Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services

Heng Xu, Hock-Hai Teo, Bernard C. Y. Tan, Ritu Agarwal,

To cite this article:
Heng Xu, Hock-Hai Teo, Bernard C. Y. Tan, Ritu Agarwal, (2012) Research Note—Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. Information Systems Research 23(4):1342-1363. https://doi.org/10.1287/isre.1120.0416

Information Systems Research
Vol. 23, No. 4, December 2012, pp. 1342–1363
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.1120.0416

Research Note

Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services

Heng Xu
College of Information Sciences and Technology, The Pennsylvania State University, University Park, Pennsylvania 16802, hxu@ist.psu.edu

Hock-Hai Teo
Department of Information Systems, National University of Singapore, School of Computing, Singapore 117418, teohh@comp.nus.edu.sg

Bernard C. Y. Tan
Department of Information Systems, National University of Singapore, School of Computing, Singapore 117418, btan@comp.nus.edu.sg

Ritu Agarwal
Robert H. Smith School of Business, University of Maryland, College Park, Maryland 20742, ragarwal@rhsmith.umd.edu

This study seeks to clarify the nature of control in the context of information privacy to generate insights into the effects of different privacy assurance approaches on context-specific concerns for information privacy. We theorize that such effects are exhibited through mediation by perceived control over personal information and develop arguments in support of the interaction effects involving different privacy assurance approaches (individual self-protection, industry self-regulation, and government legislation). We test the research model in the context of location-based services using data obtained from 178 individuals in Singapore. In general, the results support our core assertion that perceived control over personal information is a key factor affecting context-specific concerns for information privacy. In addition to enhancing our theoretical understanding of the link between control and privacy concerns, these findings have important implications for service providers and consumers as well as for regulatory bodies and technology developers.

Key words: privacy; context-specific concerns for information privacy; psychological control; control agency; individual self-protection; industry self-regulation; and government regulation

History: Elena Karahanna, Senior Editor; Mariam Zahedi, Associate Editor. This paper was received on August 20, 2008, and was with the authors 24 months for 4 revisions. Published online in *Articles in Advance* April 18, 2012.

1. Introduction

Information privacy is an increasingly critical concern for many individuals around the world. The global diffusion of mobile technologies and the unbounded options for gathering, storing, processing, disseminating, and exploiting personal information trigger consumer concerns (FTC 2010). Over the past decade, scholars in information systems have examined the topic of privacy concerns (e.g., Angst and Agarwal 2009, Bansal et al. 2010, Dinev and Hart 2006, Malhotra et al. 2004, Son and Kim 2008) related to the collection and use of personal information from a variety of different perspectives. A general conclusion from this stream of research is that individuals would resist online transactions or adoptions of new technologies in the presence of significant privacy concerns.

It has been posited that individuals tend to have lower privacy concerns if they perceive a certain degree of *control* over the collection and use of their personal information (Dinev and Hart 2004, Xu et al. 2008). Considering the potential importance of control in the context of information privacy, this study explores and empirically demonstrates the contribution of the psychological control theories to understanding information privacy. We conducted an experimental study in the specific context of location-based services (LBS). Three privacy assurance approaches (individual self-protection, industry self-regulation, and government legislation) were

manipulated in the experiment and their effects on control perceptions and privacy concerns were examined.

The current study contributes to existing privacy research in several important ways. First, prior research has shown a lack of clarity in explicating the link between control and privacy: some studies have defined privacy as control *per se* (e.g., Goodwin 1991, Milne and Rohm 2000); others have positioned control as a key factor shaping privacy (e.g., Laufer and Wolfe 1977, Dinev and Hart 2004). There have been very few attempts to bring control theories into privacy research to clarify the nature of control. The current research contributes to this controversial issue by explicating this control—privacy contention. Second, following the call by Margulis (2003a, b), current research has explicitly integrated the literature on psychological control into theories of privacy. Toward this end, we have adopted the control agency theory to make a theoretical distinction of different privacy assurance approaches by explicitly linking them with different types of control agencies. Finally, most existing privacy research focuses on examining the individual effect of privacy assurance approaches (e.g., Culnan and Bies 2003, Metzger 2006). Building on the control agency framework, this research extends the literature by proposing interaction effects of these privacy assurance approaches on alleviating privacy concerns, based on the type of control agencies they can provide.

In what follows, we first provide an overview of prior relevant literature to establish a theoretical foundation for studying privacy, privacy concerns, control, and privacy assurance approaches. Then we develop the logic underlying the research hypotheses that relate different privacy assurance approaches to privacy concerns, mediated by perceived control. This is followed by a description of the research methodology and findings. The paper concludes with a discussion of the key results, directions for future research, and the practical implications of the findings.

2. Theoretical Development

2.1. The Concept of Privacy and the Construct of Privacy Concerns

Although various conceptions of privacy have been given in the literature, "the notion of privacy is fraught with multiple meanings, interpretations, and value judgments" (Waldo et al. 2007, p. x). The rich body of conceptual work has welcomed research to synthesize various conceptions and identify common ground. For example, Solove (2007) describes privacy as "a shorthand umbrella term" (p. 760) for a set of privacy problems resulting from information collection, information processing, information dissemination, and invasion activities. Culnan and Williams (2009) argue that these activities on information reuse and unauthorized access by organizations "can potentially threaten an individual's ability to maintain a condition of limited access to his/her personal information" (p. 675). Solove's groundwork (2007) for a pluralistic conception of privacy differentiates the *concept* of privacy (as an individual state) from the *management* of privacy (arising from organizational information processing activities). From the perspectives of individuals (Dhillon and Moores 2001, Schoeman 1984), we define privacy as a state of limited access to personal information.

Another challenge faced in understanding privacy is the diversity of measurements used by prior research. Measures that have been adopted for the examinations of privacy include attitudes toward privacy (e.g., Buchanan et al. 2007), concerns for privacy (e.g., Smith et al. 1996), and privacy-related behavioral intentions (e.g., Dinev and Hart 2006). Based on an extensive review of privacy literature, Smith et al. (2011) note that the variable of "privacy concerns" becomes the central construct within IS research and it has become the proxy to operationalize the concept of "privacy." Specifically, the Smith et al. (1996) Concern for Information Privacy (CFIP) scale has been considered as one of the most reliable scales for measuring privacy concerns, using four data-related dimensions: collection, errors, unauthorized secondary use, and improper access to information. As Bansal et al. (2008) note, these four dimensions of CFIP supported the underlying definitions of the U.S. Federal Trade Commission's (FTC) fair information practices (FTC 2000), which include the stipulations that consumers be given *notice* that their personal information is being collected (mapped as *collection* of CFIP), *consent* with regard to the authorized use of their information (mapped as *unauthorized secondary use* of CFIP), *access* to personal data records to assure data accuracy (mapped as *errors* of CFIP), and *security* to prevent these data records from unauthorized access (mapped as *improper access* of CFIP).

More recently, Malhotra et al. (2004) develop a multidimensional scale of Internet Users Information Privacy Concerns (IUIPC), which adapted the instrument of CFIP into the Internet context. Based on the social contract and justice theories, IUIPC identified three dimensions of Internet privacy concerns: *collection* of personal information (rooted in the *distributive justice* theory), *control* over personal information (rooted in the *procedural justice* theory), and *awareness* of organizational privacy practices (rooted in the *interactional and information justice* theory). In this research, we ground our work in the CFIP instead of the IUIPC. This is because, compared to IUIPC's focus on an individual's subjective view of fairness, CFIP's

focus on the organizational privacy practices naturally maps with the FTC's fair information practices, which serve as the privacy standard used in the United States to address consumer privacy concerns.

2.2. General vs. Context-Specific Concerns for Information Privacy

In the IS field, most positivist studies on privacy have operationalized the construct of privacy concerns from two broad perspectives: some have treated it as a *general concern* of worries over possible loss of information privacy across contexts (e.g., Awad and Krishnan 2006, Bellman et al. 2004, Dinev and Hart 2006, Smith et al. 1996); others have approached it as a *context-specific concern* for information privacy regarding particular websites or technologies (e.g., Bansal et al. 2008, Junglas et al. 2008, Oded and Sunil 2009, Pavlou et al. 2007). Emphasizing the role of contextual factors in shaping privacy beliefs, scholars in computer science (Ackerman and Mainwaring 2005), law (Solove 2006), and sociology (Margulis 2003a) have noted that it is important to theoretically draw a distinction between *general* concerns for privacy and *context-specific* concerns. For example, Ackerman and Mainwaring (2005) point out that people's expectations and problems concerning privacy may all differ when moving among areas of computation and tasks. What may be a privacy concern in healthcare websites may be a very different problem for users than in social networking websites.

Therefore, we argue that these two types of privacy concerns (general versus context-specific concerns) have distinct characteristics: Individuals' general concerns for information privacy reflect their inherent needs and attitudes toward maintaining privacy, which are conceived to be more stable across domains or contexts. Context-specific concerns for information privacy, on the other hand, tie the individuals' assessments of privacy concerns to a specific context with a specific external agent, demanding that consumers be involving in a dynamic assessment process in which their privacy needs are evaluated against their information disclosure needs are weighed against information disclosure needs (Sheehan 2002). In terms of the relationship between these two types of privacy concerns, Li et al. (2011) have suggested that the effect of general privacy concerns may be overridden by context-specific privacy concerns because of the impact of contextual factors associated with a specific website and its information collection activities. In the IS field, Malhotra et al. (2004, p. 349) have made an explicit call for research on examining privacy concerns "at a specific level":

> *. . . privacy research in the IS domain has paid little attention to consumers' perceptions specific to a particular context . . . . However, our findings clearly reveal that to have a complete understanding of consumer reactions to information privacy-related issues, researchers should examine not only consumers' privacy concerns at a general level, but also consider salient beliefs and contextual differences at a specific level.*

Following this call for examining privacy concerns at a specific level, we focus on context-specific as opposed to general concerns for information privacy in this research. Context has been defined as "stimuli and phenomena that surround and, thus, exist in the environment external to the individual, most often at a different level of analysis" (Mowday and Sutton 1993, p. 198, as cited in Smith et al. 2011). We consider contexts to incorporate different tasks or activities that consumers may undertake with different types of companies or websites (e.g., specific vendors, online pharmacies, and social networking sites) as well as different types of information collected from consumers (e.g., behavioral, location, financial, health, and biographical). We argue that privacy concerns are context-specific, based in the specifics of by whom, why, when, and what type of personal information is being collected, distributed, and used. Concerns for information privacy in any specific context can be circumscribed by the elements within these specifics. In this research, we adapted the measures of CFIP from a general level to a context-specific level and define context-specific CFIP as "consumers' concerns about possible loss of privacy as a result of information disclosure to a specific external agent" (in our case, a service provider) (Xu et al. 2011, p. 800).

2.3. Psychological Perspective of Control

Although the element of control is embedded in most privacy definitions (e.g., Altman 1976, Goodwin 1991, Johnson 1974) and has been used to operationalize privacy in measurement instruments (e.g., Malhotra et al. 2004), its meaning has been interpreted differently (see Table 1). For example, control has been used to refer to various targets such as the choice to opt out of an information exchange (Milne and Rohm 2000), ability to affect the dissemination and use of personal information (Phelps et al. 2000), and secondary (indirect) control over the attainment of privacy-related outcomes (Johnson 1974). As Margulis (2003b) pointed out, the very nature of control is ambiguous in the context of information privacy. Similarly, Solove (2002) noted that "theorists provide little elaboration as to what control really entails, and it is often understood too narrowly or too broadly" (p. 1112). Margulis (2003a) also pointed out that privacy theorists had failed to adequately define the nature of control in their theories of privacy. It seems that the frequent link between control and privacy has not contributed as much to clarifying privacy issues as it should have. In response to the call for a stronger theoretical basis for research on information privacy,

Table 1 Frequent Linkage of Privacy and Control

Authors	Conceptualization of privacy	Role of control	Meaning of control	Nature of control
Altman (1976)	Privacy is conceptualized as selective control of access to the self or to one's group.	Privacy is defined as interpersonal control.	Control is conceptualized as an active and dynamic regulatory process.	Behavioral
Caudill and Murphy (2000)	Privacy is defined as consumers' control of their information in a marketing interaction and the degree of their knowledge of the collection and use of their personal information.	Control is one dimension defining privacy.	Control refers to the ability to decide the amount and depth of information collected (i.e., through opt-in and opt-out options).	Behavioral
Culnan (1993)	Privacy is defined as the ability of an individual to control the access others have to personal information.	Control is a core dimension underlying attitudes toward privacy.	Control refers to the ability of individuals to decide how their information is reused. Loss of control is operationalized as a dimension of privacy concerns.	Behavioral
Dinev and Hart (2004)	Privacy is defined as the right to disclose information about oneself.	Perceived ability to control is an antecedent to privacy concern.	Control refers to the mechanism a website provides for consumers to control their submitted personal information.	Behavioral
Goodwin (1991)	Privacy is defined based on two dimensions of control: control of information disclosure and control over unwanted intrusions into the environment.	Privacy is defined as control.	Control refers to the ability to decide (a) the presence of other people in the environment and (b) dissemination of information related to or provided during a transaction.	Behavioral
Hoadley et al. (2010)	Privacy is conceptualized as individuals' perceived control of their information in an online social interaction and the ease of information access by others.	Illusory loss of control can lead to privacy concern.	Control is conceptualized as a psychological perception (instead of actual controllability), and illusory loss of control, prompted by the interface change, can trigger users' privacy concerns.	Psychological
Johnson (1974)	Privacy is defined as secondary control in the service of need-satisfying outcome effectance.	Privacy is defined as behavioral selection control.	Control is conceptualized with two dimensions: primary (direct) and secondary (indirect) personal control over the attainment of privacy-related outcomes.	Behavioral
Laufer and Wolfe (1977)	Privacy is tied to concrete situations with three dimensions: self-ego, environmental, and interpersonal.	Control is a mediating variable in the privacy system.	Control refers to the ability to choose how, under what circumstances, and to what degree the individual is to disclose information.	Behavioral
Malhotra et al. (2004)	Privacy is defined 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.	Control is viewed as a dimension of privacy concern.	Control refers to individuals' ability to decide how their information is collected, used, and shared.	Behavioral
Milne and Rohm (2000)	Privacy is defined as a state, on the basis of who controls consumer data and whether consumers are informed of information collection and privacy rights.	Control is one dimension defining privacy.	Control refers to the ability to remove names from marketing list (i.e., through opt-out mechanism).	Behavioral
Phelps et al. (2000)	Privacy refers to the ability to affect the dissemination and use of personal information and control over unwanted use.	Control is one dimension defining privacy and is an antecedent to concern for firms' information practices.	Control refers to the ability to influence how personal information is used and who will have access to it.	Behavioral
Zweig and Webster (2002)	Privacy is implicitly defined as the extent to which people can control the release and dissemination of personal information.	Control is an antecedent to perceived invasion of privacy.	Control is operationalized as the technical ability to control over when one's video image is displayed.	Behavioral

this study explores and empirically demonstrates the contribution of psychological control perspective to the understanding of privacy concerns.

As shown in Table 1, there has been movement toward the interpretation of control as the *ability* of consumers to voice or exit in order to influence changes in organizational privacy practices they find to be objectionable (Malhotra et al. 2004). For example, Stewart and Segars (2002, p. 40) noted that "while consumers' privacy concerns may relate to very specific information practices such as collection, secondary use, access, and errors, the supra concern that accounts for the interdependencies among these factors may be the degree of control over their personal information that is retained by the consumer." Such focus on *actual* control in the IS literature, however, excludes those aspects of psychological control that may *not* directly involve behavioral attempts to effect a change. Hoadley et al. (2010) echoed the importance of psychological control by noting that privacy is not simply related to the factual state of information disclosure, access, and use (i.e., zeros-and-ones of data privacy). In their analysis of the event of the Facebook News Feed privacy outcry, Hoadley et al. (2010) pointed out that "no privacy (from a zeros-and-ones perspective) was compromised due to the introduction of the feed features" (p. 57), because "Facebook's old and new interfaces are isomorphic" (p. 55) in terms of the actual controllability over who had access to what information. Yet the News Feed features "induce lower levels of *perceived* control over personal information due to easier information access, which in turn leads to a *subjectively* higher perception of privacy intrusion" (Hoadley et al. 2010, p. 57).

The above discussions indicate that the perceived loss of control over personal information may be a function of not only objective reality but also "the individual's subjective beliefs, vicarious observations, and biases" (Hoadley et al. 2010, p. 57). "Veridicality is not necessary or sufficient to bring about the perception of control, although the perception of control, however illusory, may have a profound effect on the individual" (Wallston 2001, p. 49, as cited in Hoadley et al. 2010). The case of the Facebook News Feed privacy outcry has demonstrated how an "illusory" loss of control, prompted by the introduction of News Feed features, triggered users' privacy concerns. To provide a richer conceptual description of control, this study explores and empirically demonstrates the contribution of psychological control theories to the understanding of control in the privacy context.

In the psychology literature, control is commonly treated as a perceptual construct because perceived control affects human behavior much more than actual control (Skinner 1996). Perceived control has been generally defined as an individual's beliefs about the presence of factors that may facilitate or impede performance of the behavior (Ajzen 2001). Being cognitive in nature, perceived control is subjective and need not necessarily involve attempts to effect a behavioral change (Langer 1975). That is to say, perceived control may be based on the individual's evaluation of the objective reality (i.e., the resources and opportunities facilitating personal control), or it might be based on the individual's attempts to "give up control" to someone who is more able than oneself to produce the desired outcome (Miller 1980). In this research, we define perceived control over personal information as an individual's belief about the presence of factors that may increase or decrease the amount of control over the release and dissemination of personal information.

2.4. Privacy Assurance Approaches: A Control Agency Perspective

In the privacy literature, control has been understood as a form of information ownership (Westin 1967) conceptualized as the individual choice to opt in to or opt out of an electronic information exchange environment completely or selectively (Caudill and Murphy 2000), or operationalized as the technical ability to control the information display (Zweig and Webster 2002). This body of literature's focus on *individual* control, however, makes it too narrow a conception because it excludes those aspects of control that are beyond individual choice. The follow-up question is whether individuals are able to execute significant information control in all circumstances, given discrepancies in awareness and power in the process of data gathering and transfer (Schwartz 1999). The implication is that privacy assurance "is not just a matter for the exercise of individual actions but also an important aspect of institutional structure" (Xu et al. 2011, p. 799). As Solove (2002) noted, "[P]rivacy . . . is not simply a matter of individual prerogative; it is also an issue of what society deems appropriate to protect" (p. 1111). To provide a richer conceptual description of privacy assurance, this research demonstrates the contribution of control agency theory to the understanding of privacy assurance approaches. In particular, the control agency theory allows us to not only examine the effects of *personal control*, in which the self acts as the control agent to protect privacy, but also include *proxy control*, in which powerful others (such as the government and industry regulators) act as the control agents to protect privacy.

Two paths to enhancing control perceptions can be identified from the control agency perspective, which differentiates *control* conceptually among its various

components. First, perceived control can be amplified by having direct personal control, where the control agent is the self (Bandura 2001, Skinner 1996). Individuals who value personal agency would prefer exercising direct *personal control* because they "would especially feel themselves more self-efficacious when their agency is made explicit" (Yamaguchi 2001, p. 226). Personal agency suggests that individuals are motivated to act upon opportunities that allow them to be the sole initiator of their behavior (Bandura 2001). Second, perceived control can be increased by having proxy control, where the control agent is powerful others (Bandura 2001, Yamaguchi 2001). With proxy control, individuals attempt to align themselves such that they are able to gain control through powerful others. In proxy agency, "people try by one means or another to get those who have access to resources or expertise or who wield influence and power to act at their behest to secure the outcomes they desire" (Bandura 2001, p. 13).

The privacy literature describes three major approaches to help protect information privacy: individual self-protection, industry self-regulation, and government legislation (Culnan and Bies 2003, Son and Kim 2008, Tang et al. 2008, Xu et al. 2010). These approaches fall into two generic categories based on the type of control agency they provide: personal control enhancing mechanism and proxy control enhancing mechanism. The former control enhancing mechanism (via individual self-protection) comprises tools and approaches that enable individuals to directly control the flow of their personal information to others. As is evident with individual self-protection, the agent of control is the self and the effect of this agency arises due to the opportunity for direct personal control. The latter mechanism (via industry self-regulation or government legislation) refers to the institution-based approaches where powerful forces (i.e., government legislator or industry self-regulator) act as the control agents for consumers to exercise proxy control over their personal information.

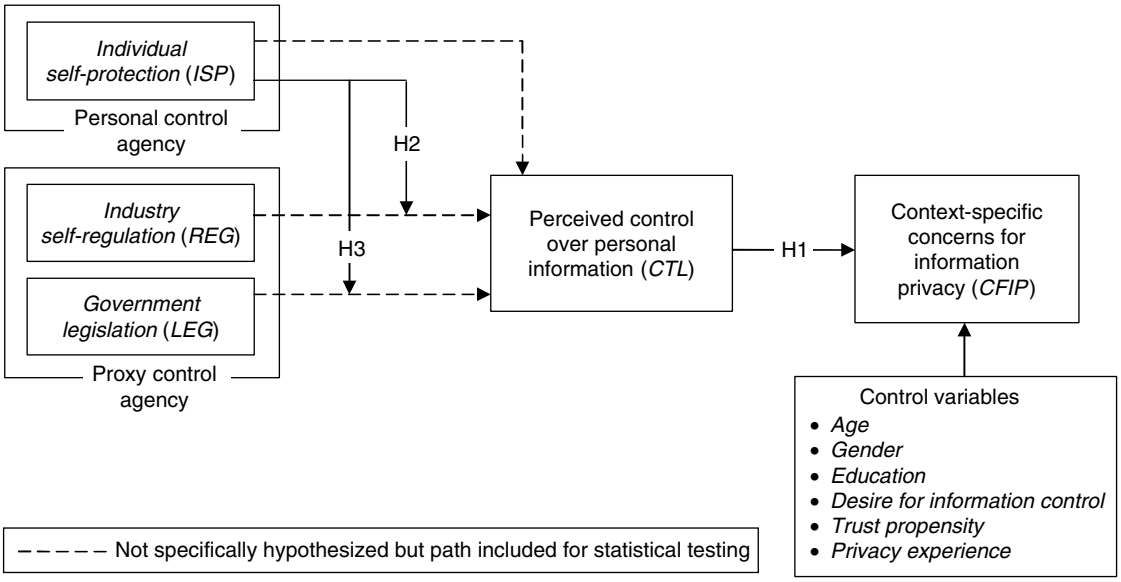
In general, the public has been skeptical about the efficacy of individual self-protection and industry self-regulation for protecting information privacy (Culnan 2000, Tang et al. 2008, Turner and Dasgupta 2003). As a result, privacy advocates continue to demand stronger government regulation to restrain abuse and mishandling of personal information by companies (Culnan 2000, Swire 1997). Prior research on privacy assurance approaches has focused on how these approaches individually influence privacy beliefs and privacy related constructs such as privacy concerns, trust, or perceived risks (Hui et al. 2007, Son and Kim 2008, Tang et al. 2008). The direct effects of these privacy assurance approaches on influencing privacy related beliefs are intuitively appealing and have been indirectly supported in prior research. Our study is particularly interested in the interaction effects, i.e., how interactions of these privacy assurance approaches may collectively influence privacy concerns through the effect on perceived control. Because these mechanisms do not appear in isolation in practice, their individual effects are less likely to be ecologically informative than are their interaction effects.

2.5. Privacy Concerns Pertaining to Location-Based Services

In contrast to most privacy research that was conducted in the conventional Web context (e.g., Bansal et al. 2010, Dinev and Hart 2006, Son and Kim 2008), we develop and empirically test a research model in an understudied context of location-based services (LBS). LBS have a number of characteristics that make them particularly suitable for current research. First, positioning systems are likely to endure as an important technology because of the significant investments made in their development and associated telecommunication infrastructure (ABI 2011, FTC 2009). Reputable firms like Google, Yahoo, and Facebook as well as startups like Foursquare, Gowalla, Loopt, and many others are entering the market of LBS. Consequently, LBS that utilize spatial location information to provide value-added services to users will become a prevalent phenomenon globally (ABI 2011). Second, compared with the Internet environment, the ubiquitous computing environment offers individuals higher potential for *control* over communication and exchange of personal information (Junglas and Watson 2006). Therefore, understanding the link between perceived control and privacy concerns has become much more important.

Finally, in a context characterized by ubiquity and uniqueness where consumers engage more activities that collect, analyze, and visualize personal information, privacy concerns have become particularly salient (ABI 2011). As highlighted in the FTC's recent town hall meeting on the mobile marketplace, the use of LBS often discloses the goegraphical location information of a user in real time, rendering the potential for privacy intrusions very significant (FTC 2009). These concerns pertain to the mobile devices' automatic generation and transmission of consumers' location information; the confidentiality of accumulated personal data (e.g., their location data, identity, and behavior data); and the potential risk that individuals would experience with a breach of confidentiality (FTC 2009). To the degree that that privacy concerns represent a major inhibiting factor in the adoption of LBS (ABI 2011), it is important to understand how such concerns can be addressed.

Figure 1 Research Model



3. Research Model and Hypothesis Development

Figure 1 presents the research model. In sum, the theoretical foundation for this study is centered on the control agency theory (Bandura 2001, Yamaguchi 2001), which suggests that mechanisms triggering control perceptions over personal information can be instrumental in alleviating privacy concerns. By explicitly associating different mechanisms with different forms of control agency, the interaction effects of these mechanisms can be predicted. In the following sections, we present arguments for why each mechanism is expected to enhance perceived control. Then the research hypotheses are constructed around interactions between the personal and proxy control enhancing mechanisms.

3.1. Effects of Perceived Control on Context-Specific Privacy Concerns

Although control has received attention as the common core of definitions of privacy (e.g., Awad and Krishnan 2006, Son and Kim 2008), researchers in law and social science have noted that it is important to treat these two concepts as separate and supporting concepts (Margulis 2003a, b; Solove 2002). Waldo et al. (2007) argued that "control over information cannot be the exclusive defining characteristic of privacy" (p. 61) and privacy is more than control. Similarly, DeCew (1997) pointed out that "we often lose control over information in ways that do not involve an invasion of our privacy" (p. 53). Consistent with the emphasis in the law and social science literature on the relationship between control and privacy, we argue in this research that control is a key variable in determining privacy state but privacy is not control *per se*. This distinction enables us to avoid conflating the concept of privacy with the concept of control, which is used to justify the effects of privacy assurance approaches through different control agencies.

Prior privacy research suggests that consumers tend to have lower levels of privacy concerns when they believe that they have control over the disclosure and subsequent use of their personal information in a specific situation (Culnan and Armstrong 1999, Culnan and Bies 2003, Phelps et al. 2000). In other words, perceived control helps reduce people's context-specific privacy concerns if they perceive current and future risks as low (Milne and Culnan 2004). Empirical evidence has revealed that consumers' control perceptions over collection and dissemination of personal information are negatively related to privacy concerns regarding particular websites (Xu et al. 2008). These considerations suggest that in a specific context, individuals tend to have lower privacy concerns if they get a sense of greater control over their personal information that is collected and used by a specific company. Following this perspective, we propose that perceived control over personal information is negatively related to context-specific privacy concerns.

Hypothesis 1 (H1). *Perceived control over personal information has a negative effect on the context-specific concerns for information privacy.*

3.2. Effects of Privacy Assurance Approaches on Personal Control

3.2.1. Personal Control Through Individual Self-Protection. Individuals are striving for primary control over their environment when they exercise

personal control through individual self-protection actions (Weisz et al. 1984). Such a mechanism empowers individuals with direct control over how their personal information may be gathered by service providers. The privacy literature (Culnan and Bies 2003, Milne and Culnan 2004, Son and Kim 2008) describes two major types of individual self-protection approaches: nontechnological and technological approaches. An array of nontechnological self-protection approaches has been discussed in terms of reading privacy policies, refusal to reveal personal information, misrepresentation of personal information, removal from mailing lists, negative word-of-mouth, complaining directly to the online companies, and complaining indirectly to third-party organizations (see Son and Kim 2008 for a review). In the context of this research, we focus on examining technological self-protection approaches because these technological privacy assurances have been understudied in the IS field.

Technological self-protection approaches comprise privacy-enhancing technologies (PETs) that allow individuals to protect their information privacy by directly controlling the flow of their personal information to others (Burkert 1997). PETs are quite numerous, with technologies such as anonymous web surfing and communication tools, cookie management tools, and the Platform for Privacy Preference (P3P) and its user agents (Cranor 2002). In the context of online social networks, to assuage user perceptions of privacy invasions, a number of social networking sites have been rolling out privacy-enhancing features that provide users with the capabilities to limit information disclosure and access (Hoadley et al. 2010). These privacy enhancing features can provide users with means to control the disclosure, access, and use of their personal information and thus may increase the level of perceived control. In the specific context of LBS, users are given PETs to turn off the location tracking from their mobile devices (Barkhuus et al. 2008, Tsai et al. 2010). Some devices also allow users to specify the accuracy of location information to be released to LBS providers (Barkhuus et al. 2008, Tsai et al. 2010). Hence, having mobile devices with PETs should facilitate individuals' beliefs that they can execute direct control over their personal information in the context of LBS.

3.2.2. Proxy Control Through Industry Self-Regulation. Industry self-regulation is a commonly used approach that mainly consists of industry codes of conduct and self-policing trade groups and associations as a means of regulating privacy practices. In practice, third-party intervention has been employed to provide trustworthiness to companies through membership of self-policing associations (e.g., Direct Marketing Association) or privacy seals (e.g., TRUSTe)[1] that are designed to confirm sufficient privacy assurance (Culnan and Bies 2003). An example of an industry self-regulator is the Cellular Telecommunications and Internet Association (CTIA), which has established guidelines for LBS providers to handle personal information linked to location (CTIA 2008). Other examples, including groups such as TRUSTe, have prescribed responsible privacy practices and implementation guidelines for LBS providers to safeguard private information (TRUSTe 2004).

Prior research has shown that companies that announce membership in self-policing associations or seals of approval foster consumers' perceptions of control over their personal information (Xu et al. 2008). Further, failure to abide by the terms of self-policing associations or seals of approval can mean termination as a licensee of the program or "referral to the appropriate law authority, which may include the appropriate attorney general's office, the FTC, or the Individual Protection Agency" (Xu et al. 2011, p. 806). Thus these self-regulatory structures create incentives for companies to refrain from behaving opportunistically (Tang et al. 2008). Hence in the context of LBS, we argue that having seals like TRUSTe certifying a firm's privacy practices may facilitate individuals' beliefs that they are able to execute proxy control over their personal information.

3.2.3. Proxy Control Through Government Regulation. According to Xu et al. (2010), "government regulation is another commonly used approach that relies on the judicial and legislative branches of a government for protecting personal information (p. 143)." Legal action was taken by the European Commission in the Directive on privacy and electronic communications (2002/58/EC)[2] that explicitly requires location information to be used only with the consent of individuals and only for the duration necessary to provide the specific services. This directive further requires that individuals be provided with simple means to temporarily deny the collection and use of their location information. In the United States, the Location Privacy Act of 2011[3] was drafted to safeguard user location information by requiring any nongovernmental entities to obtain user consent before collecting or distributing the location data. The main focus of this bill is to obtain consent from users

[1] See Direct Marketing Association at http://www.the-dma.org and TRUSTe at http://www.truste.org/ for examples.

[2] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

[3] Location Privacy Protection Act of 2011, S. 1223, 112th Cong. §3 (2011): http://franken.senate.gov/files/docs/Location_Privacy_Protection_Act_of_2011_Bill_Text.pdf.

of mobile devices before their locations are collected and shared with commercial entities or third parties such as advertisers.[4]

With government regulation, individuals can relinquish personal control and instead allow the legislation to exercise proxy control (on their behalf) to protect their personal information. Spiro and Houghteling (1981) indicated that the legal system is the most powerful approach for the execution of proxy control because it requires that offenders be punished in order to maintain its deterrent effectiveness. The legislation can decree the types of personal information companies and third parties are allowed to collect from consumers as well as the ways that collected information should be protected against misuse and breach (Swire 1997). Through enforcement agencies, regulations specify rules and provide redress to individuals who are harmed when the law is violated (Culnan and Bies 2003). Thus we argue that through the government legislation, individuals can exercise proxy control over the collection and use of their personal information by service providers in the context of LBS.

3.2.4. Interaction Effects Between Personal and Proxy Control. Thus far, we have argued that each of the three privacy assurance approaches can potentially alleviate privacy concerns via their effects on the level of perceived control. The direct effects are intuitively appealing and have been indirectly supported in prior research. For example, regarding the direct effect of individual self-protection through PETs, prior research has indicated that having mobile devices with PETs to specify users' privacy preferences makes users feel more in control of their personal information and thus alleviates their privacy concerns pertaining to LBS (e.g., Barkhuus and Dey 2003). For the industry self-regulation approach, empirical evidence has revealed that having third-party privacy seals certifying a firm's privacy practices can increase consumers' control perceptions (e.g., Xu et al. 2008). Under the government regulation approach, research has suggested that the privacy protection standards set by the government allow consumers to believe that companies will protect their disclosed information post-contractually, thereby increasing their perceived control over their personal information (e.g., Tang et al. 2008).

Our focus of this research, however, is not on the direct effects of the three privacy assurance approaches. Rather, we are interested in the extent to which personal control enhancing mechanism interacts with proxy control enhancing mechanism in affecting control perceptions. In addition, because these mechanisms do not appear in isolation in practice, their individual effects are less likely to be ecologically informative than are their interaction effects. Accordingly, we propose a theoretical possibility based on the notion that individuals tend to minimize the amount of effort on information processing and would not process more information than necessary (Berghel 1997, Eppler and Mengis 2004). Therefore, if one of the two control agencies is sufficient to make a relatively risk-free judgment, the existence of other mechanisms may not matter much. To investigate this proposition, we look into the interaction effects of the two control enhancing mechanisms by comparing the sources of control agency for each mechanism.

As discussed above, the differences in the three privacy assurance approaches can be attributed to the differences in control agency (which is either self agency triggering personal control or powerful others agency triggering proxy control). When individuals are placed in control of situations that affect them (i.e., control agency is self), they would often feel greater autonomy (Yamaguchi 2001). For example, in a study about location-based applications, Barkhuus and Dey (2003) found that when users are provided the options to indicate their own settings of how an application should collect their location information, they feel more in control of their interaction with the technology. Cognitively, self agency motivates greater user engagement and involvement, which is likely to result in positive attitudes given its guaranteed consonance with individual interests (Yamaguchi 2001). Empirical evidence has shown that imbuing the user with a sense of personal agency can have a powerful effect on attitudes because of its inherent egocentrism (Sundar and Marathe 2010). Individual self-protection that activates self agency by its very nature is expected to provide users with control of the flow of personal information from their own hands. Thus, compared with proxy agency where control is placed in the hands of other parties, self agency via individual self-protection serves to inculcate a greater sense of agency in users themselves, which could have a stronger impact on their perceived control over personal information. In a particular context of information disclosure, once people disclose their personal information, they have no ability to know what is actually being done with it and no ability to change practices they object to. Therefore, when there is self agency available for individuals to control their personal information, they are likely to have less of a need for proxy control via industry self-regulation or government legislation.

Hypothesis 2 (H2). *The availability of personal control diminishes the effects of proxy control via industry self-regulation.*

[4] See also the Location Privacy Protection Act of 2011 (S. 1223) Bill Summary: http://franken.senate.gov/files/docs/110614_The_Location_Privacy_Protection_Act_of_2011_One_pager.pdf.

Hypothesis 3 (H3). *The availability of personal control diminishes the effects of proxy control via government legislation.*

3.3. Control Variables

Scholars have identified two categories of factors that have a direct bearing on consumers' privacy concerns in a specific context, including (i) individual's personal characteristics and (ii) situational cues that enable a person to assess the consequences of information disclosure (Xu et al. 2008). In this research, we have examined the availabilities of privacy assurance approaches (individual self-protection, industry self-regulation, and government legislation) as salient situational cues that influence individuals' privacy concerns in the specific context of LBS. Factors related to individual characteristics other than those situational cues mentioned previously may influence individuals' reactions to privacy concerns. To control for those unknown effects, we have included interpersonal differences as covariates in the model.

First, we included three *demographic characteristics* (Culnan 1995, Malhotra et al. 2004): *age*, *gender*, and *education*. Demographic differences have been found to influence the degree of general privacy concerns. For example, it was found that those consumers who were less likely to be concerned about privacy were more likely to be young, male, and less educated (Culnan 1995, Sheehan 1999). Although prior research only demonstrated the influences of these demographic variables in affecting *general* privacy concerns, we control for their influences because they could potentially affect the degree of privacy concerns in a specific context of LBS.

Second, *personality traits* have been found to affect *general* privacy concerns in prior research. In this research, the individual personality differences we examine are trust propensity and desire for information control. *Trust propensity* has been defined as "the extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons" (McKnight et al. 2002, p. 339). Trust propensity increases trust belief in a specific context (e.g., toward a service provider; Pavlou and Gefen 2004) and thus may decrease individuals' specific concerns for information privacy (Hui et al. 2007). Therefore, we treat this factor as a control variable in this research. *Desire for information control* reflects individuals' expected control over what organizations do with their information as well as the amount and types of information organizations will collect (Phelps et al. 2000). This variable has been conceptualized as an individual's general tendency to desire information control, which is possessed by all individuals to a greater or lesser degree (Phelps et al. 2000). Research suggests that consumers who desire greater control over personal information were much more likely to have higher privacy concerns than were consumers who desire less control over personal information (Phelps et al. 2000). Although prior research only demonstrated the influence of desire for information control in influencing general privacy concerns, we control for its influence because it could potentially influence the degree of privacy concerns in a specific context.

Third, we include interpersonal difference in terms of *previous privacy experience* as a covariate in the model. Individuals who have been exposed to or been the victim of personal information abuses are found to have stronger concerns for information privacy in general (Smith et al. 1996). We argue that although prior research only demonstrated the influence of previous privacy experience in affecting general privacy concerns, we control for its influence because it may potentially affect the degree of privacy concerns in a specific context.

4. Research Method

4.1. Experimental Design and Manipulation

An experimental study was conducted to test the research hypotheses. Three privacy assurance approaches were manipulated independently, and their effects on individuals' psychological responses were examined. A location tracking service (location-aware mobile-coupon service) was utilized because LBS providers with this type of application tend to be more aggressive in promoting their services through active tracking of user location information, thereby resulting in greater privacy concerns among users (Barkhuus and Dey 2003).

The experiment had a $2 \times 2 \times 2$ factorial design. Eight experimental scenarios were created by manipulating the presence and absence of three privacy assurance approaches (individual self-protection, industry self-regulation, and government legislation). *Individual self-protection* (*ISP*) was manipulated by providing technological self-protection features, i.e., privacy control functions in mobile devices (see Appendix C, which is available as part of the online version that can be found at http://dx.doi.org/10.1287/isre.1120.0416). Based on Barkhuus and Dey (2003), we manipulated individual self-protection by providing subjects with an interactive graphical interface of a mobile device that allows them to restrict their location information released to the LBS provider. Because TRUSTe is widely adopted and the seal is applicable for the wireless industry, *industry self-regulation* (*REG*) was manipulated by showing subjects a TRUSTe seal with a URL link to the privacy policy of the LBS providers (see Appendix D1). A brief introduction explaining the

mission of TRUSTe was also given to the subjects to make sure they understood the significance of the TRUSTe seal (see Appendix D2). We manipulated *government legislation* (*LEG*) by telling the subjects that the use of LBS was governed by a newly enacted location privacy law which covered the collection and use of their personal information. Subjects were also presented with a piece of news related to the recent enactment of the location privacy law (see Appendix E).

4.2. Operationalization of Variables and Pilot Study

Context-Specific Concerns for Information Privacy (*CFIP*): We adapted the scale of *CFIP* developed by Smith et al. (1996) to measure privacy concerns pertaining to LBS. It has been demonstrated in the privacy literature (e.g., Angst and Agarwal 2009, Stewart and Segars 2002) that *CFIP* was better modeled as a *reflective* second-order factor.[5] When adapting *CFIP* into the Internet context to develop the scale of IUIPC, Malhotra et al. (2004) theorized and operationalized IUIPC using a reflective second-order factor. Given the strong theoretical and empirical evidence, we conceptualized *CFIP* as a reflective second-order factor comprising four first-order components: *collection of personal information*, *unauthorized secondary use of personal information*, *errors in personal information*, and *improper access to personal information*. Changes were made to the instrument of *CFIP* to reflect privacy concerns specific toward the LBS by replacing the word *companies* to *the company*, referred to as the specific service provider of LBS.

Perceived Control over Personal Information (*CTL*) was measured using five reflective indicators.[6] Prior privacy literature (Goodwin 1991, Hoffman et al. 1999, Phelps et al. 2000, Spiekermann and Cranor 2009) noted that control over personal information may be governed by two larger dimensions: (1) *control over information release* at the *frontend* where personal data flow in and out of users and (2) *control over unwanted access and use of personal information* at the *backend* where personal data are processed, stored, and transferred across different data sharing networks and infrastructure. We adapted the items measuring perceived control in the context of health psychology (Reed et al. 1993) to focus on perceived control over *personal information* in the context of privacy. We integrated elements related to the measures of perceived control over information release and over unwanted access and use.

Control Variables. To the extent possible, scales for the control variables were adapted from prior studies to fit the context of this research. *Desire for information control* was assessed with three indicators that were taken from Phelps et al. (2000). The measurement items focus on an individual's expected control over what companies do with their information as well as the amount and types of information companies will collect (Phelps et al. 2000). *Privacy experience* was measured with three questions adapted from Smith et al. (1996), and *trust propensity* was measured with three questions taken from McKnight et al. (2002). See Appendix A for the operationalization details.

The initial set of items was reviewed by six information systems faculty members and doctoral students and modestly modified as a result of the feedback. Next, we conducted a pilot study involving 86 graduate and undergraduate students to assess the strength of the manipulations, gauge the clarity of the questions, and verify the clarity and conciseness of the experimental procedure and instructions. The participants provided detailed feedback through interviews. Based on this feedback, we clarified and streamlined the experimental instructions, reorganized the instrument layout, and reworded some items.

4.3. Procedure and Task

At the start of each experimental session, the subjects were told that all instructions were available online and that they should read the instructions carefully and complete the experiment independently. After logging into the Web-based experimental system, the subjects answered a pre-session questionnaire that collected personal information for control checks. Next, we provided a cover story to all subjects (see Appendix B). They were told that Company A would soon be introducing an LBS application (location-aware mobile-coupon service) in the market and that their feedback was being solicited to evaluate this service. General information about the service provider and the service was also provided to the subjects. The experimental system tracked the browsing history of the subjects to ensure that all the pertinent experimental materials were read.

Next, the Web-based experiment system randomly generated an experimental scenario such that each subject had an equal and independent chance of being assigned to any of the eight experimental

[5] Slyke et al. (2006) was the exceptional case in which CFIP was modeled as a formative second-order factor. We conducted robustness test by re-running the PLS analyses with CFIP as a formative factor. Some path coefficients in this new model were slightly different from our current model in which CFIP was modeled as a reflective factor. But there was no significant change in terms of the overall pattern of results.

[6] Similarly to the case of CFIP, we conducted robustness tests by re-running the PLS analyses with CTL as a formative factor. Some path coefficients in this new model were slightly different from our current model in which CTL was modeled as a reflective factor. But there was no significant change in terms of the overall pattern of results.

treatments. Subjects assigned to treatments involving individual self-protection were provided with the interactive graphical interface of privacy enhancing features (see Appendix C). Subjects assigned to treatments involving industry self-regulation were shown the TRUSTe seal and the URL link to the privacy policy (see Appendix D1 and D2). Finally, subjects assigned to treatments involving government legislation were given the privacy protection laws and a piece of enforcement news (see Appendix E). The order for presenting these treatments was randomized by our online experiment system. To conclude the experiment, the subjects answered a post-session questionnaire that contained the questions measuring perceived control, context-specific concerns for information privacy, and other information for manipulation checks. Subject responses to the meaningfulness of the task (see Appendix A for questions used for task validity check) were significantly higher than the neutral value.

4.4. Participants

We recruited participants by posting announcements on the major Web portals in Singapore. The posting provided some background about the researchers and the study without revealing the experimental treatments and invited forum participants to complete this study. Those who chose to participate could easily do so by clicking on the URL provided in the posting, which would take them into the experimental system. This recruitment procedure yielded a total of 198 subjects. To motivate participants to complete this study, a lottery with four prizes[7] (a mobile phone, an MP3 player, a Bluetooth headset, and a cash prize) was offered. The strategy of rewarding subjects through raffle prizes in exchange for divulging personal attitudes or behaviors is well applied in the survey methodology (e.g., Pavlou et al. 2007, Wang and Benbasat 2009). Among the respondents, 54% were males and 46% were females; 57% respondents reported that they had no experience with using LBS for the past six months whereas 43% reported that they has some usage experience. Specific demographic information is shown in Appendix F.

Our sampling approach lacks the report on the number of individuals who have seen the request for participation, which is different from the traditional survey sampling approach where a response rate is calculated and reported to compare the demographics of the sample against those of the population. To address this sampling concern, we compared the demographic characteristics of our respondents with the general demographic characteristics of the whole Singaporean mobile phone users reported by *Singapore Statistics*[8] and the annual survey by *Infocomm Development Authority (iDA)*.[9] The respondents did not differ from a nationally representative sample in terms of gender ratio, age, mobile phone usage, and Internet and online shopping experience. Nonresponse bias (Armstrong and Overton 1977) was also assessed by verifying that (1) the respondents' demographics are consistent with current mobile phone users in Singapore and (2) that early and late respondents were not significantly different. Early respondents were those who responded within the first week (48%). The two groups of early and late respondents were compared based on their demographics (age, gender, education, income, and mobile application usage experience); perceived control; privacy concerns; desire for information control; trust propensity; and privacy experience. All t-test comparisons between the means of the two groups showed insignificant differences. Thus, we believe that the demographics of our participants who clicked on the link to our experiment are roughly consistent with those of the general mobile phone users in Singapore.

5. Data Analyses and Results

5.1. Manipulation and Control Checks

Experimental manipulations were checked by three steps. First, JavaScript programming was used to log the time each subject spent on the treatment page in order to verify that subjects had browsed the materials pertaining to their respective treatments. Data from 12 subjects were dropped because these subjects spent fewer than 10 seconds reading the manipulation materials. Second, experimental manipulations were checked using yes/no questions for the existence or absence of the privacy assurance approaches in order to confirm their awareness of the assurances. Data from eight subjects were dropped because they failed to correctly respond to the manipulation check questions. Third, we included the perceptual questions to test the effectiveness of the manipulations. Paired-sample T-tests show that all treatments were manipulated effectively. Specifically, participants in *present* ISP treatment group believed that they can better control when the service provider can track and communicate with their mobile devices than the participants in *absent* ISP treatment did ($t = 9.92$, $p < 0.001$). Participants in *present* REG treatment group believed that the service provider was less likely to violate their privacy and could protect their data better

[7] We believe that the amount of raffled prizes offered in this study is appropriate. The amount of our highest prize (around US$85) is lower than that (US$100) offered in Pavlou et al. (2007).

[8] http://www.singstat.gov.sg/keystats/annual/indicators.html.

[9] http://www.ida.gov.sg/Publications/20061205092557.aspx.

than the participants in *absent* REG treatment did ($t = 12.65, p < 0.001$). Participants in *present* LEG treatment group believed that relevant legislation could better govern the protection of their private information than the participants in *absent* LEG treatment did ($t = 16.62, p < 0.001$). These three-step manipulation checks resulted in a data set of 178 usable and valid responses.

In addition, Mann-Whitney tests showed that gender ratio and education level of subjects did not differ significantly across the various treatments. ANOVA tests revealed that subjects assigned to the various treatments did not differ significantly in terms of their age, income, mobile device usage experience, desire for information control, trust propensity, and privacy experience. Hence, the random assignment of subjects to the various treatments appeared to be effective.

5.2. Measurement Validation

A second-generation causal modeling statistical technique—partial least squares (PLS)—was used for data analysis. We evaluated the measurement model by examining the convergent validity and discriminant validity of the research instrument. Convergent validity is the degree to which different attempts to measure the same construct agree (Cook and Campbell 1979). In PLS, three tests are used to determine the convergent validity of measured reflective constructs in a single instrument: reliability of items, composite reliability of constructs, and average variance extracted by constructs. We assessed item reliability by examining the loading of each item on the construct and found that the loadings for all the items exceeded 0.65 (see Appendix G), indicating adequate reliability (Falk and Miller 1992). Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7. The average variances extracted for the constructs were all above 0.5, and the Cronbach's alphas were also all higher than 0.7. As can be seen from the confirmatory factor analysis (CFA) results in Appendix G[10] and the reliability scores in Table 2, these results support the convergent validity of the measurement model.

For the construct of *CFIP*, it is modeled as a second-order variable, reflecting four first-order factors, namely *collection*, *unauthorized access*, *error*, and *secondary use*. According to Wetzels et al. (2009), there are two approaches to estimate models with second-order factors in PLS path modeling: the repeated use of manifest indicators approach (Wetzels et al. 2009) and the latent variable score approach (Chin 1998). In this research, we adopted the latter approach to measure the second-order construct of *CFIP* using summated scales, which were represented by factor scores derived from the confirmatory factor analysis (Agarwal and Karahanna 2000).

Discriminant validity is the degree to which measures of different constructs are distinct (Campbell and Fiske 1959). To test discriminant validity (Chin 1998): (1) indicators should load more strongly on their corresponding construct than on other constructs in the model, and (2) the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model. As shown in Appendix G, all factor loadings are higher than cross-loadings. Furthermore, as shown by comparing the diagonal to the nondiagonal elements in Table 2, all constructs share more variance with their indicators than with other constructs. Therefore, all items fulfilled the requirement of discriminant validity.

Finally, although common method bias might not be a major concern when measures of independent and dependent variables are obtained from different sources (Podsakoff et al. 2003) in an experimental study, we incorporated the considerations of addressing this concern in our research. First, in the research and instrument design, to control acquiescence bias, we used bipolar scales and provided verbal labels for the midpoints of scales. Based on the feedback from pilot tests, we provided examples for those terms or concepts with which subjects may be unfamiliar. Second, following Podsakoff et al. (2003), we ran Harman's single-factor test to test for common method variance. If common method variance were a serious problem in the study, we would expect a single factor to emerge from a factor analysis or one general factor to account for most of the covariance among measures (Podsakoff et al. 2003). We performed an exploratory factor analysis by loading all items on a single factor. No general factor was apparent in the unrotated factor structure, with Factor 1 accounting for 22% of the variance, indicating that common method variance is unlikely to be a serious problem in the data. Third, we ran Lindell and Whitney's (2001) test that uses a theoretically unrelated construct (termed a marker variable), which was used to adjust the correlations among the principal constructs (Malhotra et al. 2006, Son and Kim 2008). We assessed correlation between the marker variable and our research constructs because they were assumed to have no relationships. The results indicated that the average correlation coefficient was close

[10] To perform CFA in PLS, the following procedure was suggested by Chin (1998) and applied in Agarwal and Karahanna (2000): The loadings for the construct's own indicators were provided by PLS. To calculate cross-loadings, a factor score for each construct was calculated based on the weighted sum of the construct's indicators. Then these factor scores were correlated with all other indicators to calculate cross-loadings of other indicators on the construct.

Table 2 Construct Correlation Matrix

	CTL	*COL*	*AC*	*ER*	*USE*	*DIC*	*EXP*	*TRU*	*AGE*	*SEX*	*ED*	*ISP*	*REG*	*LEG*	*ISP* × *LEG*	*ISP* × *REG*
CTL	0.89															
COL	−0.41	0.88														
AC	−0.56	0.76	0.93													
ER	−0.38	0.57	0.70	0.94												
USE	−0.59	0.69	0.88	0.63	0.96											
DIC	0.05	0.13	0.10	0.08	0.08	0.94										
EXP	−0.04	0.24	0.19	0.17	0.21	0.19	0.84									
TRU	0.12	−0.09	−0.14	−0.12	−0.15	0.14	0.03	0.79								
AGE	−0.16	0.10	0.08	0.10	0.14	0.03	0.14	0.01	1.00							
SEX	0.17	0.03	0.07	0.09	0.11	0.04	−0.02	0.12	−0.14	1.00						
ED	−0.05	0.07	0.03	0.08	0.01	0.02	0.05	0.05	0.25	−0.20	1.00					
ISP	0.20	−0.13	−0.08	−0.02	−0.08	−0.01	−0.12	0.07	−0.12	0.02	0.07	1.00				
REG	0.39	−0.15	−0.17	−0.15	−0.19	0.11	−0.03	0.05	−0.09	0.07	−0.08	−0.01	1.00			
LEG	0.32	−0.01	−0.13	−0.01	−0.20	−0.10	0.11	0.05	−0.05	0.07	−0.03	−0.01	−0.01	1.00		
ISP × *LEG*	−0.20	0.08	0.09	0.08	0.15	−0.03	−0.11	0.04	0.04	−0.08	0.15	0.01	−0.02	−0.01	1.00	
ISP × *REG*	−0.04	0.05	0.04	0.15	0.10	−0.13	−0.15	0.02	0.06	−0.12	−0.03	0.01	−0.01	−0.02	−0.01	1.00

Notes. *CTL* = *perceived control*, *COL* = *Collection*, *AC* = *Unauthorized Access*, *ER* = *Error*, *USE* = *Secondary Use*, *DIC* = *Desire for Info Control*, *EXP* = *Privacy Experience*, *TRU* = *Trust propensity*, *AGE* = *Age*, *SEX* = *Gender*, *ED* = *Education level*, *ISP* = *Individual Self-protection*, *REG* = *Industry Self-regulation*, *LEG* = *Government Legislation*. Value on the diagonal is the square root of average variance extracted (AVE).

to zero ($r = 0.02$, n.s.).[11] Thus, it seems reasonable to argue that this present study is relatively robust against common method biases.

5.3. Testing the Structural Model

After establishing the validity of the measures, we conducted the PLS analysis to test the hypotheses. Because PLS does not generate any overall goodness of fit indices, predictive validity is assessed primarily through an examination of the explanatory power and significance of the hypothesized paths. The explanatory power of the structural model is assessed based on the amount of variance explained in the endogenous construct (i.e., context-specific concerns for information privacy).

Table 3 depicts the structural models. We estimated four models. Model 1 is the full model with interaction effects, whereas Model 2 is a model with only main effects. Model 3 includes only the theoretical variables (excluding control variables) as predictors. Model 4 is a controls-only model that provides a benchmark for assessing the additional impacts of the theoretical variables. An examination of the results for the full model (Model 1) reveals that the path coefficient expressing the effect of perceived control on *CFIP* is −0.60 and highly significant ($t = 9.92$). Hypothesis H1 is thus supported: when perceived control over personal information increases, *CFIP* decreases. A comparison of Models 1 and 4 shows that the full model explains a substantive incremental variance of 30.3% (40.7% − 10.4%). In contrast, including the control variables on top of the independent variables only explains an additional 5.3% (40.7% − 35.4%) of the variance, as shown by a comparison of Models 1 and 3. These results suggest that our theoretical model is substantive enough to explain a large proportion of the variance in context-specific concerns for information privacy.

[11] We measured the marker variable of *fashion leadership* based on those items (see Appendix A) from Goldsmith et al. (1993).

Table 3 Path Coefficients for Structural Model

Effect	Model 1 interaction model	Model 2 main effects model	Model 3 theoretical constructs	Model 4 control constructs
Perceived Control (*CTL*)				
Individual self-protection (*ISP*)	0.21**	0.22**	0.21**	
Industry self-regulation (*REG*)	0.39**	0.37**	0.39**	
Government legislation (*LEG*)	0.32**	0.34**	0.32**	
ISP × *LEG*	−0.19*		−0.19*	
ISP × *REG*	−0.04		−0.04	
R^2 (%)	**33.5**	**29.5**	**33.5**	
Context-Specific Concerns for Information Privacy (*CFIP*)				
Perceived control	−0.60**	−0.60**	−0.60**	
Age	0.01	0.01		0.09
Gender	0.02	0.01		0.04
Education level	0.01	0.01		0.04
Desire for information control	0.08	0.08		0.10
Trust propensity	−0.04	−0.04		−0.13
Privacy experience	0.16*	0.15*		0.21*
R^2 (%)	**40.7**	**40.0**	**35.4**	**10.4**

*$p < 0.05$, **$p < 0.01$.

5.3.1. Interaction Test. We hypothesized the interaction effects between personal control agency and proxy control agency (H2 and H3), which were tested using PLS (see Model 1 of Table 3). As H3 predicted, there was a significant interaction between *individual self-protection* and *government legislation* ($b = -0.19, p < 0.05, \Delta R^2 = 4\%$). But the interaction between *individual self-protection* and *industry self-regulation* (H2) was not significant (see Model 1 of Table 2). The test for the significant interaction effect was conducted by following Carte and Russell (2003), to examine whether the variance explained because of the interaction effect is significant beyond the main effects, using the F-statistic $\{ = [\Delta R^2/(\mathrm{df}_{\mathrm{interaction}} - \mathrm{df}_{\mathrm{main}})]/[(1 - R^2_{\mathrm{interaction}})/(N - \mathrm{df}_{\mathrm{interaction}} - 1)]\}$. The F-statistic was $F(2,172) = 5.17$ ($p < 0.01$), thereby supporting the significant interaction effect between *individual self-protection* and *government legislation*.

To further validate the interaction effect between *individual self-protection* and *government legislation*, we followed the Chin et al. approach (2003) that was adopted in Im and Rai (2008) to perform the test comparing the R^2 values between the main and interaction effects by using Cohen's f^2 $[= (R^2_{\mathrm{interaction}} - R^2_{\mathrm{main}})/(1 - R^2_{\mathrm{main}})]$. Controlling for the study's control variables, the variance explained on *perceived control* was 33.5% when accounting for the interaction effect, whereas only 29.5% was explained with only the main effects. The interaction constructs have the effect size f^2 of 0.06, which is between a small and medium effect (Chin et al. 2003), thus confirming H3.

5.3.2. Mediation Test. In our theoretical model, we posited that *perceived control* would mediate the relationship between privacy assurance approaches and *CFIP*. To test for this mediation, we followed Nicolaou and McKnight's approach (2006) to conduct two related techniques. First, power analysis may provide information about the significance of omitted paths in a reduced model (Cohen 1988). We restricted the research model to include only the paths from privacy assurance approaches (*ISP*, *REG*, and *LEG*) to *context-specific privacy concerns*. We found all three privacy assurance approaches have direct positive effects on *CFIP* (see Figure 2(a)). However, the percentage of variance explained for *context-specific privacy concerns* decreased from 35.4% (see Model 3 of Table 2) to 18.6% (see Figure 2(a)). Chin (1998) recommends the calculation of an effect size because of the omission of paths from the model: The effect size when the perceived control path is omitted equals 0.26, which is between a medium and large effect. This shows that *perceived control* has an important effect on *CFIP* and that researchers should not exclude it from the model.

Second, Baron and Kenny (1986) suggested that mediation is demonstrated if three conditions are fulfilled: the first condition stipulates that the independent variable must significantly affect the proposed mediator. As the Table 3 shows, the relationships between the proposed mediator (*perceived control*) and the three independent variables (*ISP*, *REG*, and *LEG*) were significant. The second condition requires the independent variable must significantly affect the dependent variable. The PLS results (see Figure 2(a)) demonstrated that the three independent variables (*ISP*, *REG*, and *LEG*) were significantly related to the dependent variable (*CFIP*). The last condition stipulates that the relationship between the independent variable and the dependent variable should be weaker or insignificant when the proposed mediator is included than when the proposed mediator is not included. The results (see Figure 2(b)) indicated that the path coefficient for *individual self-protection* ($b = -0.07$) and the path coefficient for *government legislation* ($b = -0.09$) were not significant when *perceived control* was included in the model; the path coefficient for *industry self-regulation* ($b = -0.32$ compared with $b = -0.19$) was lower when *perceived control* was included in the model. Figures 2(a) and 2(b) summarize the results for testing the mediating effect of *perceived control*, which satisfied the conditions needed to establish mediation by Baron and Kenny (1986).

Sobel (1982) tests were also conducted as a means of further examining evidence for mediation above and beyond procedures recommended by Baron and Kenny (1986). This test is designed to assess whether a mediating variable significantly carries the influence of an independent variable to a dependent variable, i.e., whether the indirect effect of the independent variable on the dependent variable through the mediator variable is significant. Results of Sobel tests supported the mediating effects of perceived control for (i) the relationship between *ISP* and *CFIP*

Figure 2(a) PLS Model Without Perceived Control

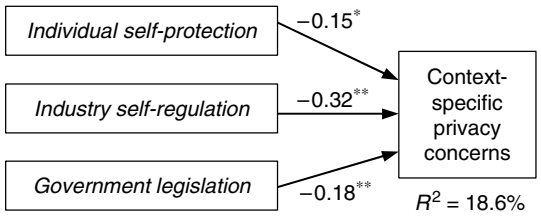
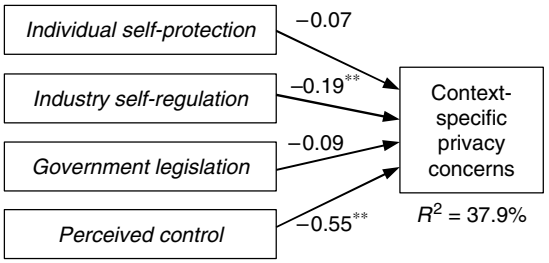


Figure 2(b) PLS Model with Perceived Control



Note. $^*p < 0.05$, $^{**}p < 0.01$.

($z = 2.96, p < 0.01$), (ii) the relationship between *REG* and *CFIP* ($z = 4.34, p < 0.01$), and (iii) the relationship between *LEG* and *CFIP* ($z = 3.33, p < 0.01$). Thus, all of the statistical tests supported *perceived control* as mediating the relationships between privacy assurance approaches (*ISP*, *REG*, and *LEG*) and *CFIP*.

6. Discussions and Implications

6.1. Discussions of Findings

This study seeks to clarify the nature of control in the context of information privacy to generate insights into the effects of different privacy assurance approaches on context-specific concerns for information privacy. We theorized that such effects are exhibited through mediation by perceived control over personal information and developed arguments in support of the interactive effects involving different privacy assurance approaches. In general, the results support our core assertion that perceived control over personal information is a key factor affecting context-specific concerns for information privacy. We extend the literature by investigating the interaction among privacy assurance approaches that provide individuals with personal control or proxy control.

By exploring the interaction effects of three privacy assurance approaches, this study takes the privacy discourse beyond a general discussion of privacy concerns. It generates insights into how the context-specific privacy concerns of individuals can be alleviated by raising their perceived control over the collection and use of their personal information in a specific context. Given the debate among scholars and practitioners on the relative effectiveness of these three (and other) approaches for reducing privacy concerns (Culnan and Bies 2003), these insights can serve as a theoretical basis for further efforts to generate insights on this topic. Beyond confirming prior findings that these three privacy assurance approaches have a direct effect on enhancing control perceptions (thereby alleviating privacy concerns) in a specific context, this study focuses on the interactions among these approaches. Specifically, two interactions are proposed and one is supported (involving individual self-protection and government legislation). Results show that the presence of individual self-protection offering personal control diminishes the impact of government legislation offering proxy control, but it does not diminish the impact of proxy control via industry self-regulation (as hypothesized).

One plausible explanation for this insignificant interaction is that individuals may perceive that the industry self-regulators are generally lacking enforcement authority. Hence individuals may not regard industry self-regulators (such as TRUSTe) as powerful others that can exercise proxy control for them. Prior studies have demonstrated weak effects of industry self-regulations on addressing consumer privacy concerns (Hui et al. 2007, Moores 2005, Moores and Dhillon 2003). In fact, Edelman (2011) recently pointed out that some industry self-regulators such as privacy certification authorities have failed to pursue complaints against major companies whose privacy breaches were found to be "inadvertent." Therefore, in the event that individuals' personal information has been misused, they may not have an effective means to seek redress because there is reasonable basis to question the enforcement power of industry self-regulators to ensure merchants act according to their privacy policies.

To obtain further insight into the interaction that is contrary to the prediction, we conducted a post hoc analysis using ANOVA. The ANOVA results (see Appendix H) confirmed the interaction pattern demonstrated in PLS: there was a significant interaction between *individual self-protection* and *government legislation* ($F = 4.34, p < 0.05$), but the interaction between individual self-protection and industry self-regulation was not significant ($F = 0.60, p = 0.44$). However, the ANOVA results also revealed an unexpected significant interaction between industry self-regulation and government legislation ($F = 4.73, p < 0.05$). After plotting the significant interaction effects with *t*-tests, we found substitution effects from these two significant interaction effects: one between *individual self-protection* and *government legislation* (*ISP* × *LEG*) and the other between industry self-regulation and government legislation (*REG* × *LEG*). As shown in Appendix H, the first interaction effect shows that the difference between the two *ISP* conditions in the *no LEG* condition is significant, whereas this difference is not significant in the *LEG* condition. Similarly, the difference between the two *LEG* conditions is significant in the *no ISP* condition, whereas this difference is not significant in the *ISP* condition. These results suggest that for the two types of control assurance, i.e., personal control via *ISP* and proxy control via *LEG*, one could substitute for the other to some extent.

Along with the aforementioned interaction effect between *individual self-protection* and *government legislation* (*ISP* × *LEG*), the relationship between industry self-regulation and government legislation (*REG* × *LEG*) shares a similar interaction pattern. The results show that the difference between the two *REG* conditions in the *no LEG* condition is significant, whereas this difference is not significant in the *LEG* condition. Similarly, the difference between the two *LEG* conditions is significant in the *no REG* condition, whereas this difference is not significant in the *REG* condition. These results suggest that for the two regulatory approaches (i.e., *industry self-regulation* and *government legislation*), one could substitute for the other to some extent.

Looking at the entire set of significant interactions, it seems that individuals understand individual self-protection and industry self-regulation in a similar fashion (even though the intent of this privacy assurance mechanism may have been to offer proxy control). If this is the case, it would explain the results showing that *industry self-regulation* interacts with *government legislation* but not with *individual self-protection*. One possible explanation for this result could be because of the weak enforcement power of industry self-regulators. Individuals may perceive that they do not have an effective means to seek redress from the industry self-regulators when their personal information has been misused. Thus, as in the case of individual self-protection, individuals have to exercise careful discretion on what personal information to provide when industry self-regulation is present. It seems that the use of individual self-protection or industry self-regulation shifts much of the onus of protecting personal information to individuals themselves. This may explain why individuals did not regard industry self-regulators as powerful others that can exercise proxy control for them.

Because the correlation matrix (in Table 2) showed substantially different correlation values between perceived control and the first-order factors of *CFIP* (*collection*, *unauthorized access*, *error*, and *secondary use*), we conducted a post hoc analysis to see how *perceived control* impacts each first-order factor of *CFIP* (see Appendix I). Results showed that *perceived control* played a significant role in alleviating privacy concerns related to all four aspects. Among the relationships between *perceived control* and the four first-order factors of CFIP, *perceived control* was more influential in addressing concerns for *secondary use* ($b = -0.61$) and *unauthorized access* ($b = -0.57$) than it was for *collection* ($b = -0.41$) and *error* ($b = -0.39$). These observations made about the variations across the four first-order factors suggest that there is value in investigating these four first-order factors of *CFIP* in future research at a more fine-grained level. From the practical perspective, LBS practitioners should pay more attention to develop and deploy privacy control mechanisms that can limit secondary use of personal information and unauthorized access to personal information.

Examining control variables in the structural models also offers some insights. Among three types of personal characteristics (*demographic differences*, *personality traits*, and *previous privacy experience*), only *previous privacy experience* was found to have a significant effect on privacy concerns. This implies that those who have encountered negative privacy experiences are more aware of undesirable consequences of disclosing personal information in the LBS context based on previous experience. Interestingly, most of the items in our list of personal characteristics (demographic differences and personality traits such as desire for information control and trust propensity) were shown to have insignificant influences on privacy concerns in the specific context of LBS. Although these variables were found to be significant when included as the predictors of *general* privacy concerns in prior research, their effects were shown to be overridden by context-specific factors that tie the assessment of privacy concerns to specific services in this research. This is consistent with the proposition of *privacy paradox* (Acquisti and Grossklags 2005) that individuals' stated levels of general privacy concerns often deviate from or are even contradictory to their actual privacy assessment in a specific context. As Berendt et al. (2005) demonstrated through an experimental study, individuals could easily forget their stated general privacy concerns and disclose very personal details when interacting with an entertaining website. Accordingly, we suggest that future privacy research should not only examine privacy concerns at a general level but also consider situational elements and contextual differences at a specific level.

6.2. Limitations and Future Research

There are several limitations in this study that present useful opportunities for further research. First, we conducted the study in Singapore, which has a strong reputation for enforcing government legislation (Harding 2001). Thus, the subjects may have well-formed and powerful beliefs about proxy control through government legislation. In countries where such government legislation is generally lacking or where enforcement of government legislation is limited, individuals may have a weaker preference for proxy control through government legislation. As Smith (2004) pointed out, different countries have approached privacy issues differently in various regulatory structures (with "omnibus" privacy bills or a "patchwork" of sector-specific laws). Therefore, future research should be conducted in other countries to provide further insights into the effects of privacy assurance approaches.

Second, we have employed a manipulation of privacy-enhancing technology as one type of individual self-protection approaches, which is commonly used in the practice of LBS. Future research can investigate whether nontechnological self-protection approaches (e.g., reading privacy policy, refusal, misrepresentation, removal, negative word-of-mouth, complaining directly to online companies, and complaining indirectly to third-party organizations; Son and Kim 2008) would yield the same impact as the privacy-enhancing technology in terms of raising perceived control over personal information.

Third, we have included a number of individual differences as control variables in this study. Future research can examine whether such differences moderate the relationship between the three privacy assurance approaches and perceived control over personal information. In addition, the role of personal disposition has been an important factor in behavioral models, such as those related to trust and the effect of personal disposition to trust on trusting behavior (e.g., McKnight et al. 2002). In light of positioning privacy concerns as context specific beliefs, it might be worthwhile to examine how disposition to value privacy (Xu et al. 2008) would impact context-specific privacy concerns. Fourth, and by design, this research is limited to the examination of the mediation role of perceived control between privacy assurance approaches and context-specific privacy concerns as well as the interaction effects involving different privacy assurance approaches. Therefore, we have not extended the nomological network to consider how those context-specific privacy concerns are translated into privacy-related intentions and behaviors. An extension of this study can view context-specific privacy concerns as a mediating variable in a larger nomological network, with it leading to privacy-related behaviors.

In addition, the respondents for this study were recruited from major Web portals in Singapore. Such a sampling approach lacks the report on the number of individuals who have seen the request for participation, which is different from the traditional survey sampling approach where a response rate is calculated and reported to compare the demographics of the sample against those of the population. Care must be taken in any effort to generalize our findings beyond the boundary of our sample. Lastly, the research model has been developed and tested in a specific context of LBS. An implication for future research is to extend the theoretical framework described in this research to other contexts that may raise similar or extended privacy issues. For example, there has been much discussed in the public media about privacy-related backlashes among social networking sites (e.g., Brandimarte et al. 2010, Wang et al. 2011). It would be interesting to test the theoretical framework developed here in the context of online social interactions to assess its applicability.

6.3. Theoretical Contributions

This study aims to contribute to existing privacy research in several ways. First, our primary contribution is to clarify the link between control and privacy in the context of LBS. Although the notion of control is embedded in many privacy definitions and has been used to operationalize privacy in instruments, its meaning has been ambiguous. In this research, we establish the mediating role of perceived control in mitigating privacy concerns in the context of LBS. Such separation of control from privacy concerns is important because it enables us to avoid conflating the concept of privacy with the concept of control.

Second, our proposed model has established the importance of a psychological perspective of control in alleviating privacy concerns. Specifically, we integrated the control agency theory into the research model and examined the efficacy of three privacy assurance approaches (individual self-protection, industry self-regulation, and government regulation) in influencing privacy concerns through the mediating effect of perceived control in the context of LBS. This represents one of the few studies that theoretically differentiate three privacy assurance approaches by linking them with different types of control agencies. Most importantly, although the privacy literature has exclusively examined the individual effect of privacy assurance approaches (e.g., Metzger 2006), this study extends the literature by proposing interaction effects of these mechanisms on alleviating privacy concerns, based on the type of control agencies they can provide. This extension is particularly relevant in today's world, which has a diversity of privacy assurance approaches. Particularly, this study derives theory-driven privacy interventions as well as provides early empirical evidence showing that implementing more privacy assurance approaches does not necessarily lead to higher control perceptions.

Third, to respond to the compelling call for research investigating the role of technologies in influencing the privacy theoretical development (Waldo et al. 2007), we viewed the technological advancement as a double-edged sword in this research: on the one hand, location-based technologies make the privacy challenge particularly vexing; on the other hand, privacy protections could be implemented through privacy-enhancing technologies (PETs). Although the negative side of technological advancement has long been highlighted as the main driver of privacy concerns in various contexts (e.g., Internet, data mining, and profiling), the positive side regarding the role of PETs has not been fully addressed in the IS field. With the active rolling out of PETs by the technologists (e.g., Squicciarini et al. 2011), it would be important for IS researchers to include the PETs in the examination of individual self-protection approaches in the privacy research.

6.4. Practical Implications

The findings of this study have useful implications for LBS providers and individuals as well as regulatory bodies and LBS technology developers. To the extent that perceived control is a key factor influencing privacy concerns pertaining to LBS, measures that can increase users' perceived control over the collection

and use of their personal information should help individuals' privacy concerns pertaining to LBS.

Although the presence of three privacy assurance approaches has an overall effect, this study suggests that, for the two regulatory approaches of privacy assurance (i.e., industry self-regulation and government legislation), implementing one of them seems adequate to install consumers' confidence in controlling their personal information in LBS. This finding sheds some light on the conflicts between the different approaches of the United States and European Union to regulating privacy—the self-regulatory approach versus the comprehensive legislative approach. In the United States, self-regulation, particularly in the context of e-commerce and online social networks, is used as a means to preempt the need for legislation, which can be more constraining to industry participants. On the opposite side of the spectrum, the European Union takes a stronger approach that relies on government enforcement of mandatory legal rules to ensure adequate privacy protection of personal information. Our finding adds to the self-regulation versus legislation debate by suggesting that having a high degree of self-regulation nullifies the need for legislation, whereas having a high degree of legislation nullifies the need for self-regulation. In addition, this study suggests that for the legislative approach of privacy assurance and the individual self-protection approach, one could substitute for the other to some extent. Because government legislation is usually more expensive to institute and only exists within a legal jurisdiction (Pavlou and Gefen 2004), promoting the individual self-protection approach should be increasingly perceived as a viable substitute for government legislation approach because of its ability to cross international, regulatory, and business boundaries.

Results of this study lead to the recommendation that for situations where regulatory bodies are not willing to enact legislation to protect the privacy of personal information or cannot enforce the legislation when violations occur, the effects of individual self-protection and industry self-regulation are likely to be pronounced. Therefore, LBS technology developers can benefit from the promotion of the individual self-protection approaches (especially through PETs) and LBS providers can increase their business by promoting industry self-regulation with a trusted third party. Without government legislation in place, it is valuable to provide individuals with individual self-protection and industry self-regulation. For example, as a startup company in the LBS industry, Loopt.com[12] has promoted its services by emphasizing its privacy-enhancing features, its TRUSTe membership, and its relationship with industry regulators to establish accepted standards of privacy protection (e.g., Center for Democracy and Technology and the Ponemon Institute). Considering that there has yet to be any international consensus on suitable legal frameworks for privacy practices, it is unrealistic to expect the privacy laws to be carried out globally. Therefore, a hybrid mechanism combining individual self-protection and industry self-regulation can effectively provide individuals with control over the collection and use of their personal information. Such a hybrid mechanism may become increasingly prevalent globally.

[12] Altman, S. "Best Practices for Location-based Services: Privacy, User Control, Carrier Relations, Advertising, and More," *Where 2.0 Conference*, Burlingame, CA, May 12–14, 2008. Available at http://en.oreilly.com/where2008/public/schedule/detail/1700.

7. Conclusion

In the years ahead, the ubiquitous computing may be reinforced by rapid advances in location-based technology that will continue to produce new mobile services for individuals. This study is one of the first attempt to develop a theory on privacy by adopting a psychological control perspective in a specific context of LBS. Our results reveal that individual self-protection, industry self-regulation, and government legislation interact to affect perceived control, which in turn influences the context-specific privacy concerns of individuals. With an understanding of the rationale for the interactions among the three privacy assurance approaches, these results serve as a basis for future theoretical development in the area of information privacy. Theoretical developments in this direction should also yield valuable insights that can guide practice.

Electronic Companion

An electronic companion to this paper is available as part of the online version at http://dx.doi.org/10.1287/isre.1120.0416.

Acknowledgments

The authors are very grateful to the senior editor, Elena Karahanna, for her encouragement and direction in helping them develop this manuscript. They are also grateful to the associate editor, Mariam Zahedi, for her very helpful guidance and to the three anonymous reviewers for their constructive advice and helpful comments on earlier versions of this manuscript. Heng Xu gratefully acknowledges the financial support of the National Science Foundation under Grant CNS-0953749.

References

ABI (2011) Location analytics and privacy: The impact of privacy on LBS, location analytics, and advertising. Allied Business Intelligence Inc. http://www.abiresearch.com/research/1007751.

Ackerman MS, Mainwaring SD (2005) Privacy issues and human-computer interaction. Garfinkel S, Cranor L, eds. *Security and Usability: Designing Secure Systems That People Can Use* (O'Reilly, Sebastopol, CA), 381–400.

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

Agarwal R, Karahanna E (2000) Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quart.* 24(4):665–692.

Ajzen I (2001) Nature and operation of attitudes. *Annual Rev. Psych.* 52(February):27–58.

Altman I (1976) Privacy: A conceptual analysis. *Environment Behav.* 8(1):7–29.

Angst CM, Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quart.* 33(2):339–370.

Armstrong JS, Overton TS (1977) Estimating nonresponse bias in mail surveys. *J. Marketing Res.* 14(3):396–402.

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

Bandura A (2001) Social cognitive theory: An agentic perspective. *Annual Rev. Psych.* 52(1):1–26.

Bansal G, Zahedi F, Gefen D (2008) The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. *Proc. 29th Annual Internat. Conf. Inform. Systems (ICIS 2008), Paris, France* (AIS, Atlanta).

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

Barkhuus L, Dey A (2003) Location-based services for mobile telephony: A study of user's privacy concerns. *Proc. INTERACT, 9th IFIP TC13 Internat. Conf. Human-Comput. Interaction, Zurich, Switzerland* (IOS Press, Amsterdam), 709–712.

Barkhuus L, Brown B, Bell M, Sherwood S, Hall M, Chalmers M (2008) From awareness to repartee: Sharing location within social groups. *Proc. Twenty-Sixth Annual SIGCHI Conf. Human Factors Comput. Systems* (ACM, Florence, Italy), 497–506.

Baron RM, Kenny DA (1986) The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *J. Personality Soc. Psych.* 51(6):1173–1182.

Bellman S, Johnson EJ, Kobrin SJ, Lohse GL (2004) International differences in information privacy concerns: A global survey of consumers. *Inform. Soc.* 20(5, Nov–Dec):313–324.

Berendt B, Gunther O, Spiekermann S (2005) Privacy in e-commerce: Stated preferences vs. actual behavior. *Comm. ACM* 48(4):101–106.

Berghel H (1997) Cyberspace 2000: Dealing with information overload. *Comm. ACM* 40(2):19–24.

Brandimarte L, Acquisti A, Loewenstein G (2010) Misplaced confidences: Privacy and the control paradox. *Proc. Workshop Econom. Inform. Security (WEIS), Boston*, June 2010, http://weis2010.econinfosec.org/papers/session2/weis2010_brandimarte.pdf.

Buchanan T, Paine C, Joinson AN, Reips U (2007) Development of measures of online privacy concern and protection for use on the internet. *J. Amer. Soc. Inform. Sci. Tech.* 58(2):157–165.

Burkert H (1997) Privacy-enhancing technologies: Typology, critique, vision. Agre P, Rotenberg M, eds. *Technology and Privacy: The New Landscape* (MIT Press, Cambridge, MA), 126–143.

Campbell DT, Fiske DW (1959) Convergent and discriminant validation by the multitrait-multimethod matrix. *Psych. Bulletin* 56(1):81–105.

Carte AT, Russell JC (2003) In pursuit of moderation: Nine common errors and their solutions. *MIS Quart.* 27(3):479–501.

Caudill EM, Murphy PE (2000) Consumer online privacy: Legal and ethical issues. *J. Public Policy and Marketing* 19(1):7–19.

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

Chin WW, Marcolin BL, Newsted PR (2003) A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inform. Systems Res.* 14(2):189–217.

Cohen J (1988) *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed. (L. Erlbaum Associates, Hillsdale, NJ).

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

Cranor LF (2002) *Web Privacy with P3P* (O'Reilly & Associates, Sebastopol, CA).

CTIA (2008) Best practices and guidelines for location based services. The Cellular Telecommunications and Internet Association (CTIA). http://www.ctia.org/content/index.cfm/AID/11300.

Culnan MJ (1993) "How did they get my name"? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quart.* 17(3):341–364.

Culnan MJ (1995) Consumer awareness of name removal procedures: Implication for direct marketing. *J. Interactive Marketing* 9(2):10–19.

Culnan MJ (2000) Protecting privacy online: Is self-regulation working? *J. Public Policy and Marketing* 19(1):20–26.

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

Culnan MJ, Bies JR (2003) Consumer privacy: Balancing economic and justice considerations. *J. Soc. Issues* 59(2):323–342.

Culnan MJ, Williams CC (2009) How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quart.* 33(4):673–687.

DeCew JW (1997) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, Ithaca, NY).

Dhillon GS, Moores T (2001) Internet privacy: Interpreting key issues. *Inform. Resources Management J.* 14(4):33–37.

Dinev T, Hart P (2004) Internet privacy concerns and their antecedents—measurement validity and a regression model. *Behav. Inform. Tech.* 23(6):413–423.

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

Edelman B (2011) Adverse selection in online "trust" certifications and search results. *Electronic Commerce Res. Appl.* 10(1):17–25.

Eppler MJ, Mengis J (2004) The concept of information overload: A review of literature from organization science, marketing, accounting, MIS, and related disciplines. *Inform. Soc.* 20(5):325–344.

Falk RF, Miller NB (1992) *A Primer for Soft Modeling* (The University of Akron Press, Akron, OH).

FTC (2000) Privacy online: Fair information practices in the electronic marketplace. Federal Trade Commission. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

FTC (2009) Beyond voice: Mapping the mobile marketplace. Federal Trade Commission. www.ftc.gov/opa/2009/04/mobilerpt.shtm.

FTC (2010) A preliminary FTC staff report on protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Federal Trade Commission. http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

Goldsmith RE, Freiden JB, Kilsheimer JC (1993) Social values and female fashion leadership: A cross-cultural study. *Psych. Marketing* 10(5):399–412.

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

Harding A (2001) Comparative law and legal transplantation in South East Asia. Nelken D, Feest J, eds. *Adapting Legal Cultures* (Hart Publishing, Oxford, Portland, OR), 199–222.

Hoadley MC, Xu H, Lee J, Rosson MB (2010) Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Res. Appl.* 9(1):50–60.

Hoffman DL, Novak TP, Peralta MA (1999) Information privacy in the marketspace: Implications for the commercial uses of anonymity on the web. *Inform. Soc.* 15(2):129–139.

Hui KL, Teo HH, Lee SYT (2007) The value of privacy assurance: An exploratory field experiment. *MIS Quart.* 31(1):19–33.

Im G, Rai A (2008) Knowledge sharing ambidexterity in long-term interorganizational relationships. *Management Sci.* 54(7):1281–1296.

Johnson CA (1974) Privacy as personal control. Carson DH, ed. *Man-Environment Interactions: Evaluations and Applications: Part* 2 (Environmental Design Research Association, Washington, DC), 83–100.

Junglas IA, Watson RT (2006) The U-constructs: Four information drives. *Comm. AIS* 17(1):569–592.

Junglas IA, Johnson NA, Spitzmüller C (2008) Personality traits and concern for privacy: An empirical study in the context of location-based services. *Eur. J. Inform. Systems* 17(4):387–402.

Langer EJ (1975) The illusion of control. *J. Personality Soc. Psych.* 32(2):311–328.

Laufer RS, Wolfe M (1977) Privacy as a concept and a social issue—multidimensional developmental theory. *J. Soc. Issues* 33(3):22–42.

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

Lindell MK, Whitney DJ (2001) Accounting for common method variance in cross-sectional research designs. *J. Appl. Psych.* 86(1):114–121.

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

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

Margulis TS (2003a) Privacy as a social issue and behavioral concept. *J. Soc. Issues* 59(2):243–261.

Margulis TS (2003b) On the status and contribution of Westin's and Altman's theories of privacy. *J. Soc. Issues* 59(2):411–429.

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

Metzger MJ (2006) Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Comm. Res.* 33(3):155–179.

Miller SM (1980) Why having control reduces stress: If I can stop the roller coaster I don't want to get off. Garder J, Seligman MEP, eds. *Human Helplessness: Theory and Applications* (Academic Press, New York), 71–95.

Milne GR, Culnan MJ (2004) Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *J. Interactive Marketing* 18(3):15–29.

Milne GR, Rohm A (2000) Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *J. Public Policy and Marketing* 19(2):238–249.

Mowday RT, Sutton RI (1993) Organizational behavior: Linking individuals and groups to organizational contexts. *Annual Rev. Psych.* 44(1):195–229.

Moores T (2005) Do consumers understand the role of privacy seals in e-commerce? *Comm. ACM* 48(3):86–91.

Moores T, Dhillon G (2003) Do privacy seals in e-commerce really work? *Comm. ACM* 46(12):265–271.

Nicolaou AI, McKnight DH (2006) Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Inform. Systems Res.* 17(4):332–351.

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

Oded N, Sunil W (2009) Social computing privacy concerns: Antecedents and effects. *Proc. 27th Internat. Conf. Human Factors Comput. Systems* (*CHI*) (ACM, Boston), 333–336.

Pavlou PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. *Inform. Systems Res.* 15(1):37–59.

Pavlou PA, Liang H, Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quart.* 31(1):105–136.

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

Podsakoff MP, MacKenzie BS, Lee JY, Podsakoff NP (2003) Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psych.* 88(5):879–890.

Reed GM, Taylor SE, Kemeny ME (1993) Perceived control and psychological adjustment in gay men with AIDS. *J. Appl. Soc. Psych.* 23(10):791–824.

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

Schwartz MP (1999) Privacy and democracy in cyberspace. *Vanderbilt Law Rev.* 52(6):1610–1701.

Sheehan KB (1999) An investigation of gender differences in online privacy concerns and resultant behaviors. *J. Interactive Marketing* 13(4):24–38.

Sheehan KB (2002) Toward a typology of Internet users and online privacy concerns. *Inform. Soc.* 18(1):21–32.

Skinner EA (1996) A guide to constructs of control. *J. Personality Soc. Psych.* 71(3):549–570.

Slyke CV, Shim JT, Johnson R, Jiang JJ (2006) Concern for information privacy and online consumer purchasing. *J. Assoc. Inform. Systems* 7(6):415–444.

Smith HJ (2004) Information privacy and its management. *MIS Quart. Executive* 3(4):201–213.

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

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

Sobel ME (1982) Asymptotic intervals for indirect effects in structural equations models. Leinhart S, ed. *Sociological Methodology* (Jossey-Bass, San Francisco), 290–312.

Solove DJ (2002) Conceptualizing privacy. *California Law Rev.* 90(4):1087–1155.

Solove DJ (2006) A taxonomy of privacy. *Univ. Pennsylvania Law Rev.* 154(3):477–560.

Solove DJ (2007) "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Rev.* 44(4):745–772.

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

Spiekermann S, Cranor LF (2009) Engineering privacy. *IEEE Trans. Software Engrg.* 35(1):67–82.

Spiro WG, Houghteling LJ (1981) *The Dynamics of Law*, 2nd ed. (Harcourt Brace Jovanovich, New York).

Squicciarini CA, Xu H, Zhang X (2011) CoPE: Enabling collaborative privacy management in online social networks. *J. Amer. Soc. Inform. Sci. Tech.* 62(3):521–534.

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

Sundar SS, Marathe SS (2010) Personalization vs. customization: The importance of agency, privacy, and power usage. *Human Comm. Res.* 36(3):298–322.

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

Tang Z, Hu YJ, Smith MD (2008) Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *J. Management Inform. Systems* 24(4):153–173.

TRUSTe (2004) TRUSTe plugs into wireless: TRUSTe's wireless advisory committee announces first wireless privacy standards. http://www.truste.org/articles/wireless_guidelines_0304.php.

Tsai YJ, Kelly GP, Cranor FL, Sadeh N (2010) Location-sharing technologies: Privacy risks and controls. *I/S: J. Law Policy Inform. Soc.* 6(2):119–151.

Turner EC, Dasgupta S (2003) Privacy on the Web: An examination of users concerns, technology, and implications for business organizations and individuals. *Inform. Systems Management* 20(1):8–18.

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

Wallston AK (2001) Conceptualization and operationalization of perceived control. Baum A, Revenson TA, Singer JE, eds. *Handbook of Health Psychology* (Lawrence Erlbaum Associates, Mahwah, NJ), 49–58.

Wang W, Benbasat I (2009) Interactive decision aids for consumer decision making in e-commerce: The influence of perceived strategy restrictiveness. *MIS Quart.* 33(2):293–320.

Wang N, Xu H, Grossklags J (2011) Third-party apps on Facebook: Privacy and the illusion of control. *Proc. ACM Sympos. Comput.-Human Interaction for Management Inform. Tech.* (*CHIMIT*), *Boston* (ACM, New York).

Weisz JR, Rothbaum FM, Blackburn TC (1984) Standing out and standing in: The psychology of control in America and Japan. *Amer. Psych.* 39(9):955–969.

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

Wetzels M, Odekerken-Schroder G, van Oppen C (2009) Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quart.* 33(1):177–195.

Xu H, Dinev T, Smith HJ, Hart P (2008) Examining the formation of individual's information privacy concerns: Toward an integrative view. *Proc. 29th Annual Internat. Conf. Inform. Systems* (*ICIS* 2008), *Paris, France* (AIS, Atlanta).

Xu H, Dinev, T, Smith HJ, Hart P (2011) Information privacy concerns: Liking individual perceptions with institutional privacy assurances. *J. Assoc. for Inform. Systems* 12(12): 798–824.

Xu H, Teo HH, Tan BCY, Agarwal R (2010) The role of push-pull technology in privacy calculus: The case of location-based services. *J. Management Inform. Systems* 26(3):135–174.

Yamaguchi S (2001) Culture and control orientations. Matsumoto D, ed. *The Handbook of Culture and Psychology* (Oxford University Press, New York), 223–243.

Zweig D, Webster J (2002) Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *J. Organ. Behav.* 23(5):605–633.