December 2006

Information Privacy in the Digital Era: An Exploratory Research Framework

Heng Xu  
*National University of Singapore*

Hock-Hai Teo  
*National University of Singapore*

Bernard Tan  
*National University of Singapore*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2006](http://aisel.aisnet.org/amcis2006)

**Recommended Citation**

[http://aisel.aisnet.org/amcis2006/120](http://aisel.aisnet.org/amcis2006/120)

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2006 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Information Privacy in the Digital Era: An Exploratory Research Framework

Heng Xu  
Department of Information Systems  
National University of Singapore  
xuheng@comp.nus.edu.sg

Hock-Hai Teo  
Department of Information Systems  
National University of Singapore  
teohh@comp.nus.edu.sg

Bernard C. Y. Tan  
Department of Information Systems  
National University of Singapore  
btan@comp.nus.edu.sg

ABSTRACT

Information privacy is at the center of discussion and controversy among multiple stakeholders including business leaders, privacy activists, and government regulators. However, conceptualizations of information privacy have been somewhat patchy in current privacy literature. In this paper we review the conceptualizations of information privacy through three different lenses (i.e., from the exchange, control and social contract views), and then identify alternative propositions related to factors that influence judgments about degree of privacy concerns. This exploratory research framework will serve as a starting point for further research.

Keywords  
Information Privacy, Privacy Calculus, Control, Trust.

INTRODUCTION

As information technologies increasingly expand the ability for organizations to store, process, and exploit personal data, privacy is at the center of discussion and controversy among multiple stakeholders including business leaders, privacy activists, and government regulators. Studies suggest that the loss of consumer confidence related to privacy fears has already hindered the growth of e-commerce by tens of billions of dollars (Cavoukian and Hamilton 2002). Governments throughout the world are taking notice, and in many jurisdictions there has been a concerted effort to restore confidence in e-commerce with data protection legislation as a complement to industry self-regulation. As such, information privacy has become a business issue, a social issue and a legal issue—increasingly difficult to ignore.

Although the term “Information Privacy in the Digital Era” or “Consumer Privacy Concerns” has been considerably hyped in the media, conceptualizations of information privacy have been somewhat patchy. There is a need for research that seeks not only to understand human conceptualizations of information privacy but also to discover what factors influence judgments about the degree of privacy concerns. Drawing on the marketing, psychological and social theories, we examine the information privacy phenomenon through three different lenses. The first lens, referred to as the exchange lens, conceptualizes privacy as a “privacy calculus” which contributes to the understanding of the trade-offs that consumers are willing to make when they exchange their personal information for certain benefits. The second lens, referred to as the control lens, emphasizes the role of control perception in explaining the privacy phenomenon. The third lens, referred to the social contract lens, frames the discussion of the bond of trust between organizations and individuals over information privacy. We apply each lens separately to discuss the conceptualizations of information privacy and to explore factors influencing privacy concerns. This exploratory research framework will serve as a starting point for further research on conceptualizing information privacy in details.

ORIGIN AND MEANING OF PRIVACY

Although various definitions of privacy have been given, there is no commonly accepted definition of this concept (Goodwin 1991) and thus privacy is considered as an elastic concept (Allen 1988) which subsumes a wide variety of definitions
In an 1890 law review article, Warren and Brandis first articulated the need for individuals to secure “the right to be left alone”\(^1\), which became the classic definition of privacy (Warren et al. 1984). In the 1960s, as mainframe computer technologies were assimilated into mainstream business and governmental organizations during this period, users of these technologies began exploring the massive computing and storage capabilities to create databases of information on individuals. In anticipation of some of the challenges to privacy that these systems would bring, one seminal book was published during this period: Alan Westin’s (1967) *Privacy and Freedom*, which made a significant contribution to our knowledge of privacy. Westin’s seminal view defined 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” (1967, p. 7).

Continued technological breakthroughs in the mid-to-late 1980s, including the personal computer, workstations, and communications network, enabled even broader diffusion of database management, marketing, and telemarketing tools (Turner et al. 2003). The collection, storage, and distribution of personal information continued to raise public apprehension regarding the accuracy of information, the ability of entities to safeguard and protect the distribution of personal information, and how the information would be used (Culnan 1993; Turner et al. 2003).

From the 1990s till present, continued advances in information technology in general and the growth in the use of Internet specifically, further facilitate the collection, distribution, and use of personal information (Turner et al. 2003). This is the period when the potential intrusion of privacy becomes a more critical and acute concern. The rise of identity theft in the late 1990s, along with highly publicized stalking cases based on accessing public record files, raised major issues about public’s privacy concerns about personal data in business and government record systems (Westin 2003). In consumer marketing, “the technology-based business model of the 1990s—we must know you to serve you—came into fundamental collision with the now dominant consumer model—let me decide what you know about me, thanks” (Westin 2003, p.442).

**VIEWING INFORMATION PRIVACY THROUGH THREE DIFFERENT LENSES**

Three domains of research inform our understanding of the nature of information privacy (see Figure 1). Each incorporates a different conceptualization of information privacy: economic, psychological, and social. Each of these lenses looks at information privacy differently and therefore provides a valid basis upon which the factors influencing judgments about the degree of privacy concerns could be reasonably proposed. These domains are presented as guiding propositions for future research.

---

\(^1\) According to Bigelow (1986), this notion originated from Michigan Supreme Court Justice Thomas M. Cooley.
exchange for some benefit, subject to an assessment that their personal information will subsequently be used fairly and that they will not suffer negative consequences in the future (Laufer et al. 1977). Similarly, Stone and Stone (1990) developed an expectancy theory based model to identify the antecedents and consequences of the motivation to protect organizational privacy. The basis of this model echoed the idea of privacy calculus by incorporating prior research on expectancy theory models of motivation and the view that “individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes” (Stone et al. 1990, p. 363).

This economic exchange perspective of information privacy is especially evident in works of analyzing privacy concerns (e.g., Culnan 2000; Culnan et al. 1999; Culnan et al. 2003; Milne et al. 1993; Milne et al. 2000; Milne et al. 1999; Sheehan et al. 2000). It was noted that the findings of the self-disclosure literature perspective—the focus on the interpersonal context notwithstanding—can be applied to an impersonal commercial context as well (Culnan 2000; Culnan et al. 1999; Milne et al. 1993). Specifically, consumers often consider the nature of the benefit being offered in exchange for information when deciding whether an activity violates their privacy (Culnan 1993; Goodwin 1991; Milne et al. 1993; Sheehan et al. 2000). Such benefit could have a specific financial value (such as a cash payment, product, or service), and in some cases, the value could be information based (such as access to information that is of interest) (Sheehan et al. 2000). In a study that attempted to measure the dollar value of information privacy, Hann et al. (2002) found that individuals are willing to trade off privacy concerns for economic benefits. In addition, the strategy of rewarding subjects in exchange for divulging personal attitudes or behaviors is well documented in the survey methodology literature as a means of increasing response rates (e.g., Barker 1989; Chebat et al. 1993).

Such an exchange perspective of privacy has been found to be “the most useful framework for analyzing contemporary consumer privacy concerns” (Culnan et al. 2003, p. 326). Consumers can be expected to behave as if they are performing a privacy calculus in assessing the outcomes they will receive as a result of providing personal information to corporations (Culnan 2000; Culnan et al. 1999; Culnan et al. 2003; Goodwin 1991; Milne et al. 2000; Milne et al. 1999). Hence, individuals will exchange their personal information as long as they perceive adequate benefits will be received in return—that is, benefits which exceed the perceived risks of the information disclosure (Culnan et al. 2003). In other words, consumers, when requested to provide personal information to corporations, would perform a risk-benefit analysis (i.e., ‘privacy calculus’) to assess the outcomes they would face in return for the information, and respond accordingly (Culnan 1995; Culnan et al. 2003). Based on such an analysis, a positive net outcome should mean that consumers are more likely to disclose their personal information and accept the potential negative outcome that accompanies the disclosure of personal information as long as they perceive that the benefits exceed the risks of disclosure (Culnan et al. 2003). Although this proposition is intuitively appealing and well known in information privacy literature, it “has not been tested empirically” (Culnan et al. 2003, p. 327). This gap in existing information privacy research provides further impetus for us to propose:

**Proposition 1a:** Higher level of benefit perception on personal information disclosure should lead to lower level of privacy concern.

**Proposition 1b:** Lower level of risk perception on personal information disclosure should lead to lower level of privacy concern.

### Information Privacy: A Control Lens

A second major perspective considers information privacy to be related to the control of personal information. This perspective is found in various prior works (e.g., Altman 1977; Johnson 1974; Laufer et al. 1973; Margulis 1974; Westin 1967) which have contributed to and stimulated research and theory on privacy as a control related concept. By adopting the limited-access approach to privacy (i.e., individual controls the information access to herself), a number of privacy theorists have put emphases on the concept of control when defining privacy. For example:

Westin (1967): privacy is “the right of the individual to decide what information about himself should be communicated to others and under what conditions”.

Proshansky, Ittelson and Rivin (1970): gaining privacy is to obtain freedom of choice or options to achieve goals, “… control over what, how, and to whom he communicates information about himself…”

Rapoport (1972): privacy is the ability to control interaction, to have options, devices and mechanisms to prevent unwanted interaction and to achieve desired interaction.

Altman (1974): “the selective control over access to the self or to one’s group.” “Privacy is an interpersonal boundary control process, designed to pace and regulate interactions with others.”
Margulis (1977): “privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability”.

Stone et al. (1983): “the ability (i.e., capability) of the individual to control personally (vis-à-vis other individuals, groups, organizations, etc.) information about one’s self”.

Margulis (2003a): privacy is viewed as control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access.

From the above control-oriented definitions of privacy, it seems that privacy theorists have applied the term “control” widely in the privacy literature as the justification or motivation for defining privacy. Wolfe and Laufer (1974) suggested that “the need and ability to exert control over self, objects, spaces, information and behavior is a critical element in any concept of privacy” (p. 3). Westin’s (1967) frequently cited “components” of privacy—solitude, anonymity, intimacy, and reserve—identify ways in which individuals control information about themselves.

The above view of privacy as a control related concept is also found in the works of a number of consumer privacy studies (e.g., Dinev et al. 2004; Foxman et al. 1993; Goodwin 1991; Nowak et al. 1997; Phelps et al. 2000; Sheehan et al. 2000). For instance, consumers perceive information disclosure as less privacy-invasive when, among other things, they believe that they will be able to control future use of the information and that the information will be used to draw accurate inferences about them (Culnan et al. 1999). It was further indicated that although much of the previous psychological, legal, and philosophical research has focused on control over physical intrusions, contemporary technology suggests that control over information represents the greater concern (Goodwin 1991). Control, therefore, becomes the key factor which provides the greatest degree of explanation for privacy concern (Sheehan et al. 2000).

Some researchers have equated the concept of privacy with control. Johnson (1974), for instance, defined privacy as “secondary control in the service of need-satisfying outcome effectance” (p. 91). Goodwin (1991) defined consumer privacy by two dimensions of control: control over information disclosure and control over unwanted physical intrusions into the consumer’s environment. However, many researchers reason that control is actually one of the factors that shape privacy and that privacy is not control per se (Laufer et al. 1977; Margulis 2003a; 2003b). For instance, Laufer and Wolfe (1977) conceptualized control as a mediating variable in the privacy system by arguing that “a situation is not necessarily a privacy situation simply because the individual perceives, experiences, or exercises control” (p. 26). Conversely, the individual may not perceive she has a control, yet the environmental and interpersonal elements may create perceptions of privacy (Laufer et al. 1977). Therefore, privacy should be more than control (Laufer et al. 1977; Margulis 2003a; 2003b) and control might be one of the factors which determine privacy state (Dinev et al. 2004).

These considerations suggest that perceived control over disclosure and subsequent use of personal information is a separate construct from privacy concerns and that the two constructs are negatively related. Hence, we hypothesize that perceived control over disclosure and subsequent use of personal information is an antecedent to privacy concerns.

**Proposition 2:** Higher level of control perception over disclosure and subsequent use of personal information should lead to lower level of privacy concern.

**Information Privacy: A Social Contract Lens**

A third important perspective on information privacy views it through a social contract lens (e.g., Caudill et al. 2000; Culnan 1995; Culnan et al. 2003; Hoffman et al. 1999; Milne 1996; Milne et al. 1993; Phelps et al. 2000). The Integrative Social Contract Theory (ISCT) (Donaldson et al. 1994; 1995; 1999), the most widely used ethical theory in the context of information privacy, has been used to strengthen the bond of trust between corporations and consumers. ISCT posits that members of a given community or industry behave fairly if their practices are governed by social contracts

2 ISCT encompasses two different types of social contracts (Donaldson and Dunfee 1999, p.19): 1) the hypothetical or “macro” contract, reflecting hypothetical agreement among rational members of a community. Such contract usually refers to broad, hypothetical agreements among rational people and it is designed to establish objective background standards for social interaction. 2) The “extant” or “micro” contract, reflecting an actual agreement within a community. Such contract usually refers to non-hypothetical, actual (although typically informal) agreements existing within and among industries, national economic systems, corporations, trade associations, and so on.
participants in a particular transaction, and thus it clearly corresponded to the exchange relationship central to marketing thought and practice (Donaldson et al. 1994; 1995; 1999; Dunfee et al. 1999).

According to this ISCT perspective, a social contract is held to occur when consumers provide personal information to certain corporations, and the corporation in turn offers some benefits to the consumer (Caudill et al. 2000; Culnan 1995; Milne 1996; Milne et al. 1993; Phelps et al. 2000). A social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behavior of those involved (Caudill et al. 2000). For the corporation, one generally understood obligation accruing from entering into this social contract is that the corporation will undertake the responsibility to manage consumers’ personal information properly (Caudill et al. 2000; Culnan 1995; Milne 1996; Milne et al. 1993; Phelps et al. 2000). This implied contract is considered breached if consumers are unaware that their information is being collected, if the corporation rents the consumers’ personal information to a third party without permission, or if the corporation divulges the consumers’ personal information to unauthorized parties without consumers’ consent, or if the corporation uses the consumers’ personal information for other purposes without notifying consumers (Culnan 1995; Milne 1996; Phelps et al. 2000).

Thus, the social contract, dictating how corporations handle consumers’ personal information in an implicit form (not in an economic or a legal form), involves unspecified obligations and requires consumers’ trust on the corporation’s compliance to this social contract (Caudill et al. 2000; Culnan et al. 2003; Hoffman et al. 1999). The concept of social contract in the consumer privacy context means that consumers are willing to disclose personal information for certain benefits as long as they trust the corporation that it would uphold its side of social contract. Hence, the lack of consumer trust in customer-centric enterprises seems to be a critical barrier that hinders the efforts of these enterprises to collect personal information from consumers for the purpose of providing services. According to Hoffman et al. (1999), close to 95% of consumers have declined to provide personal information to websites, and 63% of these indicated this is because they do not trust those collecting the data. It is very likely that the customer-centric enterprises that are considered trustworthy by consumers may incur consumers’ lower privacy perceptions. That is to say, consumer trust may play an important role in alleviating consumers’ privacy concerns.

In reviewing the extant online trust literature, it seems that the concept of privacy concern has been implicitly incorporated in various studies regarding issues of trust in the online environment. For instance, many trust researchers proposed various models of trust that consider the privacy policies and third party seals (e.g., BBBOnline and TRUSTe seal) as the structural assurances built into a Web site which might affect trusting beliefs and trust related behaviors (e.g., Gefen et al. 2003; McKnight et al. 2002). However, the explicit involvement of privacy is frequently overlooked among these studies. Davison et al. (2003) feel “quite astonishing that a high proportion of the burgeoning literature on trust in the context of B2C fails to control for privacy, fails to meaningfully consider it, or even completely overlooks it” (p. 344). We, therefore, attempt to address this gap by predicting the role of trust in alleviating privacy concerns:

**Proposition 3: Higher level of trust belief should lead to lower level of privacy concern.**

**CONCLUSION**

To date, the conceptualizations of the phenomenon of information privacy are varied and somewhat confused. This study provides one of the first attempts to synthesize the conceptualizations of information privacy, which showed that the phenomenon of information privacy could be explained from at least three different theoretical perspectives (i.e., from the exchange, control and social contract views). Further research could be directed to investigate how these three different theoretical perspectives could be integrated or contrasted in the privacy literature. In addition, since some scholars have suggested that the phenomenon of information privacy may be culturally dependent (e.g., Milberg et al. 2000), future research should add the fourth theoretical perspective - the cultural lens to the current research framework.

**REFERENCES**


