The Information Society
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/utis20

A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet

Ardion Beldad [a], Menno de Jong [a] & Michaël Steehouder [a]
[a] Department of Technical and Professional Communication, University of Twente, Enschede, the Netherlands

Available online: 15 Jul 2011

To cite this article: Ardion Beldad, Menno de Jong & Michaël Steehouder (2011): A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet, The Information Society, 27:4, 220-232

To link to this article: http://dx.doi.org/10.1080/01972243.2011.583802

The Information Society, 27: 220–232, 2011
Copyright © Taylor & Francis Group, LLC
ISSN: 0197-2243 print / 1087-6537 online
DOI: 10.1080/01972243.2011.583802

Routledge
Taylor & Francis Group

A Comprehensive Theoretical Framework for Personal Information–Related Behaviors on the Internet

Ardion Beldad, Menno de Jong, and Michaël Steehouder

Department of Technical and Professional Communication, University of Twente, Enschede, the Netherlands

Although there is near consensus on the need for privacy, the reality is that people's attitude toward their personal information privacy is complex. For instance, even when people claim that they value their information privacy, they often trade their personal information for tangible or intangible benefits. In this article, the research on different ways in which people respond to risks to privacy is examined. They include information seeking to reduce uncertainty, the withholding of information, and the provision of fabricated information. The impact of trust and inducements on Internet users' willingness to share personal information is also examined. Thereafter, important postulates from theories in communication, social psychology, and sociology are synthesized into a comprehensive theoretical framework for personal information-related behaviors in the online environment.

Keywords information privacy, online privacy, privacy theories, privacy protection strategies

In a world where privacy is a right, sharing personal data, offline or online, can somehow be discomforting. Divulging one's personal data, for one, would have never been a problem if such data were devoid of any value and if they could just be "left alone"—a phrase central in Warren and Brandeis's (1980) conceptualization of "privacy." However, personal data have become a commodity, and this commoditization process increases their susceptibility to different forms of exploitation.

Due to the risks involved in online disclosure of personal data, Internet users understandably long for assurance that personal data shared online will not be betrayed. When the assurance is nowhere to be found, people clamor for control over their data and are reluctant to provide personal information whenever asked. But the reality is that people's attitude toward their personal data and information privacy is complex. This complexity is reflected in Westin's (1991) categories of people in accordance with their information privacy concerns: privacy fundamentalist, pragmatist, and privacy unconcerned. While people in the first category hardly reveal any information about themselves, those in the last category readily share their personal data in most circumstances. Furthermore, even when people claim that they value their information privacy, they often trade their personal data for tangible or intangible benefits (Culnan and Bies 2003; Olivero and Lunt 2004). This suggests that people differ in terms of the value they attach to their information privacy (Volkmann 2003).

This article focuses on people's personal information-related behaviors online. However, most of the empirical studies cited in this article were conducted within the context of online commercial exchanges. This can be justified by the fact that studies on information privacy concerns within the context of online noncommercial transactions are rather limited, or even nonexistent. As the following analysis shows, these studies provide valuable input for our current purposes.

The article begins with a discussion of the concept of privacy. Thereafter, the research on different ways in which people respond to risks to privacy is examined. They include information seeking to reduce uncertainty, withholding of information, and provision of fabricated information. The impact of trust and inducements on people's willingness to share personal information is also examined. Lastly, important postulates from theories in communication, social psychology, and sociology are synthesized into a comprehensive theoretical framework for personal information-related behaviors online.

Received 9 September 2009; accepted 19 September 2010.

Address correspondence to Ardion Beldad, University of Twente, Faculty of Behavioral Sciences, Department of Technical and Professional Communication, PO Box 217, 7500 AE Enschede, the Netherlands. E-mail: a.beldad@utwente.nl

PRIVACY: A MULTIFACETED CONCEPT

Privacy as an individual's right to "be left alone" (Warren and Brandeis 1890) is a widely accepted view of privacy. There is also the notion of privacy as one's freedom from intrusion. The latter, however, has been regarded as both "too broad and too narrow," making a consensus elusive when a specific case is under consideration (Moor 1991). The multifaceted nature of privacy has quite understandably, as Newell (1995) underscores, led to a profusion of definitions, often conflicting ones. According to Solove (2006), "privacy" is an umbrella term that refers to a wide and diverging group of related things.

Clark's (1997) and DeCew's (1997) typologies reflect the multifaceted nature of privacy. The first dimension of Clark's typology is labeled "privacy of the person" and is concerned with the integrity of the person's body. Issues here include blood transfusion without consent and compulsory immunization. The second dimension is labeled "privacy of personal behavior," which encompasses all behavior, but more specifically sensitive areas such as sexual preferences and religious practices. DeCew refers to this dimension of privacy as "accessibility privacy," which allows an individual to have seclusion for behavior that is socially defined as private, for example, sexual and bathroom activities. The third dimension, according to Clark, is privacy of personal communications or "interception privacy," which enables people to communicate among themselves, through different forms of media, free from surveillance or monitoring by others. This corresponds to DeCew's "expressive privacy" that protects an individual's right to express one's self-identity or personhood through speech and activity.

Aspects of the three types of privacy Clark identified also correspond to Van Dijk's (2006) conceptualization of privacy as either physical (the right to selective intimacy) or relational (the right to make contacts selectively). Physical privacy pertains to the inviolability of the human body, whereas relational privacy refers to the individual's ability to determine one's personal relationships without the observation and interference of other people (Van Dijk 2006).

Privacy of personal data or information,[1] the fourth dimension in Clark's typology, affords individuals the opportunity to prevent the automatic transmission of their data to other individuals or groups. This type of privacy is also referred to as "information privacy" (DeCew 1997) or "the right to selective disclosure" (Van Dijk 2006). The fourth dimension is particularly salient in the online environment.

What makes online information privacy different from offline information privacy is the qualitative difference in the magnitude of threat the former entails, which include, unauthorized data transfer, weak security, data magnets, and indirect data collection (Rezgui, Bouguettaya, and Eltoweissy 2003). And since personal data have become an economic commodity (Franzak, Pitta and Fritsche 2001; Olivero and Lunt 2004; Turner and Dasgupta 2003), those who collect them can easily succumb to the temptation of sharing them for commercial purposes without the consent of those to whom the data pertain. There are also real concerns that collected personal data may not be adequately protected and unauthorized third parties might have access to them (Wang, Lee, and Wang 1999).

Clark's (1997) "privacy of personal data" clearly emphasizes the ability of individuals to control the flow of their personal data. The concept of "control" is salient in Westin's (1967) definition of privacy "as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (7). A number of other definitions of privacy have also emphasized control as a critical factor for information privacy (Altman 1975; Diffie and Landau 1998; Fried 1984; Nissembaum 1998). When control is referred to in this context, it encompasses control over both information flow and the access others have to a person's information (Diffie and Landau 1998; Nissembaum 1998). It can, therefore, be argued that when individuals have control over information dissemination and information access they have acquired a certain level of information privacy (Moor 1991; Newell 1995).

The notion of privacy as control over information dissemination and access has, however, been criticized for its vagueness with regard to (1) the kinds of personal information over which people can expect to have control and (2) the amount of control they can expect to have over their personal information (Tavani 2007). Such shortcomings in the conceptualization of privacy as control spurred the formulation of a modified notion of privacy as control and restricted access, which advocates for the provision of varying levels of access to different people for different types of information at different times (Moor 1997). From this perspective emerged a privacy model known as restricted access and limited control (RALC) (Tavani 2007), which highlights the need for the creation of "privacy zones" that would enable people to limit or restrict others from accessing their personal information (Tavani 2008).

According to this perspective, absolute control over information about oneself is not necessary for managing one's privacy. Some degree of control can be achieved through choice, consent, and correction. One can exercise choice, where available, and act prudently. Correspondingly, one can give or withhold consent when asked. Furthermore, one can access and correct erroneous information about oneself when possible or make demands for

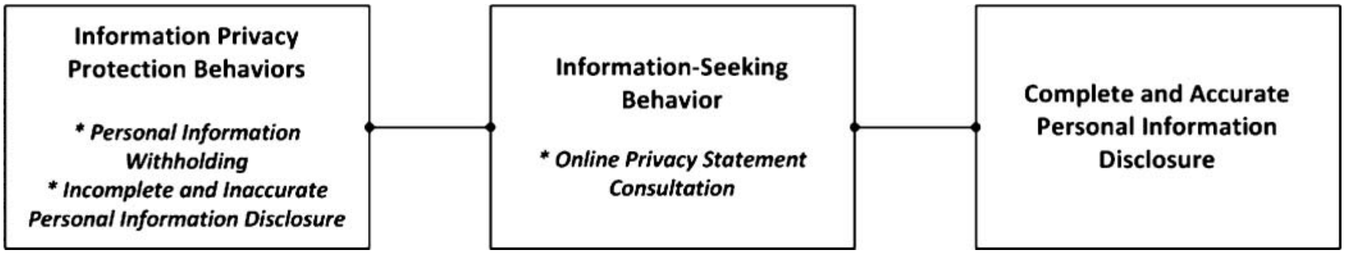
Information Privacy Protection Behaviors
* Personal Information Withholding
* Incomplete and Inaccurate Personal Information Disclosure
Information-Seeking Behavior
* Online Privacy Statement Consultation
Complete and Accurate Personal Information Disclosure

FIG. 1. Personal information-related behaviors.

access when it is not readily available (Ashworth and Free 2006, Tavani and Moor 2001; Tavani 2007). In general, control over personal information can be exercised both before and after information disclosure. Control of information after disclosure, however, depends on the organizations gathering the data. Here public policy can play a particularly important role.

ONLINE INFORMATION PRIVACY AS A RESPONSE TO RISKS

The extension of human interactions from the physical world to the digital environment has led to an expansion of the claim to information privacy rights in the cyberspace. People who are very concerned about their privacy in an offline environment are also prone to bringing their privacy concerns to the online world (Lwin and Williams 2003; Yao, Rice, and Wallis 2007). Their concerns are heightened not only because they do not know the information practices of online organizations (Reagle and Cranor 1997), but also because they do not have the ability to control the access others have to their information (Hoffman, Novak, and Peralta 1999).

The risks related to the disclosure of personal data are copious and depend on the amount and type of the personal information disclosed. For instance, one's contact details shared online could result in the inundation of one's mailbox with unsolicited marketing materials, as the said data could be sold to marketing organizations. Sharing one's income and health-related information could have more serious consequences. Regardless of the type and amount of personal data shared, what is certain is that, in one way or another, such data could be abused either by the organizations collecting them or by third parties with the right technology to access whatever data are stored in organizational databases. In reality, people in the digital environment have limited control over how their information will be used once shared, just as they have limited control over who will have access to their personal data.

So what do Internet users do to ensure the protection of their information privacy in an online environment? Since privacy risks are inescapable, Internet users would be expected to engage in various protection strategies, ranging from behavioral to technologically enabled. However, it is important to note that people also differ in their privacy concerns (Ackerman, Carnor, and Reagle 1999; Sheehan 2002), which means that personal information-related behaviors can be seen as a continuum, as shown in figure 1, with information privacy protection behaviors such as information withholding and incomplete and incorrect information sharing on one side and complete and correct information disclosure on the other side.

Information Seeking and Uncertainly Reduction

Uncertainties stem from situations that are ambiguous, complex, unpredictable, or probabilistic; from the absence or inconsistency of information; and from feelings of insecurity about one's own state of knowledge or the state of knowledge in general (Brashers 2001). Because uncertainties cause discomfort, people seek to eliminate them by acquiring pertinent information (Heath and Bryant 2000). When people are unsure about the other party in the encounter, disturbance in the flow of the interaction is bound to occur (Berger 1986).

In a similar vein, Berger and Calabrese's (1975) uncertainty reduction theory (URT) postulates that high levels of uncertainty accelerate information-seeking behavior and correspondingly a decline in uncertainty decreases information-seeking behavior. In effect, uncertainty spurs the need for information. Correspondingly, the need for information is a "function of extrinsic uncertainty produced by a perceived discrepancy between the individual's current level of certainty about important environmental objects and a criterion state he seeks to achieve" (Atkin 1973, 206). Accordingly, figure 2 hypothesizes that people's uncertainties about the use of their personal data once disclosed trigger concerns regarding information privacy violations, which would eventually spur them to perform information-seeking behaviors.

An online privacy statement is often the only source of information for users with regard to how their personal data will be used once shared online (Vail, Earp, and Anton 2008). Therefore, users who are serious about protecting their online information privacy are likely to check the

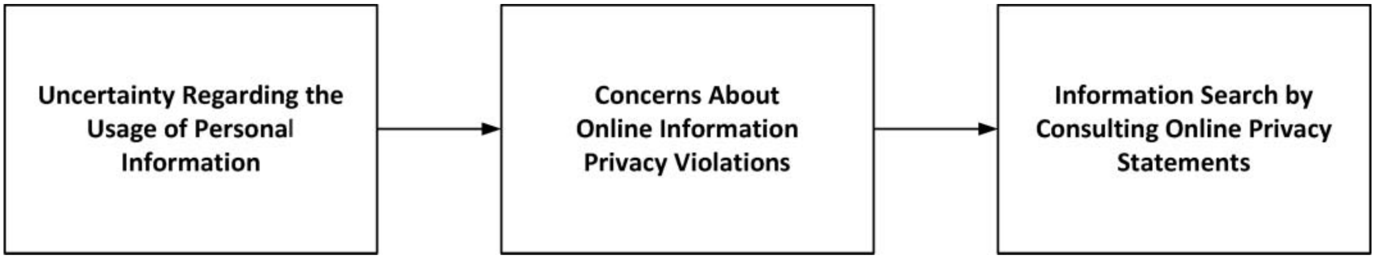
Uncertainty Regarding the Usage of Personal Information
Concerns About Online Information Privacy Violations
Information Search by Consulting Online Privacy Statements

FIG. 2. Hypothesized three-stage process of information seeking to reduce uncertainty regarding online privacy.

privacy policy of the sites they visit (Jensen and Potts 2004). Results of a survey by Milne and Culnan (2004) suggest that privacy policies or notices are used as one part of an overall strategy for dealing with the risks of online personal information disclosure. In other words, Internet users are inclined to read privacy notices to manage information privacy-related risks. Milne and Culnan's study also shows that users consult privacy policies to acquire information about how their personal data will be used by organizations that collect them (Milne and Culnan 2004), which is understandable, given that privacy policies are often the only means for them to know how organizations will use and process their data (Vail, Earp, and Anton 2008). In a similar vein, Pan and Zinkhan (2006) found that Internet users who perceive high levels of information privacy risks are more likely to read online privacy statements.

Assuming that users have religiously perused a privacy statement on a Web site, can we automatically expect them to opt for information disclosure to commence online transactions with organizations? Probably yes, if users were convinced that online organizations would do whatever they have indicated on their online privacy statements. The answer would be probably "no," if users regarded privacy statements as an intricate mishmash of hollow promises. Thus, information search can result in either users being persuaded that information disclosure is safe, prompting their decision to share complete and correct information, or users getting cautious, leading to the withholding of correct personal information and even the transmission of fabricated information.

Information Withholding and Incomplete Information Disclosure

Moor (1997) argues that the creation of a "privacy zone" enables people to decide how much information should stay private and how much information should be divulged. Similarly, Pedersen (1997) advances the notion of boundary control, which is both a process of restricting and seeking interaction to achieve a desired degree of access to the self (or one's group) by others at a defined moment and in a particular circumstance (Pedersen 1997). Boundaries are opened when personal information is voluntarily shared and closed when information is withheld (Stanton 2002). The concept of boundary control makes a marked difference between the self and the nonself—or the other (Altman 1975).

Based on the already-mentioned premises, communication privacy management (CPM) framework suggests that people formulate rules to guide them in deciding whether or not to disclose personal information and in determining the most effective strategies to protect their privacy (Petronio 2002). It also posits that people create rules to maximize the benefits and to minimize the risks of information disclosure.

CPM is anchored on five principles that seek to capture the ways people regulate the withholding or the sharing of their private information. First, people believe that they own their information. Second, such a belief in information ownership influences people's view that they are entitled to control the flow of information to others. Third, the decision to open or close privacy boundaries is guided by a set of rules that people create individually. Fourth, when people disclose information, they consider recipients as stakeholders of the information and presuppose that recipients will observe existing privacy rules or negotiate to make some revisions on the rules. Fifth, privacy management in an imperfect world can be turbulent, especially when one's privacy management rules are disrupted or one's privacy boundary is trespassed (Petronio 2002; 2007).

Although a number of studies have investigated the various behavioral strategies users employ for managing their privacy in online transactions (Earp and Baumer 2003; Milne, Rohm, and Bahl 2004; Sheehan and Hoy 1999), only Metzger (2007) uses CPM for understanding privacy regulation practices of Internet users. Metzger argues that Internet users erect boundaries and formulate rules to decide when to disclose information. Her research suggests that information withholding in online exchanges is a common information privacy protection strategy. The decision to employ such a strategy, however, is dependent on the appraised sensitivity of the personal information requested. According to Son and Kim (2008), information privacy concerns primarily contribute to Internet users' reluctance to share their personal information. Information concealment or refusal to share personal information is seen both as an important aspect of privacy (Posner 1984) and as an exercise of control over one's personal information (Milne, Rohm, and Bahl 2004).

People not only withhold personal data but also falsify them as another information privacy protection strategy. They are most likely to falsify sensitive personal data, but not those deemed relevant for the completion of a specific online transaction (Metzger 2007). Furthermore, the type of information that is requested is an important indicator of whether or not the Internet users will decide to disclose their information—the more sensitive the requested information, the weaker is their confidence in disclosing them online (Castaneda and Montoro 2007).

Internet users are conscious about the amount and type of personal information they divulge online (Paine et al. 2007), which enables them to control the outflow of their information without the risks of forfeiting possible online benefits (Sheehan and Hoy 1999). Metzger (2007) points out that people are wary about supplying their information whenever requested because they know that they have limited opportunities to negotiate mutually accepted privacy rules, which prompts them to erect privacy boundaries through information withholding and information falsification. People would probably have lesser inclination to withhold or fabricate their personal information if they were adequately notified on how information they would disclose would be used (Kobsa 2007).

From the perspective of protection motivation, the fear of compromising one's information privacy in the digital environment is a strong motivation for an individual to adopt some forms of privacy-protection strategies such as refusing to share personal data or opting to disclose incorrect or incomplete personal information. Ronald Rogers' protection motivation theory (PMT) postulates that protection motivation arises from the cognitive appraisal of a depicted event as noxious (threat severity) and likely to occur (probability of threat occurrence), along with the belief that a recommended coping response can effectively prevent the threatening event from happening (Rogers 1975, 1983).

However, if the privacy threats are not appraised to be severe or as likely to occur, protection motivation would not be triggered (Rogers 1983). We can only assume that when Internet users do not magnify the severity of the privacy threats and the likelihood that they will occur, users' inclination to perform privacy protection behaviors would be lower, which would probably result in their decision to supply correct and complete personal data for the completion of an online transaction.

Users' decision to share personal information completely and accurately might not always be shaped by their lowered assessment of the risks. There is also the possibility that they are not aware of the risks involved in their decision to share something about themselves. As Simon (1955) claims, human beings, by nature, possess limited computational and predictive abilities, which make decision making within a rational framework relatively crude.

The fact that people do not always have complete information primarily contributes to the "boundedness" of human rationality (Simon 1972). Individual decision processes with respect to information privacy are restrained not only by bounded rationality but also by incomplete information (Acquisti and Grossklags 2005) and systematic deviations from rationality (Acquisti and Grossklags 2005; Kobsa 2007). Incomplete information becomes a problem for Internet users if they just share personal information without being aware of the risks involved in the disclosure and without any knowledge about the ways to protect their personal information (Acquisti and Grossklags 2004).

Impact of Trust and the Lack Thereof

Threats to information privacy can be caused either by the organization collecting the personal data or by external parties possessing the expertise and technology to acquire unauthorized access to users' personal data. The perceived risks of having users' data abused either by the collecting organization or by an unauthorized third party dampen information sharing among users. Although users' awareness of the risks involved in online personal information disclosure could reduce their trust in an online organization soliciting personal information (Olivero and Lunt 2004), there is substantial empirical support for the positive impact of trust in organizations and in their Web sites on users' intention and willingness to share whatever information is requested (Schoenbachler and Gordon 2002; Zimmer et al. 2010).

Users' trust in this case is not one-dimensional, but is expected to target two organizational characteristics—the organization's ability to protect users' personal information from unwarranted external intrusion, and its motivation and intention to protect and to respect collected pieces of personal information considering the organization's ability to abuse them. When trust in either both or one of these two categories is missing, one can just expect users to refuse to disclose their personal information or they may even provide fabricated information about themselves.

In deciding whether or not to trust organizations in terms of their ability and motivation to protect personal data, users may look for a number of cues. First, there is the privacy statement, which is expected to inform users how their personal data will be collected, processed, and used. A couple of studies show that Internet users read online privacy statements either as a strategy to manage one's online information privacy (Milne and Culnan 2004) or as a way to address information privacy concerns (Pan and Zinkhan 2006).

Although it is also known that most Internet users do not bother to read privacy statements (Arcand et al. 2007; Jensen, Potts, and Jensen 2005; Meinert, et al. 2004; Vu et al. 2007), they are most likely to trust organizations that post privacy statements on their Web sites (Pan and Zinkhan 2006) and would feel greater control over their personal data when shared with organizations whose websites contain those documents (Arcand et al. 2007). Aside from online privacy statements, seals of approval from third-party certifying organizations have also been found to improve users' positive evaluation of the privacy practices of online organizations (Miyazaki and Krishnamurthy 2002) and to encourage online information disclosure (LaRose and Rifon 2007).

Concerns about unauthorized access to users' personal information in organizational databases could also prompt users to expect that organizations deploy security technologies. Koufaris and Hampton-Sosa (2004) claim that the presence of security mechanisms significantly increases users' trust in initial online exchanges. In fact, the presence of security measures on Web sites is regarded as more important than privacy statements and seals of approval in building Internet users' trust (Belanger, Hiller, and Smith 2002).

Internet users also consider a positive organizational reputation when deciding to supply personal information for online transactions (Olivero and Lunt 2004; Xie, Teo, and Wan 2006). Users without any prior experience with an online organization consider the organization's reputation as an indicator of that organization's trustworthiness (Chen 2006; Kim, Ferrin, and Rao 2003; Koufaris and Hampton-Sosa 2004; McKnight, Choudhoury, and Kacmar 2002). Organizations with a reputation to protect are not expected to engage in opportunistic behaviors that will result in the depreciation of their reputation (Herbig, Milewicz, and Golden 1994), such as selling their clients' personal information to third parties. Indeed, Internet users will not hesitate to disclose their personal information to well-known online organizations with an image to maintain (Olivero and Lunt 2004).

Only When the Price is Right

People may claim that they value their information privacy (Ackerman, Carnor, and Reagle 1999; Acquisti and Grossklags 2005; Nehf 2007; Strandburg 2006), but offers of benefits often induce people to provide personal information (Nehf 2007; Olivero and Lunt 2004). People will trade their personal information, even it would mean jeopardizing their information privacy, if the perceived value of the benefits outweighs the estimated costs of information disclosure as per their calculations (Berendt, Gunther, and Spiekermann 2005; Culnan and Bies 2003; Henderson and Snyder 1999; Laufer and Wolfe 1977; Norberg and Dholakia 2003; Olivero and Lunt 2004). In general, there is increasing recognition of voluntary provision of personal information for monetary and other benefits as a form of economic exchange.

From a social exchange perspective, human behavior and social interaction are an exchange of both tangible and intangible goods (Homans 1958, 1961). Somebody engaged in an exchange considers what he is giving up as a cost and what he is about to receive as a reward and his behavior changes as profit (reward minus cost) is maximized (Homans 1958). Blau (1964) defines social exchange as the voluntary action of individuals who are motivated by the returns they are expected to bring and typically do in fact bring from others. Although social exchange can be seen as resembling economic exchange, with the principles of elementary economics perfectly reconcilable with those of elementary social behavior (Homans 1961), the two perspectives on exchange differ in their conceptual cores (Emerson 1987).

The entailment of unspecified obligations primarily differentiates social exchanges from economic exchanges (Blau 1964). Blau underscores that while economic exchanges are moored on a formal contract that specifies the exact amount to be exchanged, the benefits involved in social exchange are not definitively priced in terms of a single quantitative medium of exchange, which is the reason why obligations in social exchanges are not specific. Emerson (1987) claims that goods involved in social exchanges have subjective values.

In computer-mediated interactions, exchanges are common, involving not just material goods but also intangible ones. Setting aside online shopping involving tangible commodities with defined prices, a pure economic exchange, nonmaterial goods are also exchanged for nonmaterial rewards and benefits. People sign in to become members of social networking sites, disclosing personal information in exchange for online membership and the opportunity to connect with other online members. People register with webmail services at the expense of sharing specific personal data just to have an e-mail address. People request documents and information from online organizations but requests can only be completed on "payment" with their personal information.

Thus, personal information, with its subjective value, can be traded for another commodity also with subjective value, like membership to a networking site, or another item with a defined price, like a gift check. One study reveals that while most respondents were relatively sensitive to online privacy concerns, some respondents showed a degree of willingness to disclose personal information in exchange for money or convenience (Hann et al. 2007). In this case, people do consider the information collected from them as their input into an exchange with an online agent, and this spurs them to expect to receive something of value (Ashworth and Free 2006).

As mentioned earlier, benefits can be tangible or intangible. Tangible benefits for the disclosure of personal information online could be vouchers, cash, or gift items. Rewards in the form of monetary vouchers have a positive impact on Internet users' willingness to provide accurate personal information for personally identifiable data (Xie et al. 2006). Thus, online users seem to be calculating the impact of disclosing a certain amount of information against the value of monetary rewards to be received.

Could it be that the higher the monetary reward, the greater is the probability of Internet users disclosing more sensitive information? According to Olivero and Lunt (2004), Internet users were willing to give away some degree of information privacy in lieu of rewards only for those personal data whose loss of control was deemed to be not too risky. This suggests that users are calculating and balancing the information they will give with what they will receive in the exchange (Sheehan and Hoy 2000).

Intangible benefits include the convenience of doing things online such as e-shopping, getting an e-mail account, joining online social networks, and experiencing the comforts of personalization and personalized services—all requiring the disclosure of personal information. Results of a survey by Chellapa and Sin (2005) reveal that perceived benefits of personalization are almost two times more influential than Internet users' concern for privacy in determining their usage of personalized services.

Figure 3 outlines the process in which people weigh the incalculable costs of their decisions to disclose personal data against the expected value of the benefits they can derive from information sharing. When the expected benefits from information disclosure do not outweigh the value attached to the personal data to be disclosed, information withholding or incomplete information disclosure could be forthcoming.

Other Factors Influencing Information Withholding and Complete Personal Information Disclosure

While risk perceptions, trust, and expected benefits are crucial factors in people's decision to either withhold their personal data or disclose them accurately and completely, other factors also need to be considered. Users' relationship with organizations requesting their personal data should not be discounted as an important influence, since users would not hesitate to share their data with online organizations with which they have established relationships (Olivero and Lunt 2004).

Regardless of relational depth, people can still disclose personal information despite a preference for keeping such information private (Strandburg 2006). According to Strandburg (2006), people share information not just for the benefits that can be derived from the sharing but also for the "taste" of disclosure itself. In a study on information disclosure in social networking sites, some respondents admitted that they were not sure why they shared information, with others claiming that they had become so used to filling out forms that they did not think twice before supplying any information (Strater and Richter 2007).

Another recent investigation of the phenomenon of information sharing in networking sites had a relatively similar finding—that despite concerns over online information privacy as substantiated by the use of available privacy settings, Internet users still displayed a general tendency to disclose information (Christofides, Muise, and Desmarais 2009). Perhaps this is true of people belonging to Westin's privacy-unconcerned category—people who

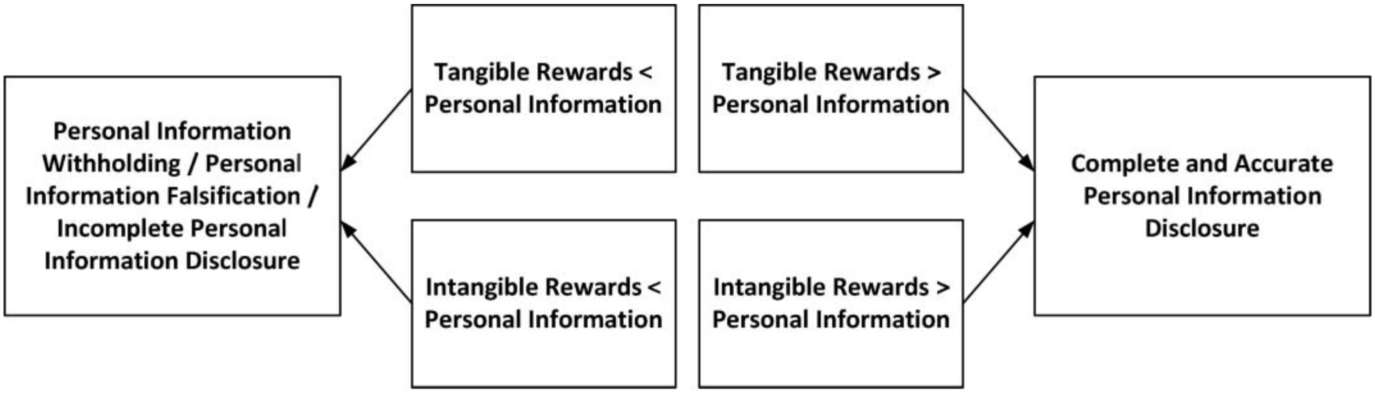
Personal Information Withholding / Personal Information Falsification / Incomplete Personal Information Disclosure
Tangible Rewards < Personal Information
Intangible Rewards < Personal Information
Tangible Rewards > Personal Information
Intangible Rewards > Personal Information
Complete and Accurate Personal Information Disclosure

FIG. 3. Cost-benefit calculations of personal information disclosure and personal information protection.

get a kick from online disclosure of personal information. Probably the privacy fundamentalists will not view information disclosure as some kind of a stimulating drug but a toxic substance to be evaded.

Although it is apparent that some Internet users have developed a habit of information sharing when doing things online, such habitual disclosure might be influenced by users' disposition to trust in a variety of situations, as well as by their previous experience with online disclosures. Disposition to trust refers to a tendency to be willing to depend on others (McKnight, Cummings, and Chervany 1998). With a higher disposition to trust, people would be inclined to do something even without consideration of the negative effects of a particular action.

Internet users with more experience in online transactions requiring information disclosure are less concerned about online information privacy (Bellman et al. 2004; Cho et al. 2009; Metzger 2004), in general, and are less concerned about privacy risks such as improper access to and unauthorized secondary use of data (Bellman et al. 2004), in particular. Higher levels of Internet experience would result in lowered information privacy concerns and risk perception, which would expectedly prompt a heightened willingness to disclose personal information (Metzger 2004).

PROPOSED COMPREHENSIVE THEORETICAL FRAMEWORK FOR PERSONAL INFORMATION-RELATED BEHAVIORS

While empirical studies on the factors that influence users' willingness (or reluctance) to share their personal information are numerous, as the discussion in preceding sections shows, these studies were conducted without the benefit of a comprehensive theoretical framework. We propose a comprehensive theoretical framework for personal information-related behaviors that highlights the different determinants of the different types of behaviors, as emphasized by different theoretical perspectives.

The need to protect personal information in the online environment is rooted in the need to uphold information privacy. However, the context within which information privacy arises as an issue has a strong bearing on how people deal with their personal information, especially in the online environment.

This article argues that people's personal information-related behaviors can be conceptualized as a continuum—with information privacy protection behaviors such as information withholding and incomplete and inaccurate disclosure on one side, and complete and accurate information disclosure behaviors on the other. Situated in the middle of the continuum is information-seeking behavior directed at understanding how organizations will use, process, and protect personal data collected from their clients, such as users checking privacy statements on organizational websites.

Although the behavior just described is not a prerequisite for information withholding or complete information disclosure, it is likely that Internet users who are too concerned about the risks involved in the sharing of their personal information would first resort to information-seeking behavior before deciding to withhold or completely share data about themselves. As explained earlier, the accumulation of the necessary information on organizational uses and processing of users' personal data may not automatically result in complete personal data disclosure.

Users have to be convinced that collecting organizations will do whatever they have indicated on their online privacy statements. Those who do not trust the claims of organizations may shy away from information disclosure and resort to information privacy protection behaviors. While perceptions of risks could easily thrust people to seek information, their levels of trust in organizations in terms of how they will process, use, and protect their personal data (Vu et al. 2007) and their positive prior experience with those organizations (Milne and Culnan 2004) could significantly reduce their felt need to consult online privacy statements.

Information privacy protection behaviors in an online environment are often precipitated by privacy concerns, which arise from the belief that personal information disclosure is very risky due to the high probability of abuse either by the collecting organization or by external third parties. People who are highly concerned about their information privacy might magnify the risks involved in information disclosure, while those with lower privacy concerns would tend to underestimate the magnitude of risks. The impact of risk perceptions on privacy concerns should not also be discounted. People's estimation of the risks in information disclosure might even increase or decrease their levels of privacy concerns.

The degree of risk perception in online sharing of personal information could be shaped by the appraised sensitivity of personal information to be divulged. One may not worry so much about disclosing one's preference in film or music, but the concern would surely be different when that same person is asked to indicate his or her income or disclose information regarding his or her health. Users' appraisal of the sensitivity of information requested by organizations would also be instrumental in either driving users to perform information privacy protection behaviors or prompting them to disclose complete and accurate personal information.

Complete personal information disclosure can be expected if users do not estimate higher risks or when they are not aware of the risks in divulging their information or when they trust organizations' ability and motivation to protect their information. The proposed comprehensive model shows that a two-way relation also exists between trust and risk perceptions. Users' level of trust could influence their risks perceptions, or their perceptions of the risks could have a bearing on their willingness to trust.

Users' lack of trust in organizations' ability and motivation to protect their clients' personal data have been found to strongly prompt them to withhold their personal data or disclose them incompletely and inaccurately. However, complete information disclosure is imminent when users trust that online organizations are competent in ensuring the protection of their clients' personal data and when those organizations are believed to have close-to-nil inclinations to abuse those data. Several empirical studies have indicated that trustworthiness cues such as privacy protection assurances, seals of approval, security features, and a positive organizational reputation have considerable impact on users' degree of trust in online organizations.

Although some researchers argue that Internet users would be very willing to compromise their information privacy by disclosing their personal information in exchange for something in the digital environment, there is no denying that users can also be rational in dealing with information sharing. Rationality dictates that users weigh the benefits that can be gained from supplying their personal information for an online transaction against the costs (specifically the risks) of their intention to share their information. The premise is that when the benefits outweigh the costs, complete information disclosure can be expected. However, when the risks of information disclosure exceed the estimated value of the benefits expected from the disclosure, users may resort to privacy protection behaviors.

Nevertheless, other factors, which could be described as either rational or nonrational, should also be considered as important determinants of Internet users' intention to withhold their personal data, share them incompletely, or disclose them accurately. While trust, risk appraisal, and benefits calculation could be regarded as rational factors influencing personal information-related behaviors, nonrational elements have also been found to be determinants of information withholding and information disclosure. Users with sufficient experience with online transactions are found to have lower privacy concerns (Bellman et al. 2004; Cho et al. 2009), which would most likely result in a heightened willingness to share requested personal information. Habits also play a part. While some people, especially "privacy fundamentalists," may have the habit of refusing information disclosure under any circumstance; others, probably those "privacy unconcerned," habitually share information regardless of the risks and the benefits.

An important rational factor that could also influence users' decision to withhold or disclose personal data is their appraisal of the relevance of the data for a transaction. The less the relevance of the data for an exchange, the lower will be the tendency of users to disclose them whenever requested. The comprehensive theoretical framework in figure 4 shows all the important postulations on personal information-related behaviors, according to the theoretical perspectives discussed in this article.

CONCLUSION

Organizations can reduce users' level of risk perceptions only when they win users' trust in the organization's ability and motivation to protect personal data collected from users. Several empirical studies, particularly on online commercial exchanges, have shown that users look for a number of cues to assess whether or not an organization can be trusted with their personal data. Because of privacy issues and the concerns regarding the security of personal data, users expect the availability of privacy statements and security features on websites used for the collection of data.

From a theoretical standpoint, the impact of such cues on trust formation and risk perception reduction would depend on users' level of privacy concerns. For instance, while privacy statements may not mean much for people who have totally submitted to the belief that information disclosure is extremely risky or the "privacy fundamentalists," the same documents may be forceful enough to sway nonfundamentalists to share their information whenever asked online. We can postulate the same thing for the impact of perceived benefits on one's willingness to disclose information.

Nonetheless, when one decides to share pieces of personal information for an online transaction, this should not always be viewed as an indication of that person's trust in the organization collecting the information. Even in the absence of trust, many Internet users would still share complete and accurate personal information when the expected benefits from the disclosure act outweigh the costs (or the risks) of information sharing. But that might be limited to users who are not concerned about their information privacy or those who maintain a pragmatic stance toward such type of privacy. Conversely, this type of behavior is unlikely to be seen from users who harbor a deep-seated belief that personal information disclosure is an extremely risky act.

Understanding why some Internet users' would unrelentingly disclose complete and accurate personal information, while others would conscientiously refuse to share any information about themselves can be a complex pursuit. It is certainly worthy of further research, which would greatly benefit from a multidisciplinary approach.

While there are a growing number of empirical studies that focus on the factors influencing personal information disclosure or withholding in the online environment, these

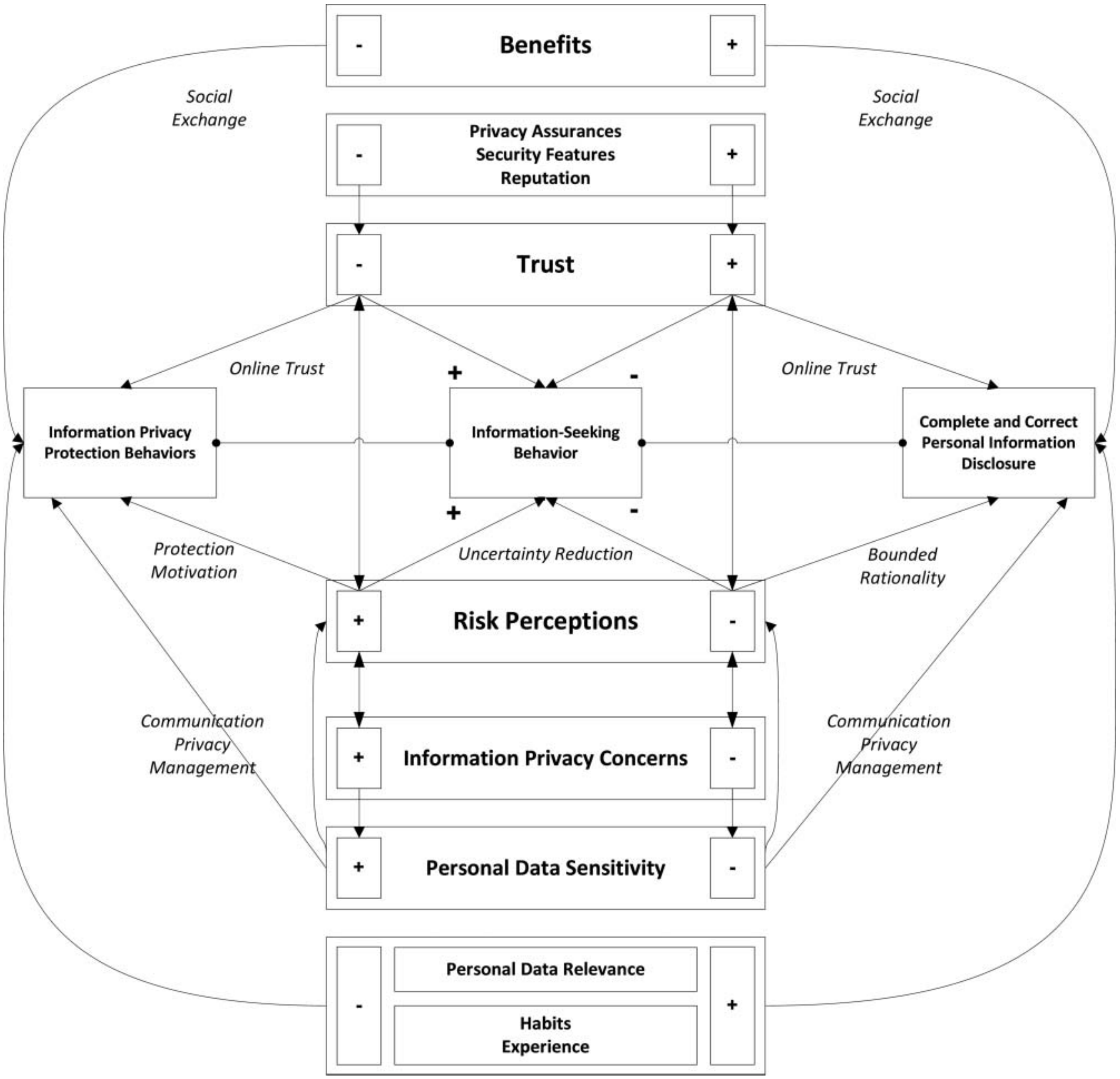

FIG. 4. Comprehensive theoretical framework for personal information-related behaviors.

studies are constrained by models that are not comprehensive. For instance, there is an overemphasis on the impact of trust and risk on disclosure intentions at the expense of other possible factors such as the expected benefits that could be derived from the disclosure act and the appraised relevance of the information to be disclosed for the completion of a particular online transaction. We believe that to fully understand why Internet users would withhold or share personal information during online transactions it is imperative to consider the important premises of a number of theoretical perspectives from social psychology, sociology, psychology, communication, and even economics.

Researchers of online information privacy regardless of their disciplinary affiliations are likely to benefit from the theoretical framework we have proposed in this article. On one level, it presents a multidisciplinary synthesis. On another level, it is applicable to not only personal information behaviors within the frame of online commercial exchanges but also those in noncommercial transactions. We hope the proposed framework will stimulate and facilitate research that is mindful of the multidimensionality of personal information-related behaviors online.

NOTE

[1] Throughout this article, personal information and personal data would be interchangeably used.

REFERENCES

Ackerman, M. S., L. F. Cranor, and J. Reagle. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. *EC '99: Proceedings of the 1st ACM Conference on Electronic Commerce, Denver, CO* 1999;1–8. http://portal.acm.org/citation.cfm?id=336995 (accessed April 4, 2009).

Acquisti, A., and J. Grossklags. 2004. Privacy attitudes and privacy behavior: losses, gains, and hyperbolic discounting. In *Economics of information security*, eds. J. Camp and S. Lewis, 165–78. Boston: Kluwer Academic.

Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy* 3(1):26–33.

Altman, I. 1975. *The environment and social behaviour*. Monterey, CA: Brooks/Cole.

Arcand, M., J. Nantel, M. Arles-Dufour, and A. Vincent. 2007. The impact of reading a Web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review* 31(5):661–81.

Ashworth, L., and C. Free. 2006. Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics* 67(2):107–23.

Atkin, C. 1973. Instrumental utilities and information seeking. In *New models for mass communication research*, ed. P. Clarke, 205–39. Beverly Hills, CA: Sage.

Belanger, B., J. S. Hiller, and W. J. Smith. 2002. Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems* 11(3–4):245–70.

Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20(5):313–24.

Berendt, B., O. Gunther, and S. Spiekermann. 2005. Privacy in e-commerce: Stated preferences vs. actual behavior. *Communications of the ACM* 48(4):101–6.

Berger, C. R. 1986. Uncertain outcome values in predicted relationships: Uncertainty reduction theory then and now. *Human Communication Research* 13(1):34–38.

Berger, C. R., and R. J. Calabrese. 1975. Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research* 1(2):99–112.

Blau, P. M. 1964. *Exchange and power in social life*. New York: Wiley.

Brashers, D. E. 2001. Communication and uncertainty management. *Journal of Communication* 51(3):477–97.

Castaneda, J. A., and F. J. Montoro. 2007. The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research* 7(2):117–41.

Chellapa, R. K., and R. G. Sin. 2005. Personalization versus privacy: an empirical examination of the online consumers' dilemma. *Information Technology and Management* 6(2):181–202.

Chen, C. 2006. Identifying significant factors influencing consumer trust in an online travel site. *Information Technology and Tourism* 8:197–214.

Cho, H., M. Rivera-Sanchez, and S. S. Lim. 2009. A multinational study on online privacy: Global concerns and local responses. *New Media & Society* 11(3):395–416.

Christofides, E., A. Muise, and S. Desmarais. 2009. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior* 12(3):341–45.

Clark, R. 1997. *Introduction to dataveillance and information privacy, and definition of terms*. http://www.rogerclarke.com/DV/Intro.html#Priv (accessed April 3, 2009).

Culnan, M. J., and R. J. Bies. 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues* 59(2):323–42.

DeCew, J. W. 1997. *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Diffie, W., and S. Landau. 1998. *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: MIT Press.

Earp, J. B., and D. Baumer. 2003. Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM* 46(4):81–83.

Emerson, R. M. 1987. Toward a theory of value in social exchange. In *Social exchange theory*, ed. K. S. Cook, 11–46. Newbury Park, CA: Sage.

Franzak, F., D. Pitta, and S. Fritsche. 2001. Online relationships and the consumer's right to privacy. *Journal of Consumer Marketing* 18(7):631–41.

Fried, C. 1984. Privacy [a moral analysis]. In *Philosophical dimensions of privacy: An anthology*, ed. F. D. Schoeman, 203–22. Cambridge: Cambridge University Press.

Hann, I. L., Hui, K. L., Lee, S. Y. T., and Png, I. P. 2007. Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems* 24(2):13–42.

Heath, R. L., and J. Bryant. 2000. *Human communication theory and research* (2nd ed.). Mahwah, NJ: Erlbaum.

Henderson, S. C., and C. A. Snyder. 1999. Personal information privacy: Implications for MIS managers. *Information and Management* 36(4):213–20.

Herbig, P., J. Milewicz, and J. Golden. 1994. A model of reputation building and destruction. *Journal of Business Research* 31(1):23–31.

Hoffman, D. L., T. P. Novak, and M. A. Peralta. 1999. Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web. *The Information Society* 15(2):129–39.

Homans, G. 1958. Social behavior as exchange. *American Journal of Sociology* 63(6):597–606.

———. 1961. *Social behavior: Its elementary forms*. London: Routledge & Kegan Paul.

Jensen, C., and C. Potts. 2004. Privacy policies as decision-making tools: An evaluation of online privacy notices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vienna, Austria* 2004:471–78. http://portal.acm.org/citation.cfm?id=985752 (accessed April 4, 2009).

Jensen, C., C. Potts, and C. Jensen. 2005. Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies* 63(1–2):203–27.

Kim, D. J., D. L. Ferrin, and H. R. Rao. 2003. A study of the effect of consumer trust on consumer expectations and satisfaction: The Korean experience. *ICEC '03 Proceedings of the 5th International Conference on Electronic Commerce, Pittsburgh, PA* 2003:310–15. http://portal.acm.org/citation.cfm?id=948046 (accessed April 10, 2009).

Kobsa, A. 2007. Privacy-enhanced personalization. *Communications of the ACM* 50(8):24–33.

Koufaris, M., and W. Hampton-Sosa. 2004. The development of initial trust in an online company by new customers. *Information & Management* 41(3):377–97.

LaRose, R., and N. J. Rifon. 2007. Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs* 41(1):127–49.

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

Lwin, M. O., and J. D. Williams. 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):257–72.

McKnight, D. H., H. Choudhoury, and C. Kacmar. 2002. The impact of initial consumer trust on intentions to transact with a Web site: A trust building model. *Journal of Strategic Information Systems* 11(3–4):297–323.

McKnight, D. H., Cummings, L., and N. L. Chervany. 1998. Initial trust formation in new organizational relationships. *Academy of Management Review* 23(3):473–90.

Meinert, D. B., D. K. Peterson, J. R. Criswell, and M. D. Crossland. 2004. Would regulation of Website privacy policy statements increase consumer trust? *Informing Science Journal* 9:123–42.

Meztger, M. J. 2004. Privacy, trust, and disclosure: exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication* 9(4). http://jcmc.indiana.edu/vol9/issue4/metzger.html (accessed June 12, 2009).

———. 2007. Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication* 12(2):335–61.

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

Milne, G. R., A. J. Rohm, and S. Bahl. 2004. Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38(2): 217–32.

Miyazaki, A. D., and S. Krishnamurthy. 2002. Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs* 36(1):28–49.

Moor, J. H. 1991. The ethics of privacy protection. *Library Trends* 39(1–2):69–82.

———. 1997. Towards a theory of privacy in the information age. *Computers and Society* 27(3):27–32.

Nehf, J. P. 2007. Shopping for privacy on the Internet. *Journal of Consumer Affairs* 41(2):351–65.

Newell, P. B. 1995. Perspectives on privacy. *Journal of Environmental Psychology* 15(2):87–104.

Norberg, P. A., and R. R. Dholakia. 2004. Customization, information provision and choice: What are we willing to give up for personal service? *Telematics and Informatics* 21(2):143–55.

Nissenbaum, H. 1998. Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy* 17(5–6): 559–96.

Olivero, N., and P. Lunt. 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology* 25(2):243–62.

Paine, C., U. D. Reips, S. Stieger, A. Joinson, and T. Buchanan. 2007. Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human-Computer Studies* 65(6):526–36.

Pan, Y., and G. M. Zinkhan. 2006. Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing* 82(4):331–38.

Pedersen, D. M. 1997. Psychological functions of privacy. *Journal of Environmental Psychology* 17(2):147–56.

Petronio, S. 2007. Translational research endeavors and the practices of communication privacy management. *Journal of Applied Communication Research* 35(3):218–22.

Petronio, S. 2002. *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

Posner, R. A. 1984. An economic theory of privacy. In *Philosophical dimensions of privacy: An anthology*, ed. F. D. Schoeman, 333–45. Cambridge: Cambridge University Press.

Reagle, J., and L. F. Cranor. 1997. The platform for privacy preferences. *Communications of the ACM* 42(2):48–55.

Rezgui, A., A. Bouguettaya, and M. Y. Eltoweissy. 2003. Privacy on the Web: Facts, challenges, and solutions. *IEEE Security and Privacy* 1(6):40–49.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91:93–114.

———. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychophysiology*, eds. J. T. Cacioppo and R. E. Petty, 153–74. New York: Guilford.

Schoenbachler, D. D., and G. L. Gordon. 2002. Trust and customer willingness to provide information in a database-driven relationship marketing. *Journal of Interactive Marketing* 16(3):2–16.

Sheehan, K. B. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society* 18(1):21–32.

Sheehan, K. B., and M. G. Hoy. 1999. Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising* 28(3):37–51.

———. 2000. Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing* 19(1):62–73.

Simon, H. A. 1955. A behavioural model of rational choice. *Quarterly Journal of Economics* 69(1):99–118.

———. 1972. *Models of bounded rationality: Behavioural economics and business organization* (vol. 2). Cambridge, MA: MIT Press.

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

Son, J. Y., and S. S. Kim. 2008. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly* 32(3):503–29.

Stanton, J. M. 2002. Information technology and privacy: A boundary management perspective. In *Socio-technical and human cognition elements of information systems*, ed. S. Clarke, E. Coakes, G. Hunter, and A. Wenn, 79–103. London: Idea Group.

Strandburg, K. J. 2006. Social norms, self control, and privacy in the online world. In *Privacy and technologies of identity: A cross-disciplinary conversation*, ed. K. J. Strandburg and D. S. Raicu, 31–53. New York: Springer Science.

Strater, K., and H. Richter. 2007. Examining privacy and disclosure in a social networking community. *SOUPS '07 Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA*, 157–58. http://portal.acm.org/citation.cfm?id=1280706 (accessed April 4, 2009).

Tavani, H. T. 2007. Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy* 38(1):1–22.

———. 2008. Informational privacy: Concepts, theories, and controversies. In *The handbook of information and computer ethics*, ed. K. E. Himma and H. T. Tavani, 131–64. Hoboken, NJ: Wiley-Interscience.

Tavani, H. T., and J. H. Moor. 2001. Privacy protection, control of information, and privacy-enhancing technologies. In *Readings in cyberethics*, ed. R. A. Spinello, and H. T. Tavani, 378–91. Sudbury, MA: Jones and Bartlett.

Turner, E. C., and D. Dasgupta. 2003. Privacy on the Web: An examination of user concerns, technology and implications for business organizations and individuals. *Information Systems Management* 20(1):8–18.

Vail, M. W., J. B. Earp, and A. I. Anton. 2008. An empirical study of consumer perceptions and comprehension of Web site privacy policies. *IEEE Transactions on Engineering Management* 55(3):442–53.

Van Dijk, J. 2006. *The network society* (2nd ed.). London: Sage.

Volkman, R. 2003. Privacy as life, liberty, property. *Ethics and Information Technology* 5(4):199–210.

Vu, K. P., V. Chambers, F. Garcia, B. Creekmur, J. Sulaitis, D. Nelson, R. Pierce, and R. Proctor. 2007. How users read and comprehend privacy policies. In *Human interface, Part II*, ed. M. J. Smith and G. Salvendy, 802–11. Berlin-Heidelberg: Springer-Verlag.

Wang, H., M. K. O. Lee, and C. Wang. 1999. Consumer privacy concerns about internet marketing. *Communications of the ACM* 41(3):63–70.

Warren, S. D., and L. D. Brandeis. The right to privacy. *Harvard Law Review* 4(5). http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm (accessed September 20, 2010).

Westin, A. F. 1967. *Privacy and freedom*. London: Bodley Head.

———. 1991. *Harris-Equifax consumer privacy survey*. Atlanta, GA: Equifax.

Xie, E., H. H. Teo, and W. Wan. 2006. Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters* 17(1):61–74.

Yao, M. Z., R. E. Rice, and K. Wallis. 2007. Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology* 58(5):710–22.

Zimmer, J. C., R. E. Arsal, M. Al-Marzouq, and V. Grover. 2010. Investigating online information disclosure: Effects of information relevance, trust and risk. *Information & Management* 47(2):115–23.