix A

Measurement items (measured on 7-point Likert-type scale)

Perceived privacy (PRIV) When you answer the following questions about your privacy, please think about the limited access the Web sites have to your personal information

1. I feel I have enough privacy when I use these Web sites.
2. I am comfortable with the amount of privacy I have.
3. I think my online privacy is preserved when I use these Web sites.

Perceived information control (PCTL)

1. I think I have control over what personal information is released by these Web sites.
2. I believe I have control over how personal information is used by these Web sites.
3. I believe I have control over what personal information is collected by these Web sites.
4. I believe I can control my personal information provided to these Web sites.

Perceived privacy risk (RISK)

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

Anonymity (ANYT)

1. I believe I can hide my true identity on these Web sites.
2. I believe I can stay anonymous and do everything I want on these Web sites.
3. I can keep my information anonymous on these Web sites.

Secrecy (SCRT)

1. I believe, I can conceal some information from these Web sites when I want to.
2. I feel I can falsify some of my personal information if it is asked for by these Web sites.
3. I believe, I can refuse to give my personal information to these Web sites when I think it is too personal.

Confidentiality (CFDT)

1. I believe my personal information provided to these Web sites remains confidential.

2. I believe these Web sites will prevent unauthorized people from accessing my personal information in their databases.
3. I believe my personal information is accessible only to those authorized to have access.

Information sensitivity (IS) When visiting Web sites that collect information, many people find there is some information that they generally feel comfortable providing, some information they feel comfortable providing only under certain conditions, and some information is too personal that they never or rarely feel comfortable providing. Please indicate how much you agree with the following statements:

1. I do not feel comfortable with the type of information these Web sites request from me.
2. I feel that these Web sites gather highly personal information about me.
3. The information I provide to these Web sites is very sensitive to me.

Perceived benefits of information disclosure (BEN)

1. Revealing my personal information on these Web sites will help me obtain information/products/services I want.
2. I need to provide my personal information so I can get exactly what I want from these Web sites.
3. I believe that as a result of my personal information disclosure, I will benefit from a better, customized service and/or better information and products.

Importance of information transparency (TR) *Please specify the importance of …*

1. whether these Web sites will allow me to find out what information about me they keep in their databases;
2. whether these Web sites tell me how long they will retain information they collect from me; and
3. the purpose for which these Web sites want to collect information from me.

Regulatory expectations (LAW)

1. I believe that the law should protect me from the misuse of my personal data by online companies.
2. I believe that the law should govern and interpret the practice of how online companies collect, use, and protect my private information.
3. I believe that the law should be able to address violation of the information I provided to online companies.

Appendix B

Mediation tests

To obtain further insight into the potential mediating effects of perceived information control, we conducted a *post hoc* analysis following Baron and Kenny's (1986) recommendations for examining the mediating effects. In a mediation relationship, there is a direct effect between an independent variable (IV) and a DV and also indirect effects between an IV and a mediator variable, and between a mediator variable and a DV. Mediation is useful when we need to explain how the IV–DV relationship can be statistically explained by the IV–Mediator–DV relationship.

Baron and Kenny's (1986) argue that mediation is demonstrated if three conditions are fulfilled: the first condition stipulates that the IV must significantly affect the proposed mediator. As shown in Regression (1) in Table B1, the relationships between the proposed mediator (perceived information control) and the three

Table B1 Testing the mediating effects of perceived information control (PCTL)

Regression	*Dependent variable*	*R^2 (%)*	*β*
Regression (1)	Perceived Information Control (PCTL)	31.8	
Anonymity (ANYT)			0.223**
Secrecy (SCRT)			0.220**
Confidentiality (CFDT)			0.191**
Regression (2)	Perceived Privacy (PRIV)	23.9	
Anonymity (ANYT)			0.285**
Secrecy (SCRT)			0.257**
Confidentiality (CFDT)			0.014
Regression (3)	Perceived Privacy (PRIV)	47.2	
Anonymity (ANYT)			0.148*
Secrecy (SCRT)			0.151**
Confidentiality (CFDT)			0.142
Perceived Information Control (PCTL)			0.584**

*$P<0.05$, **$P<0.01$.

Table B2 Testing the mediating effects of perceived risk (RISK)

Regression	*Dependent Variable*	*R^2 (%)*	*β*
Regression (1)	Perceived Risk (RISK)	37.1	
Perceived Benefits of Info. Disclosure (BEN)			−0.315**
Information Sensitivity (IS)			0.160**
Expectations of Info. Transparency (TR)			0.188*
Regulatory Expectations (LAW)			0.217**
Regression (2)	Perceived Privacy (PRIV)	34.5	
Perceived Benefits of Info. Disclosure (BEN)			0.200**
Information Sensitivity (IS)			−0.430**
Expectations of Info. Transparency (TR)			−0.049
Regulatory Expectations (LAW)			−0.147
Regression (3)	Perceived Privacy (PRIV)	38.9	
Perceived Benefits of Info. Disclosure (BEN)			0.148*
Information Sensitivity (IS)			−0.409**
Expectations of Info. Transparency (TR)			−0.042
Regulatory Expectations (LAW)			−0.146
Perceived Risk (RISK)			−0.150**

*$P<0.05$; **$P<0.01$.

IVs were all significant. The second condition requires the IV must significantly affect the DV. As shown in Regression (2) in Table B1, anonymity (ANYT) and secrecy (SCRT) were significantly related to perceived privacy (PRIV). But confidentiality (CFDT) was not significantly related to perceived privacy (PRIV). The last condition stipulates that the relationship between the IV and the DV should be weaker or insignificant when the proposed mediator is in the regression equation than when the proposed mediator is not in the equation. The results, shown in Regression (3) in Table B1 indicated that β for anonymity ($\beta=0.285$ compared with $\beta=0.148$) and β for secrecy ($\beta=0.257$ compared with $\beta=0.151$) were lower when perceived information control (PCTL) was included in the model. Table B1 summarizes the results for testing the mediating effect of perceived information control, which indicate partial mediation except for confidentiality, transparency, and regulatory expectations, which were not mediated.

Similarly, we conducted a *post hoc* analysis following Baron and Kenny's (1986) recommendations for examining the mediating effects of perceived risk (RISK). Table B2 summarizes the results, which indicated that RISK mediates the effects of perceived benefits of information disclosure (BEN) and information sensitivity (IS) on perceived privacy (PRIV). However, the results failed to demonstrate the mediation effect of RISK for the relationship between expectations of information transparency (TR) and perceived privacy (PRIV), as well as for the relationship between regulatory expectations (LAW) and perceived privacy (PRIV).

In all, Baron and Kenny mediation tests provided above did not bring a conclusive argument about the extent of the partial mediation, especially the importance of the non-hypothesized relationships between the seven leftmost exogenous variables in our model, and the DV of perceived privacy. It is not known how much more explanatory power is brought into the model if these relationships are present in our model in the first place. To further investigate the mediation effects and empirically validate our model by SEM methods rather than the simpler multiple regression techniques, we ran the fully saturated PLS model, per the recommendations by Gefen *et al* (2011, p. viii) who discussed the importance of the saturated model in SEM validation. Per the authors:

> This is rarely done in reported PLS research but it should. It is mainly needed to compare the theoretical model, which includes only the hypothesized paths, with the saturated model, which includes all possible paths in order to verify (1) that the significant paths in the theoretical model also remain significant in the saturated model, and (2) that adding the paths via the saturated model does not significantly increase the f^2, a standard measure of effect size. By convention, f^2 values of 0.02, 0.15, and 0.35 are labeled small, medium, and large effects, respectively, f^2 is calculated as (R^2 saturated model−R^2 theoretical model/(1−R^2 saturated model).

Table B3 presents the results from the saturated model and the comparison with the results from the hypothesized model. One can see that both conditions are met: first, all the significant paths in our theoretical model also remain significant in the saturated model; and second, with the only exception of information sensitivity, none of the leftmost variables have direct effect to perceived privacy. This result indicates full mediation for the six of the seven leftmost variables. Adding the additional paths in the saturated model changed the R^2 from 52.2 to 56.1%, giving a small effect size of 0.089. This procedure validated our theoretical model. While the significance of the direct

Table B3 Theoretical and saturated structural models

	Effect	*Model 1* *Theoretical model*		*Model 2* *Saturated model*	
		Path coefficients	*t-value*	*Path coefficients*	*t-value*
Perceived information control	Anonymity	0.223**	2.90	0.226**	3.11
	Secrecy	0.220**	2.47	0.210*	2.32
	Confidentiality	0.191**	2.78	0.202*	2.26
	R^2 (%)	**31.8**		**31.5**	
Perceived privacy risk	Perceived benefits of information disclosure	−0.315**	4.86	−0.311**	4.80
	Information sensitivity	0.160**	2.65	0.146*	1.94
	Importance of information transparency	0.188*	2.29	0.190*	2.30
	Regulatory expectations	0.217**	2.54	0.219**	2.62
	R^2 (%)	**37.1**		**36.1**	
Perceived privacy	Perceived information control	0.620**	11.47	0.503**	8.04
	Perceived privacy risk	−0.211**	4.00	−0.111*	1.83
	Anonymity			0.095	1.31
	Secrecy			0.129	1.64
	Confidentiality			0.107	1.32
	Perceived benefits of information disclosure			0.096	1.64
	Information sensitivity			−0.133*	1.90
	Importance of information transparency			−0.021	0.37
	Regulatory expectations			0.035	0.51
	R^2 (%)	**52.2**		**56.1**	

*Significant at 5% level; **significant at 1% level.

effect of Information sensitivity to perceived privacy is relatively small, possible theoretical underpinning of the relationship should be considered in future research.

Finally, an additional insight about the mediation can be obtained by performing a pseudo *F*-test, per Burton-Jones and Straub (2006). Applying the test to our data yields a pseudo *F*-test of 16.198, which is not significant ($16.198 > 0.05$). This demonstrates that the saturated model did not explain significantly more R^2 than did our original model.