State of the Information Privacy Literature: Where are We Now And Where Should We Go?
Author(s): Paul A. Pavlou
Source: *MIS Quarterly*, Vol. 35, No. 4 (December 2011), pp. 977-988
Published by: Management Information Systems Research Center, University of Minnesota
Stable URL: http://www.jstor.org/stable/41409969
Accessed: 11-02-2018 16:34 UTC

REFERENCES
Linked references are available on JSTOR for this article:
http://www.jstor.org/stable/41409969?seq=1&cid=pdf-reference#references_tab_contents
You may need to log in to JSTOR to access the linked references.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at http://about.jstor.org/terms

Management Information Systems Research Center, University of Minnesota is collaborating with JSTOR to digitize, preserve and extend access to *MIS Quarterly*

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

MIS Quarterly

THEORY AND REVIEW

STATE OF THE INFORMATION PRIVACY LITERATURE: WHERE ARE WE NOW AND WHERE SHOULD WE GO?

Paul A. Pavlou
Fox School of Business, Temple University, 334 Alter Hall,
Philadelphia, PA 19122 U.S.A. {pavlou@temple.edu}

While information privacy has been studied in multiple disciplines over the years, the advent of the information age has both elevated the importance of privacy in theory and practice, and increased the relevance of information privacy literature for Information Systems, which has taken a leading role in the theoretical and practical study of information privacy. There is an impressive body of literature on information privacy in IS, and the two Theory and Review articles in this issue of MIS Quarterly review this literature. By integrating these two articles, this paper evaluates the current state of the IS literature on information privacy (where are we now?) and identifies promising research directions for advancing IS research on information privacy (where should we go?). Additional thoughts on further expanding the information privacy research in IS by drawing on related disciplines to enable a multidisciplinary study of information privacy are discussed.

Keywords: Information privacy, personal information, information privacy concerns

Introduction

Information privacy refers to the concept of controlling how one's personal information is acquired and used (e.g., Stone et al. 1983; Warren and Brandeis 1890; Westin 1967). Despite the relative simplicity of most definitions of information privacy (maintaining control over one's personal information), there has been a tremendous amount of research across disciplines over the years. Nevertheless, much ambiguity and disagreement still surrounds the concept of information privacy. This is because information privacy is an arguably complex concept that can be studied from many perspectives, including law, economics, psychology, management, marketing, and Information Systems. Accordingly, there is a very rich literature on information privacy that is dispersed across multiple disciplines, and there is a plethora of insights on the nature, antecedents, and outcomes of information privacy and related constructs, such as information privacy concerns, attitudes, regulations, policies, and practices.

The advent of the information age has exacerbated concerns about information privacy (Davies 1997). The global and open nature of the Internet allows personal information to be easily collected, stored, processed, and utilized by multiple parties, both within and outside a specific economic exchange, thereby making information privacy concerns a major issue for the information age (Smith et al. 2011). Specifically, the tension between the proper use of personal information and information privacy has been touted as one of the most serious ethical debates of the information age (Mason 1986). Furthermore, advances in information technology have greatly expanded opportunities for technical solutions to address information privacy concerns (Bélanger and Crossler 2011), further allowing IS researchers to take a leading role in the practical implementation of technological solutions to mitigate information privacy concerns. Therefore, the information age has rendered information privacy a core topic in IS research.

In e-commerce relationships, the issue of information privacy is also taking center stage. Websites (firms) collect information about customers through their websites to capture their needs and strategically use the information for customized promotions. While commercial websites increasingly rely on collecting consumer information to formulate their marketing strategies (Bessen 1993), consumers often view this practice as an invasion of their information privacy (Culnan and Armstrong 1999). As more and more consumers become anxious

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

about protecting their personal information from commercial websites, privacy is becoming a major concern for consumers (Pavlou and Fygenson 2006). For example, Wang and Emurian (2005) showed that information privacy concerns are "a most formidable barrier to people engaging in e-commerce" (pp. 105-121). Still, sharing of personal information is necessary to establish a relationship between websites and consumers, thus raising the importance of information privacy in e-commerce relationships. The collection of personal information lays a heavy burden on firms to ensure adequate privacy protection (Miller and Tucker 2009). Because concerns about information privacy have taken central sage in e-commerce relationships, information privacy has even further attracted the interest of IS researchers.

Given the relevance of information privacy for IS researchers with the advent of the information age and the emergence of e-commerce, there is an impressive body of literature on information privacy in Information Systems. Accordingly, the two Theory and Review articles appearing in this issue of *MIS Quarterly* seek to review and guide information privacy research in the IS literature. By integrating these two manuscripts, this paper aims to evaluate the current state of the IS literature on information privacy (where are we now?) and identify promising research directions for further advancing IS research on information privacy (where should we go?).

Overview of the Two Articles

Both the article by Bélanger and Crossler and the article by Smith, Dinev and Xu provide excellent coverage of the current state of the broader literature on information privacy with primary emphasis on the Information Systems and selective coverage of related fields, such as economics and law. Moreover, both papers offer a synthesis of the literature that results in several specific recommendations for future IS research on information privacy.

This paper offers an overview of the main points and recommendations of the two Theory and Review articles, and then attempts to integrate the articles to answer two fundamental questions: where are we now and where should we go?

Review of "Privacy in the Digital Age" (Bélanger and Crossler)

Bélanger and Crossler provide a critical analysis of the IS literature on information privacy based on an in-depth review of over 100 journal articles and over 100 conference proceedings papers derived from an analysis of a total of over 500 articles. Their review starts by classifying the contributions made by these studies to the information privacy literature, followed by a classification based on the level of analysis (Skinner et al. 2006), the nature of the underlying theory (Gregor 2006), and sample characteristics of the populations used in these studies of information privacy in the IS literature.

Conceptualization of Information Privacy

Bélanger and Crossler offer a rich discussion on the definition, nature, and conceptualization of information privacy, drawing on studies that have viewed privacy as a moral or legal right (e.g., Clarke 1999) and the ability to control one's personal information (e.g., Stone et al. 1983). Specifically, Clarke (1999) identified four distinct dimensions of privacy: privacy of a person, behavior privacy, communication privacy, and data privacy. Bélanger and Crossler argue that personal communication and data privacy can be merged into the information privacy construct given the digitization of information and communications, thereby focusing the broader privacy literature on the concept of information privacy.

Bélanger and Crossler review multiple definitions of information privacy in the literature, concluding that one's control over personal information, particularly the secondary uses of this information, is a common theme across most studies on information privacy (Bélanger et al. 2002). While several definitions and dimensions of information privacy are reviewed by the authors (e.g., Skinner et al. 2006; Smith et al. 1996; Solove 2006), the study relies on a definition of information privacy based on Clarke, specifically, the interest people have in controlling, or at least significantly influencing, the handling of information about themselves.

Information Privacy Concerns

Considerable emphasis is paid by Bélanger and Crossler to concerns about information privacy following the literature on organizational practices (Smith et al. 1996) and the general notion of an individual's subjective view of fairness regarding information privacy (Malhotra et al. 2004). Information privacy concerns are usually measured in the IS literature using self-reported scales (e.g., Malhotra et al. 2004; Smith et al. 1996; Stewart and Segars 2002). While researchers used many variations of these scales using different dimensions of information privacy concerns, there is a general consensus in the literature that information privacy concerns correspond to a person's willingness to render personal information (e.g., Dinev and Hart 2006), transaction activity (e.g., Pavlou et al. 2007), and government regulation (Milberg et al. 2002).

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

Relationship of Information Privacy with Related Concepts

Bélanger and Crossler provide a broad overview of studies that have examined the effects of information privacy concerns, such as intentions to use various types of online services (e.g., Bélanger et al. 2002), disclose personal information (e.g., Culnan and Armstrong 1999), engage in e-commerce transactions (Dinev and Hart 2006), and undertake online purchases (Brown and Muchira 2004). The concept of attitudes toward information privacy is also reviewed, which often has different connotations, such as attitude toward privacy in general (e.g., Razzouk et al. 2008), attitude toward privacy practices (Miyazaki and Krishnamurthy 2002), attitude toward other people's privacy (Earp and Payton 2001), or attitude toward data access (Mossholder et al. 1991). While the multitude of information privacy attitudes makes it difficult to have a coherent stream of literature (Bélanger and Crossler 2011), an interesting finding is that, in the presence of information privacy attitudes, information privacy concerns no longer seem to affect an individual's willingness to disclose personal information. Finally, how information privacy concerns can be mitigated with various means, such as monetary incentives (Hui et al. 2007), and privacy attitudes in the context of RFID are deemed an important question for future research by Bélanger and Crossler.

Information Privacy Practices

Bélanger and Crossler also review various individual and organizational actions regarding information privacy protection. In terms of individual practices, while the literature suggests that people are not always knowledgeable about proper practices to protect their personal information, there is much literature that instructs people to be cautious when divulging personal information and using proper software to protect their privacy (Chen and Rea 2004). In terms of organizational practices, the literature has focused on instituting appropriate policies, designing fair information practices, and complying with the organization's privacy policies. Special emphasis has been paid in the literature to how information privacy practices deal with the protection of consumers' personal information (Bélanger and Crossler 2011).

Information Privacy Tools and Technologies

Research on information privacy tools and technologies focuses on privacy invasive technologies and privacy enhancing technologies based on an examination of privacy threats and corresponding solutions. Most of this line of work has been conducted by computer scientists (not IS researchers), and much of the work is largely conceptual as opposed to implementable with specific technological tools and solutions. Bélanger and Crossler identify a gap in this literature in the sense that the user's input has not been adequately examined in studies on the conceptual design of information privacy tools and technologies, thereby creating an opportunity for IS researchers to examine the user's input and feedback into the design and implementation of information privacy tools and technologies.

Sample Characteristics in IS Information Privacy Research

Bélanger and Crossler also examine the nature of the respondents in studies of information privacy in the IS literature. In terms of studies on information privacy concerns, practices, and attitudes, they find that most studies use consumers and professionals (versus students); however, in terms of information privacy in e-commerce, samples tend to be distributed equally between students and consumers/citizens. In general, while student data can be informative, the notion of generalizability using diverse populations is stressed by Bélanger and Crossler. Moreover, the country of origin of respondents in information privacy studies is reviewed by Bélanger and Crossler, and they note that the majority of studies are conducted in the United States. Accordingly, there is little knowledge on information privacy differences across countries. Nonetheless, Bélanger and Crossler review several conference proceedings papers on information privacy that have used data from countries other than the United States, and many interesting differences exist across countries, such as differences in the level of information privacy concerns across individuals and information privacy practices. They conclude by stressing the need for more studies on information privacy in multiple countries using, preferably, non-student populations.

Levels of Analysis

Bélanger and Crossler also analyze the information privacy literature across levels of analysis, concluding that most studies have been conducted at the individual level of analysis. They also note that information privacy could be conceptualized as a multilevel concept, albeit information privacy was not adequately researched across multiple levels. Bélanger and Crossler offer a detailed analysis of the literature on information privacy on each of the four levels of analysis (individual, group, organizational, and societal), and accordingly propose that more studies need to be conducted at the group, organizational, and societal levels, specifically to concurrently examine multiple levels and their interactions by viewing information privacy as a multilevel concept. The authors conclude their analysis by focusing on information

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

privacy concerns as a concept that lends itself to multiple levels of analysis, and they accordingly propose a multilevel model of information privacy concerns (Figure 2, p. 1032). Finally, Bélanger and Crossler propose a set of research questions that can be posed by adopting a multilevel perspective on information privacy and integrating the four levels of analysis.

Conclusions and Recommendations

Finally, Bélanger and Crossler categorize the papers in their literature review using Gregor's (2006) categorization of theory contributions. The results show that the majority of the literature on information privacy focuses on *explaining and predicting*, followed by *analyzing* as the second major area, while *design and action* was distant third. Accordingly, they suggest that IS research should focus more on design and action with emphasis on building actual implementable tools to protect information privacy. Specifically, building on their analysis of the various levels of analysis, Bélanger and Crossler recommend that IS researchers consider the development of more and easier to use information privacy protection tools and technologies for individuals, groups, organizations, and society. In conclusion, Bélanger and Crossler offer five recommendations for information privacy research (Table 4, p. 1035): (1) move beyond the individual level of analysis and explore the other four levels of analysis, (2) utilize a broader diversity of sample populations, (3) conduct more design and action research, (4) conduct more studies investigating the *why* related to privacy as opposed to the *how*, and (5) justify the use of existing construct measurements and develop more common measurements to be used across studies.

Review of "Information Privacy Research" (Smith, Dinev, and Xu)

Smith, Dinev, and Xu provide an interdisciplinary review of privacy-related research in order to enable a more cohesive treatment of the information privacy literature. They categorize a large sample of 320 privacy articles, books, and book sections in two categories: (1) using an ethics-based nomenclature of normative, purely descriptive, and empirically descriptive studies, and (2) based on their level of analysis: individual, group, organizational, and societal. Furthermore, Smith, Dinev, and Xu direct their attention to three major areas in which the IS literature on information privacy has primarily focused: (1) the conceptualization of information privacy, (2) the relationship between information privacy and related constructs, and (3) the contextual nature of information privacy and its relationships in various contexts.

Conceptualization of Information Privacy

While there is considerable work on information privacy, Smith, Dinev, and Xu find that much of the confusion surrounding the conceptualization of information privacy is because the concept has different meanings across disciplines, such as a right or entitlement (in the law literature), a state of limited access or isolation (in the social psychology literature), and control over information (in the information systems literature). Interestingly, the Younger Committee Report (1972) concluded that general privacy could not be satisfactorily defined. Smith, Dinev, and Xu review many approaches to defining general privacy across various disciplines, broadly classified as either *value-based* or *cognate-based* (Figure 1, p. 992, and Table B4). Value-based definitions view general privacy as a human right integral to society's moral value system. As reviewed by Smith, Dinev, and Xu, the article by Warren and Brandeis (1890) in *Harvard Law Review* defined general privacy as "the right to be left alone." Notably, the perspective of "privacy as a right" has since shaped numerous opinions and has been given constitutional sanction by the U.S. Supreme Court (Breckenridge 1970).

The role of context shapes the meaning and conceptualization of information privacy. Bansal et al. (2008) elaborated on context to refer to discipline, time, location, occupation, culture, and rationale, all of which may alter the meaning of information privacy. Following the importance of context, Smith, Dinev, and Xu examine various facets of context that shape the meaning of information privacy, namely information sensitivity, industry sector, political sector, and technological applications. Summarizing these various perspectives related to the conceptualization of information privacy, Smith, Dinev, and Xu conclude there is no single concept of information privacy that crosses all disciplines and that could be embraced by all observers. Nonetheless, they distinguish between information privacy and other related constructs, such as anonymity, secrecy, transparency, confidentiality, security, and ethics. This is an important contribution given the need to clearly distinguish a construct (information privacy) from related constructs, and there are ongoing debates regarding the distinction between privacy and related constructs, such as anonymity and security.

Relationship of Information Privacy with Related Concepts

Perhaps the most important question raised by Smith, Dinev, and Xu in regard to the relationship between information privacy and other constructs is the extent to which the context matters in the relationships between information privacy and

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

other constructs. In the literature, there is a disagreement regarding the extent to which these relationships are generalized across contexts, such as different types of information, different industries, and new technological applications. This follows the notion that the context changes the very meaning and conceptualization of information privacy, and therefore it is likely to change its relationship with other constructs.

Smith, Dinev, and Xu find that the most common dependent variables of information privacy deal with an individual's willingness to disclose information and engage in transactions with others. Moreover, trust has been viewed as an interrelated variable to information privacy. Notably, some studies view trust as a mediator between information privacy and willingness to disclose private information (e.g., Dinev and Hart 2006), some view trust as an antecedent of privacy (e.g., Bélanger et al. 2002; Eastlick et al. 2006), others describe trust as a consequence of information privacy (Bansal et al. 2010; Malhotra et al. 2004), while others view trust as a moderator of the effects of information privacy on behavior (Bansal et al. 2008). Moreover, information privacy concerns seem to have a weaker effect on online consumer behavior relative to trust (Ba and Pavlou 2002; Pavlou and Gefen 2004). In sum, reducing information privacy concerns highly correlates with trust, albeit the exact (causal) directionality of the relationship (Zheng and Pavlou 2010) is still a debated issue in the literature.

Privacy Paradox and the Privacy Calculus

The *privacy paradox* was described as the phenomenon where an individual expresses strong privacy concerns but behaves in a contradictory way to these concerns. For example, despite self-reported privacy concerns, some consumers still share their personal information (e.g., Acquisti and Grossklas 2005). There are several explanations for this interesting paradox. Privacy is not absolute, and it can be assigned an economic value based on economic principles, such as a cost–benefit calculation (Bennett 1995). However, because the benefits and risks of disclosing personal information may spread over time, different people may differentially assess the costs and benefits of information privacy (Acquisti 2004), and thereby act in a seemingly irrational way by assigning different discounting to their expected future benefits and costs.

Related to the privacy paradox, there is also considerable work on the *privacy calculus* (e.g., Ackerman 2004), namely, that consumers will seek reveal certain information about themselves to obtain certain benefits. This follows the economic view that rational consumers are willing to reveal private information about themselves to marketers in exchange for specific benefits but they would still keep other information as a secret if they do not expect to receive any benefits (Varian 1996). Pursuing this privacy calculus, Smith, Dinev, and Xu review an abundance of literature on concerns and benefits of information privacy.

Concerns for Information Privacy

The excessive use of personal information hurts consumer privacy in two major ways. First, the improper use of personal information due to lack of appropriate privacy controls (Smith et al. 1996), such as by unsolicited e-mails, credit card fraud, or identity theft. This is casually referred to as the right not to be disturbed. Second, the unauthorized use of personal information without the consumer's consent for purposes outside of the original exchange (Culnan 1993). Accordingly, concerns about information privacy relate to the improper use of personal information, disclosure of personal information to outside parties, and the unauthorized secondary use of personal information without the individual's consent. The concept of information privacy risk has been proposed as an antecedent of information privacy concerns (e.g., Dinev and Hart 2006), often described as the degree to which an individual perceived a potential for a loss associated with personal information (Featherman and Pavlou 2003).

Benefits of Information Privacy

Smith, Dinev, and Xu also review the benefits of information privacy using the notion of privacy as a commodity. According to Bennett (1995), consumers voluntarily disclose their private information because they view privacy as a commodity that can be sacrificed in return for economic benefits. For example, websites collect personal information in exchange for customized advertising that better fits the consumers' needs (Wang and Wang 1998). Moreover, when consumers are comfortable with the process by which their personal information is managed, they are less concerned about their privacy (Sheehan and Hoy 2000), and they may be more comfortable pursuing the benefits from sacrificing their information privacy (White 2004). Smith, Dinev, and Xu proposed three major types of information privacy benefits—*financial rewards*, *personalization*, and *social adjustment benefits*—which were reviewed in the following studies that focused on the privacy calculus by contrasting privacy concerns with expected benefits. Phelps et al. (2000) presented a conceptual model in which consumers' privacy concerns are determined by the type of personal information requested, the amount of information control offered, and the potential consequences and benefits offered in the exchange. Hann et al. (2008) also showed that consumers' willingness to provide personal information over the Internet involves weighing privacy concerns, the website's privacy protection, and the

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

benefits exchanged with their information. Similarly, Awad and Krishnan (2006) showed that consumers with a high level of privacy concerns are likely to perceive personalized offerings to be of less value to them than consumers with a low level of privacy concerns. In addition, Kobsa and Teltzrow (2005) showed that website users disclosed significantly more information about themselves when the website explained the site's privacy protection practices and the users' benefits pertaining to each of the requested pieces of personal information. Finally, Xu et al. (2010) examined the role of push–pull technology in shaping the privacy calculus, showing that location-based services can shift the benefits of personalization relative to privacy concerns.

Levels of Analysis

When privacy is measured as privacy concerns, it is almost always the case that it is captured at the *individual* level of analysis. This is largely because the individual can assess the consequences of information disclosure (Xu et al. 2008), suffer from personal information abuses (Smith et al. 1996), and be informed about the information practices of the entity he or she engages with (Culnan 1985, Malhotra et al. 2004; Phelps et al. 2000). Privacy concerns are also associated with personality differences (Bansal et al. 2010), demographic differences (Culnan 1993; Culnan and Armstrong 1999; Sheehan 1999; 2002), and cultural differences (Dinev et al. 2006a; 2006b). Besides the individual level on which much of the literature has focused, there is considerably less work on the group and organizational levels (Smith et al. 2011). However, there is relatively more work at the societal level. Notably, work on information privacy at the societal level has primarily focused on regulation and how industry self-regulation and government regulation should protect citizens' right to privacy. Smith, Dinev, and Xu review the extensive research on market regulation related to information privacy, ranging from societal differences in treating information privacy as a right versus a commodity (Jentzsch 2001), contrasting European and American approaches to information privacy in online markets (Dholakia and Zwick 2001), and the relative role of industry self-regulation (Hui et al. 2007).

Conclusions and Recommendations

Smith, Dinev, and Xu offered three overarching conclusions that help guide future research. First, despite many theoretical developments on information privacy based on normative studies, empirically descriptive studies are deemed to have the potential to add value to the literature. Second, some of the levels of analysis have received much less attention in the privacy literature; accordingly, Smith, Dinev, and Xu call for future research on these under-researched levels of analysis, namely the group and organizational level of analysis. Third, empirical studies are proposed to add the greatest value if they focus on antecedents to privacy concerns and on actual outcomes. Accordingly, the authors recommend that researchers be alert to an overarching macro model with the following order: Antecedents → Privacy Concerns → Outcomes (APCO).

Integration of the Two Articles

In attempting to integrate the two articles and identify common themes and opportunities, I focused on their similarities and differences in terms of (1) how they evaluate the state of the literature on information privacy (where are we now?) and (2) what avenues for future research they proposed based on their identified gaps in the literature (where should we go?).

Where Are We Now?

Conceptualization of Information Privacy

Both papers note the inherent difficulties associated with conceptualizing and defining the concept of information privacy. While Bélanger and Crossler offer a specific definition of information privacy to guide their analysis (consistent with the notion of individuals having some level of control and influence over their personal information), Smith, Dinev, and Xu stress the difficulty of a well-accepted definition and maintain that several factors may change the meaning of information privacy. Nonetheless, both articles use the term information privacy in a similar fashion, which is largely consistent with the overall conceptualization and meaning of the concept in the IS literature, thereby making it possible to readily compare their findings. Interestingly, the conceptualization of the concept of information privacy was not noted as an important avenue for future IS research, perhaps implying that it may not be possible to reach a consensus on the conceptualization of information privacy, or there is little IS research can further contribute to the definition of information privacy. This is perhaps a valid observation from both articles given that the Younger Committee Report (1972) concluded that privacy could not be satisfactorily defined.

Information Privacy Concerns

Both articles emphasize the importance of information privacy concerns as a unique construct that has received considerable attention in the IS literature. Smith, Dinev, and Xu focus on information privacy concerns in relation to the privacy calculus, where information privacy concerns must be

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

contrasted with specific benefits, while Bélanger and Crossler focus on information privacy concerns in its own right. Nonetheless, both articles explain the nature of concerns surrounding information privacy, and they provide an exhaustive set of IS studies that have examined information privacy concerns. Taken together, the two articles stress the importance and provide a comprehensive coverage of the concept of information privacy concerns that has attracted much interest in the IS literature. Notably, Smith, Dinev, and Xu position information privacy concerns as a key mediating variable in their proposed macro-level model, while Bélanger and Crossler stress the need for more precise measurement of information privacy concerns.

Relationship between Information Privacy and Related Constructs

Both articles note that the information privacy literature has overlapping constructs nestled within loosely bounded nomological networks, with Smith, Dinev, and Xu attempting to provide a generic model around information privacy concerns and Bélanger and Crossler focusing on specific effects of information privacy concrns. As noted above, special attention was given by both articles to information privacy concerns, emphasizing the demonstrated effects of information privacy concerns on multiple outcomes, such as people's intentions to share personal information, intentions to transact with other entities, and broader economic effects. Taken together, the articles provide comprehensive coverage of multiple constructs that have various relationships with information privacy concerns.

Trust is specifically noted as a closely related variable, and both articles cite several studies that simultaneously examined information privacy and trust. While different studies offer somewhat contradictory results regarding the exact relationship and relative effects of trust and information privacy, in general, trust is usually viewed as a stronger predictor of behavior that often mediates the relationship between information privacy concerns and willingness to transact (Van Slyke et al. 2006). In summary, trust and information privacy are closely linked concepts that are usually simultaneously examined in the literature, but there is a need for future research to test the mediating or stronger effect of trust relative to information privacy (e.g., Bélanger et al. 2002; Pavlou et al. 2007; Van Slyke et al. 2006).

Finally, both articles note the privacy paradox in the literature where an individual's concerns about information privacy do not necessarily map with the individual's intentions to share personal information (e.g., Norberg et al. 2007). Smith, Dinev, and Xu provide a potential explanation based on the economics literature that is based on the notion that individuals differentially discount risks and benefits over time, thereby blurring their privacy calculus. Nonetheless, the trade-off between the costs (risks) and benefits of information privacy is an important question that has broader theoretical and practical implications, as I discuss below.

Where Should We Go?

A critical aspect for Theory and Review pieces is to offer novel avenues for future research by building on the analysis and critique of the literature, the identified gaps in the literature, and new opportunities that arise by challenging some of the assumptions in the literature. These two articles take different perspectives on the direction information privacy research should go and accordingly offer quite distinct recommendations for future research in the area.

Descriptive Versus Prescriptive (Design) Studies?

Perhaps the most immediate distinction between the two articles lies in their recommendations for the type of studies (descriptive or explanatory versus predictive or design; Gregor 2006) that should be undertaken. Smith, Dinev, and Xu note that most existing studies in the broader literature are normative in nature, prescribing how information privacy laws, regulations, policies, and practices should be formed (therefore proposing the need for more empirical descriptive or explanatory studies). Bélanger and Crossler note that much of the IS literature on information privacy focused on explaining and predicting, with only a few studies focused on prescription (design and action).

While there is some apparent contradiction in these recommendations at first glance, Bélanger and Crossler call for design and action research that focuses on the design of IT artifacts for the protection and control of information privacy, which is rather different from the traditional normative studies in economics and law. This is consistent with the design science perspective in IS research, which aims to build specific tools and technologies to deal with various aspects of information privacy, such as information privacy concerns. Similarly, Smith, Dinev, and Xu call for moving away from normative studies about "how" things should be in relation to information privacy and more empirical descriptive studies that aim at explaining "why" certain things occur. In fact, Bélanger and Crossler's fourth major recommendation (Table 4, p. 1035) calls for "conducting more studies investigating the *why* related to privacy as opposed to the *how*." There is no contradiction between the two studies, but Bélanger and Crossler focus primarily on design and action studies that

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

would enable IS researchers to build information privacy technologies and tools, and Smith, Dinev, and Xu refer to the broader information privacy literature that goes beyond IS studies.

Levels of Analysis

Both articles recognize that information privacy is a multilevel phenomenon, and both articles also determine that information privacy has rarely been studied as a multilevel concept. There is a strong consensus that the great majority of the information privacy literature is based on studies at the individual level of analysis. Therefore, both articles recommend future research on the other levels of analysis, with Smith, Dinev, and Xu proposing future research on the group and organizational level of analysis, that has not received much attention in the literature compared to the individual and societal levels, and Bélanger and Crossler proposing future studies on multilevel effects of information privacy and research across levels. In sum, both articles note the apparent lack of studies on the group and organizational level of analysis, and they both call for future research to go beyond the individual level of analysis. Moreover, an interesting perspective offered by Bélanger and Crossler is to conduct studies across two or more levels of analysis to examine potential interactions among levels by viewing information privacy as a multilevel concept.

Measurement of Privacy

As with many complex constructs, perhaps the most challenging element of the information privacy literature is the precise measurement of the construct of information privacy. As noted by Smith, Dinev, and Xu, "because of the near impossibility of measuring privacy itself…almost all empirical privacy research in the social sciences relies on measurement of a privacy-related proxy of some sort" (p. 997). Information privacy concerns have often been used as a proxy for information privacy starting with the work of Smith et al. (1996) who developed the *concern for information privacy* scale with four interrelated dimensions (collection, errors, secondary use, and unauthorized access to information). Similar attempts were subsequently made by Stewart and Segars (2002) and Malhotra et al. (2004) to improve the scale of information privacy. Nonetheless, as maintained by Bélanger and Crossler, there is a need for more precise measurement of information privacy and more commonality in the methods used to capture information privacy in order to further advance the literature. Information privacy could also be considered a formative construct following Cenfetelli and Basselier (2009), Jarvis et al. (2003), and Petter et al. (2007).

Nomological Network of Information Privacy

While both studies agree on the relationships between information privacy (concerns) and other constructs, more emphasis on the relationships between information privacy and other constructs is recommended by Smith, Dinev, and Xu, who specifically propose the key mediating role of information privacy concerns. Smith, Dinev, and Xu call for additional research on identifying constructs that can mitigate information privacy concerns, which perhaps corresponds to Bélanger and Crossler's notion of conducting design and action studies to build technological tools to mitigate information privacy. While the difference in the two approaches lies in the type of research (explanatory versus design), both articles recognize the need for solutions to reduce information privacy concerns. Notably, it is critical to identify which factors can outweigh the effect of information privacy concerns on people's willingness to provide personal information to other entities in a relationship. And finally, while both articles reach a broad consensus on the effects of information privacy concerns, it is clear that more work could be conducted to identify all potential consequences of information privacy. Smith, Dinev, and Xu's macro level (APCO) model (Antecedents → Privacy Concerns → Outcomes) is a good starting framework.

Generalizability

Bélanger and Crossler note that most of the information privacy research has used student populations and been conducted in the United States. While not as explicitly stated by Smith, Dinev, and Xu, they also note the importance of examining differences across societies, cultures, and countries. Therefore, it is safe to conclude that the external validity of studies on information privacy is an open issue in the IS literature, and both articles seem to agree that future research could attempt to enhance the generalizability of existing findings. Notably, Bélanger and Crossler call for research to use a broader diversity of sampling populations by tapping nonstudent populations outside the United States, and this relates to Smith, Dinev, and Xu's recommendations for more empirical descriptive studies.

Further Thoughts

Taken together, these two articles provide excellent coverage of the IS literature on information privacy and provide several very promising avenues for future research that would certainly further advance IS research on information privacy and help maintain its leading role in the interdisciplinary study of privacy. Nonetheless, it is important to note some

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

potential extensions of these two articles that could help further advance research on information privacy in a truly interdisciplinary direction.

Economics of Information Privacy

First, while both articles have primarily focused on behavioral and organizational aspects of information privacy (which arguably spans the majority of studies in the IS literature), and besides a modest discussion on the information privacy paradox and the privacy calculus, the IS economics literature on information privacy has not received much attention. However, the very notion of information privacy has long been described as an economic trade-off between the costs and risks of sharing personal information relative to the economic benefits of revealing personal information (Posner 1978, 1981; Stigler 1980). This is because personal information is an economic good in markets with asymmetric information that relates to the agency problems of adverse selection and moral hazard (Pavlou et al. 2007). Specifically, individuals do not know *ex ante* which entities have appropriate information protection practices (adverse selection) and *ex post* whether their personal information will be inappropriately used (moral hazard). Accordingly, markets for managing customer information have long been established (Taylor 2004) with the primary purpose of managing personal information in optimal ways, and there is a rich body of research in IS economics that can further extend the literature on information privacy.

The trade-offs associated with sharing personal information with other entities have guided much research on information privacy from an IS economics perspective, such as the trade-off between information privacy and price sensitivity (e.g., Acquisti and Varian 2005), analyzing the choice between consumers opting for marketing promotions versus concealing their personal information (Hann et al. 2008), price discrimination (Odlyzko 2003), personalization versus privacy (Chellappa and Sin 2005), the economic effects of privacy seals (Benassi 1999) and other privacy assurances (Hui et al. 2007), the cost of privacy breaches (Acquisti et al. 2006) and the cost of privacy regulation (Miller and Tucker 2009), overcoming information privacy concerns with monetary incentives (Hann et al. 2007), how exclusive rights can help individuals control the collection and use of their personal information (Laudon 1996), the demographics of the do-not-call list (Varian et al. 2005), the firm's incentives and level of investment in collecting personal information (Taylor 2004), and the optimal level of government regulation in terms of information privacy protection (Tang et al. 2008).

In sum, there is a very rich body of research on information privacy that is based on information economics, and it is possible to integrate these findings with the broader IS literature on information privacy reviewed by Bélanger and Crossler and by Smith, Dinev, and Xu. For example, much of the work in IS economics is empirical and descriptive, thus informing the literature on descriptive studies that explains the dynamics of information privacy (following Smith, Dinev, and Xu's recommendation for more empirical descriptive studies). Besides, IS economics studies often explore variables related to information privacy, such as incentives to alleviate information privacy concerns, thereby contributing to Smith, Dinev, and Xu's suggestion for enhancing the nomological network of related constructs to information privacy. Finally, many IS economics studies are undertaken at the societal level, aiming to enhance the surplus for consumers and producers (firms), contributing to the information privacy literature on the societal level of analysis (which was recommended by both Bélanger and Crossler and by Smith, Dinev, and Xu). Accordingly, there are many opportunities for integrating the behavioral/organizational with the IS economics literature on information privacy, and the integration will help undertake the proposed recommendations in the two Theory and Review articles. Interested readers are directed to Hirshleifer (1971), Hui and Png (2006), and Varian (1996) for a detailed review of the literature on the economics of information privacy, which could help provide the fundamental economic principles needed to integrate these two streams of IS research.

Interdisciplinary Lens on Information Privacy

Second, both of these Theory and Review articles arguably focus on work on information privacy primarily conducted by IS researchers and published in IS journals. However, as clearly acknowledged in both articles, the field of information privacy is an inherently interdisciplinary one that transcends many fields, such as law and economics. Accordingly, there is much potential in integrating work in related disciplines when attempting to expand beyond the particular lens of IS, and in fact many of the proposed recommendations for future research by Bélanger and Crossler and by Smith, Dinev, and Xu could be informed by research in related disciplines. Specifically, the marketing and accounting literatures provide fertile ground for interdisciplinary work.

In marketing, there has been a very active body of research on information privacy (e.g., Rust et al. 2002; Wang and Wang 1998). Some notable studies include how much privacy matters in direct marketing (Nowak and Phelps 1997), how marketing incentives can be used to encourage consumers to provide their personal information (Ward et al. 2005), contextual factors that affect an individual's willingness to divulge personal information (John et al. 2011), what is the impact of relative judgments on privacy concerns (Acquisti et al. 2011),

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

the dimensionality of information privacy (Lwin and Williams 2003), and gender differences (Sheehan 1999). Marketing studies can be used to guide future research on several of the opportunities suggested by the two Theory and Review papers in this issue, such as providing additional empirical descriptive studies on information privacy (Smith, Dinev, and Xu), enhancing the measurement of information privacy concerns (Bélanger and Crossler), enriching the nomological network of information privacy with marketing constructs (Smith, Dinev, and Xu), and enhancing the generalizability of information privacy by tapping onto a larger population of consumers from different countries, cultures, and national origins (Bélanger and Crossler).

In accounting, there is also interest in information privacy with emphasis on reporting structures, disclosures, and assurance services in the e-commerce market (Sunder et al. 2003) and standards or evolution in privacy disclosure practices in e-commerce (Jamal et al. 2005). Accounting studies can be beneficial to the IS literature by helping guide design research (according to Bélanger and Crossler's recommendation for more design and action work), on how reporting structures, disclosure practices, and assurance services should be designed to reduce information privacy concerns and better regulate information privacy in e-commerce.

In sum, IS researchers may benefit from considering related streams of literature in marketing, accounting, and other disciplines, and the excellent recommendations proposed by Bélanger and Crossler and by Smith, Dinev, and Xu could be further enriched by studies on information privacy undertaken from an interdisciplinary perspective.

Concluding Remarks

These two Theory and Review pieces underscore the importance of information privacy in the IS literature and highlight the great advancements that IS research has offered in the broader literature on information privacy. Most important, the proposed recommendations pave the way for further advancing the field of information privacy by addressing important gaps (such as under-researched levels of analysis) and exploring promising opportunities (such as a multilevel view of information privacy and designing tools to combat information privacy concerns). Future IS research on information privacy could also draw on related disciplines, such as economics, marketing, and accounting, to lead a multidisciplinary study of information privacy and ensure that the contributions of IS research are widely disseminated across many disciplines. The ultimate goal of this paper is to entice researchers to build on the existing information privacy literature in Information Systems, as masterfully reviewed by Bélanger and Crossler and by Smith, Dinev, and Xu, and to draw on related disciplines and streams of research for a truly interdisciplinary study of information privacy.

References

Ackerman, M. 2004. "Privacy in Pervasive Environments: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8:6), pp. 430-439.

Acquisti, A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," in *Proceedings of the 5th ACM Electronic Commerce Conference*, New York: ACM Press, pp. 21-29.

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

Acquisti, A., and Grossklags, J. 2005. "Privacy and Rationality in Individual Decision Making," *IEEE Security & Privacy* (3:1), pp. 26-33.

Acquisti, A., John, L., and Lowenstein, G. 2011. "The Impact of Relative Judgments on Concern about Privacy," *Journal of Marketing Research* (forthcoming).

Acquisti, A., and Varian H. 2005. "Conditioning Prices on Purchase History," *Marketing Science* (24:3), pp. 1-15.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Ba, S., and Pavlou, P. A. 2002. "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premium and Buyer Behavior," *MIS Quarterly* (26:3), pp. 243-268.

Bansal, G., Zahedi, F., and Gefen, D. 2008a. "The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation," in *Proceedings of 29th International Conference on Information Systems,* Paris, France, December 14-17.

Bansal, G., Zahedi, F. M., 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), pp. 138-150.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

Bélanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3-4), pp. 245-270.

Benassi, P. 1999. "TRUSTe: an Online Privacy Seal Program," *Communication of the ACM* (42:2), pp. 56-59.

Bennett, C. J. 1995. *The Political Economy of Privacy: A Review of the Literature*, Hackensack, NJ: Center for Social and Legal Research.

Bessen, J. 1993. "Riding the Marketing Information Wave," *Harvard Business Review* (71:5), pp. 150-160.

Breckenridge, A. C. 1970. *The Right to Privacy*, Lincoln, NE: University of Nebraska Press, Lincoln.

Brown, M., and Muchira, R. 2004. "Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior," *Journal of Electronic Commerce Research* (5:1), pp. 62-70.

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

Cenfetelli, R. T., and Bassellier, G. 2009. "Interpretation of Formative Measurement in Information Systems Research," *MIS Quarterly* (33:4), pp. 689-707.

Chellapa, R., and Sin, R. G. 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumers' Dilemma," *Information Technology and Management* (6:2-3), pp. 181-202.

Chen, K., and Rea Jr., A. I. 2004. "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques," *The Journal of Computer Information Systems* (44:4), pp. 85-92.

Clarke, R. 1999. "Internet Privacy Concerns Confirm the Case for Intervention," *Communications of the ACM* (42:2), pp. 60-67.

Culnan, M. J. 1985. "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing* (9), pp. 10-19.

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

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

Davies, S. G. 1997. "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," in *Technology and Privacy: The New Landscape*, P. E. Agre and M. Rotenberg (eds.), Cambridge, MA: MIT Press, pp. 143-165.

Dholakia, N., and Zwick, D. 2001. "Contrasting European and American Approaches to Privacy in Electronic Markets: A Philosophical Perspective," *Electronic Markets* (11:2), pp. 116-120.

Dinev, T. Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006a. "Internet Users' Privacy Concerns and Beliefs about Government Surveillance: An Exploratory Study of Differences between Italy and the United States," *Journal of Global Information Management* (14:4), pp. 57-93.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006b. "Privacy Calculus Model in E-Commerce: A Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

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

Earp, J. B., and Payton, F. C. 2001. "Data Protection in the University Setting: Employee Perceptions of Student Privacy," in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, Los Alamitos, CA: IEEE Computer Society Press.

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* (59:8), pp. 877-886.

Featherman, M. S., and Pavlou, P. A. 2003. "Predicting E-Services Adoption: A Perceived Risk Facets Perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp. 611-642.

Hann, I. H., Hui, K. L., Lee, S.Y T., and Png, I. P. L. 2007. "Overcoming Information Privacy Concerns: An Information Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp. 13-42.

Hann, I-H., Hui, K. L., Lee, S. Y. T., and Png, I. P. L. 2008. "Consumer Privacy and Marketing Avoidance: A Static Model," *Management Science* (54:6), pp. 1094-1103.

Hirshleifer, J. 1971. "The Private and Social Value of Information and the Reward to Inventive Activity," *American Economic Review* (61:4), pp. 561-574.

Hui, K. L., and Png, I. P. L. 2006. "The Economics of Privacy," Chapter 9 in *Economics and Information Systems, Handbooks in Information Systems*, T. Hendershott (ed), Amsterdam: Elsevier.

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

Jamal, K. Sunder, S., and Maier, M. M. 2005. "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom," *Journal of Accounting Research* (43:1), pp. 73-96.

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

Jentzsch, N. 2001. "The Economics and Regulation of Financial Privacy: A Comparative Analysis of the United States and Europe," Working Paper, John F. Kennedy Institute for North American Studies, Free University of Berlin.

John, L., Acquisti, A., and Lowenstein, G. 2011. "Strangers on a Plane: Context-Dependent Willingness to Divulge Personal Information," *Journal of Consumer Research* (37:5), pp. 858-873.

Kobsa, A., and Teltzrow, M. 2005. "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior," *Lecture Notes in Computer Science: Privacy Enhancing Technologies* (3424), D. Martin and A. Serjantov (eds.), Berlin: Springer, pp. 329-343.

Laudon, K. C. 1996. "Markets and Privacy," *Communications of the ACM* (39:9), pp. 92-104.

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

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

Mason, R. 1986. "Four Ethical Issues of the Iformation Age," *MIS Quarterly* (10:1), pp. 4-12.

Milberg, S. J., Smith, H. J., and Burke, S. J. 2000. "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), pp. 35-57.

Miller, A. R., and Tucker, C. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," *Management Science* (55:7), pp. 1077-1093.

Miyazaki, A. D., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *The Journal of Consumer Affairs* (36:1), pp. 28-49.

Mossholder, K. W., Giles, W. F., and Wesolowski, M. A. 1991. "Information Privacy and Performance Appraisal: An Examination of Employee Perceptions and Reactions," *Journal of Business Ethics* (10:2), pp. 151-156.

Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms

Behaviors," *The Journal of Consumer Affairs* (41:1), pp. 100-126.

Nowak, G., and Phelps, J. 1997. "Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters" *Journal of Direct Marketing* (11:4), pp. 94-108.

Odlyzko, A. 2003. "Privacy, Economics, and Price Discrimination on the Internet," in *Proceedings of the 5th International Conference on Electronic Commerce*, New York: ACM Press, pp. 355-366.

Pavlou, P. A., and Fygenson, M. 2006. "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly* (30:1), pp. 115-143.

Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1), pp. 27-53.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal–Agent Perspective," *MIS Quarterly* (31:1), pp. 105-136.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (33:4), pp. 623-656.

Posner, R. 1978. "An Economic Theory of Privacy," *Regulation* (2), pp. 19-26.

Posner, R. 1981. "The Economics of Privacy," *American Economic Review* (71:2), pp. 405-409.

Phelps, J. E., D'Souza, G., and Nowak, G. J. 2001. "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation," *Journal of Interactive Marketing* (15:4), pp. 2-17.

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

Razzouk, N. Y., Seitz, V., and Nicolaou, M. 2008. "Consumer Concerns Regarding RFID Privacy: An Empirical Study," *Journal of Global Business and Technology* (4:1), pp. 69-78.

Rust, R. T., Kannan, P. K., and Peng, N. 2002. "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science* (30:4), pp. 455-464.

Sheehan, K. B. 1999. "An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors," *Journal of Interactive Marketing* (13:4), pp. 24-38.

Sheehan, K. B. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns," *Information Society* (18:1), pp. 21-32.

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

Skinner, G., Han, S., and Chang, E. 2006. "An Information Privacy Taxonomy for Collaborative Environments," *Information Management & Computer Security* (14:4), pp. 382-394.

Smith, H. J. Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

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

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp. 477-564.

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

Stigler, G. J. 1980. "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies* (9:4), pp. 623-644.

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

Sunder, S., Jamal, K., Maier, M. 2003. "Privacy in E-Commerce: Development of Reporting Standards, Disclosure and Assurance Services in an Unregulated Market," *Journal of Accounting Research* (41:2), pp. 285-309.

Tang, Z., Hu, Y. J., and Smith, M. D. 2008. "Gaining Trust through Online Privacy Protection: Self Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems* (24:4), pp. 153-173.

Taylor, C. R. 2004. "Consumer Privacy and the Market for Customer Unformation," *RAND Journal of Economics* (35:4), pp. 631-650.

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

Varian, H. R. 2006. "Economic Aspects of Personal Privacy," School of Information, University of California, Berkeley (http://people.ischool.berkeley.edu/~hal/Papers/privacy/).

Varian, H. R., Wallenberg, F., and Woroch, G. 2005. "The Demographics of the Do-Not-Call List," *IEEE Security Privacy* (3:1), pp. 34-39.

Wang, H., and Emurian, H. 1998. "An Overview of Online Trust: Concepts, Elements, and Implications," *Computers in Human Behavior* (21:1), pp. 105-125.

Wang, H., and Wang, C. 1998. "Consumer Privacy Concerns About Internet Marketing," *Communications of the ACM* (41:3), pp. 63-70.

Ward, S., Bridges, K., and Chitty, B. 2005. "Do Incentives Matter? An Examination of Online Privacy Concerns and Willingness to Provide Personal and Financial Information," *Journal of Marketing Communications* (11:1), pp. 21-40.

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

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

White, T. B. 2004. "Consumer Disclosure and Disclosure Avoidance: A Motivational Framework," *Journal of Consumer Psychology* (14:1/ 2), pp. 41-51.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View," in *Proceedings of 29th International Conference on Information Systems*, Paris, France, December 14-17.

Xu, H., Teo, H. H., Tan, B. C. Y., 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), pp. 137-176.

Younger Committee Report. 1972. "Report of the Committee on Privacy," Cmnd.5012 HMSO.

Zheng, Z., and Pavlou, P. A. 2010. "Toward a Causal Interpretation for Structural Models: A New Bayesian Networks Method for Observational Data with Latent Variables," *Information Systems Research* (21:2), pp. 365-391.

This content downloaded from 61.129.42.30 on Sun, 11 Feb 2018 16:34:58 UTC
All use subject to http://about.jstor.org/terms