THE EFFECTS OF SELF-CONSTRUAL AND PERCEIVED CONTROL ON PRIVACY CONCERNS

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

Abstract

Recent advances in mobile computing technology have led to a proliferation of location-based services (LBS). Although LBS offer users the flexibility of accessing networks and services while on the move, potential privacy violations have emerged as a contentious issue because information related to the consumer's identity, movements, behavior, and habits are available to the LBS provider. Adopting the psychological control and self-construal perspectives, this paper focuses on three leading mechanisms that can alleviate privacy concerns in the LBS context. We draw from the control agency and self-construal theories to propose a framework linking three mechanisms (privacy-enhancing technology, industry self-regulation, and government legislation) to privacy concerns through the mediating effects of perceived control the moderating role of self-construal. We test the predictions of the framework using data obtained from 141 mobile phone users through an experiment. Results show that all the three mechanisms are effective in increasing perceived control, which in turn mitigates privacy concerns. We also find that people who value independent-self prefer personal control through technology-based mechanisms; whereas people who value interdependent-self prefer proxy control through industry self-regulation and through government legislation. In addition to enhancing our theoretical understanding of information privacy in the LBS context, these findings have important implications for LBS providers and consumers, as well as for regulatory bodies and LBS technology developers.

Keywords: Privacy concerns, perceived control, self-construal, location-based services

Introduction

As information technologies increasingly expand the ability for organizations to collect, process, distribute and exploit personal data, information privacy is an ever-present concern. Innovative technologies and infrastructures, from ubiquitous computing to smart technologies, are being rapidly introduced and adopted in daily life; personal digital devices, from personal digital assistants (PDA) to smart phones, carry with them new possibilities of ubiquitous information access, and so for privacy invasions. Public opinion polls reveal that consumers are generally concerned about merchants having excessive access to their personal information (USC 2007). Over the past decade, the issue of information privacy has drawn considerable attention among researchers in disciplines such as public policy (Caudill and Murphy 2000), marketing (Milne and Rohm 2000), organizational behavior (Milberg et al. 2000), and information systems (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996). A general conclusion from prior research is that consumers will resist technologies, such as ubiquitous computing applications, in the presence of significant privacy concerns.

Research also suggests that consumers tend to have lower privacy concerns if they perceive a certain degree of control over the collection and use of their personal information (Nowak and Phelps 1997; Sheehan and Hoy 2000). However, the subtle link between control and privacy concerns has not been verified in empirical research. As noted by Margulis (2003a; 2003b), privacy theorists have failed to integrate the literature on psychological control into theories of privacy. As a consequence, the phenomenon of psychological control has not contributed as much

to our understanding of privacy concerns as it should have. In response to the call for a stronger theoretical basis for privacy research, we propose and empirically test the *perceived control–privacy concerns* relationship in this study. Specifically, we examine three mechanisms that can potentially empower consumers with greater control over information privacy for their impacts on privacy concerns, via their influence on perceived control. These three mechanisms are privacy-enhancing technology, industry self-regulation, government legislation (Culnan and Bies 2003). In addition, drawing on the social theoretical perspective of linking privacy to the *self* related concepts, we further examine the moderating role of self-construal on affecting consumers' perceived control over collection and use of personal information. The self-construal serves to shift an individual's frame of reference toward either an interdependent self or independent self on a chronic basis (Singelis 1994). It is likely that such chronic self perceptions may shift the individual's reference group which will, in turn, influence their preferences on control agency and control perceptions.

We test our research framework in an understudied ubiquitous computing context. This context is noteworthy because potential users of ubiquitous computing applications (e.g., location-based services) are seriously concerned about the privacy implications of disclosing their personal information (Beresford and Stajano 2003). In addition, the ubiquitous information environment offers consumers relatively more *control* over the communication and exchange process than has been the case in Internet or traditional media environment such as broadcast and prints (Junglas and Waston 2003b). It becomes more important for service providers, privacy advocates, and policy makers to realize that the effects of privacy assurance mechanisms might be very different to different individuals. Thus, our research extends current knowledge by capturing the complexity of the *perceived control–privacy concerns* relationship with the recognition of the diversity of users and in a context marked by ubiquity and uniqueness (Junglas and Waston 2003b).

This study advances theoretical development on information privacy in two important ways. First, it theorizes the role of psychological control in alleviating privacy concerns and investigates how control perceptions can be effectively established through different mechanisms. Second, recognition of the diversity of people (self-construal) represents an incremental contribution that provides a rich understanding on how privacy concerns could be alleviated through different mechanisms for different individuals, and therefore, informs privacy research and practice in information systems (IS) discipline. The findings are also potentially useful to privacy advocates, regulatory bodies, merchants, wireless service providers and device manufacturers to help shape or justify their decisions concerning ubiquitous computing environment.

Theoretical Foundations and Research Hypotheses

The central thesis of this study is built on the argument that the effectiveness of the privacy assurance mechanisms to materially alleviating privacy concerns depends on how each mechanism increases perceived control over information privacy. In a recent study by Xu and Teo (2004), the control agency theory (Yamaguchi 2001) was proposed as potential theoretical foundation in psychology for privacy studies. In the current study, we adopt the same vehicle of control agency to explain the differences both in the way how the three privacy assurance mechanisms differ and in the way how the self-construal moderates the effects of privacy assurance mechanisms on perceived control.

In the discussion that follows, we first elaborate on rising consumer privacy concerns pertaining to location-based services (LBS). Then we review the literature on psychological control and control agency. Mapping the control agency framework to the information privacy context, we theorize how control perceptions can be effectively established through the three privacy assurance mechanisms. Finally, we describe the concept of self-construal, hypothesizing its moderating effects on the relationship between privacy assurance mechanisms and perceived control over information privacy.

Location-Based Services and Privacy Concerns

Propelled by advances in wireless communication technology in the past decade, location-based services (LBS) are becoming a prevalent phenomenon globally (Rao and Minakakis 2003). LBS include location-aware applications that utilize geographical positioning information to provide value-added services to consumers (Barnes 2003). The growth trajectory of LBS is striking. According to Allied Business Intelligence (ABI 2004), global LBS revenue is expected to increase from US$0.5 billion in 2004 to US$3.6 billion by the end of the decade. In the US, a key driver

of LBS growth is the US Federal Communications Commission E911 Phase II bill, which requires emergency services to have the ability to automatically locate the position of any cell phone dialing 911 to within 100 meters (FCC 2004). Coupled with technology developments, this mandate has created a large market for innovative LBS.

Unsurprisingly, the commercial potential and rapid growth of LBS have been accompanied by concerns regarding the collection and use of individual information by LBS providers. These concerns pertain to the confidentiality of accumulated consumer information (e.g., continuous location information and other personal identifiable information) (FCC 2004) and the potential risk that consumers would experience with a breach of confidentiality (Gidari 2000). Continuous location information often reveals the position of a person in real time, rendering the potential intrusion of privacy an acute concern (Beinat 2001). This situation is exacerbated by the fact that some LBS providers are able to combine continuous location information of consumers with other personally identifiable information. Such an extensive collection of information is subject to potential abuse and improper handling of such information can expose consumers to significant risk. Indeed, the Big Brother imagery (Orwell 1949) looms in the popular press when LBS are discussed (e.g., Levy 2004). To the degree that that privacy concerns represent a major inhibiting factor in the adoption of LBS (Beinat 2001; Wallace et al. 2002), it is clearly important to understand how they can be addressed. This study theoretically develops and empirically tests a model that explains how the privacy concerns of consumers associated with LBS use may be alleviated.

Privacy Concerns: A Perceived Control Perspective

In the privacy literature, the concept of privacy is closely associated with the psychological *control* of personal information (Johnson 1974; Westin 1967). Several privacy theorists have implicitly adopted such a control perspective when defining privacy. For example, Altman (1974) defines privacy as "the selective control over access to the self or to one's group". Stone et al. (1983) define privacy as "the ability of the individual to control personal information about one's self". More recently, Margulis (2003a) views privacy as "control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access".

Adopting such a control perspective, privacy theorists argue that the loss of control over personal information is central to the notion of privacy invasion. Some empirical studies provide evidence that control is a key factor that explains individual perceptions of privacy invasion (Sheehan and Hoy 2000). Consumers tend to perceive information disclosure as less privacy-invasive if they believe that they have control over the collection and use of their personal information (Culnan and Armstrong 1999). In other works, Malhotra et al. (2004) posit that control is one of the most important factors affecting privacy concerns among Internet users. However, although this link between psychological control and privacy concerns has been frequently discussed in the literature, there have been very few attempts (see Johnson 1974, for an example) to integrate control theories into privacy research. Given the key role that control plays in the discussions of privacy, it is clearly useful to employ control theories to build a theoretical framework for privacy research.

In the psychology literature, psychological control is commonly treated as a perceptual construct because perceived control affects human behavior much more than actual control (Skinner 1996). As a cognitive construct, perceived control is subjective and need not necessarily involve attempts to affect a behavioral change (Langer 1975). Specifically, perceived control is defined as a belief about the extent to which an agent can produce desired outcomes (Skinner et al. 1988).

Most researchers in mainstream psychology may mean personal control when they simply refer to control. For example, Skinner (1996) concluded after a comprehensive review of the control-related constructs that the prototypical control is personal control, in which the agent of control is the self. However, Yamaguchi (2001) goes beyond the simple notions of control typically presented in mainstream psychology by outlining not only personal control (in which the self acts as the agent of control), but also proxy control (in which powerful others act as the agent of control). According to Yamaguchi (2001, p.226), people would especially feel greater autonomy when they exercise direct *personal control* in which the self acts as the control agent. However, when exercise of personal control is neither readily available nor encouraged, people might well relinquish their direct control preferences and seek "security in proxy control" (Bandura 1982, p.142). *Proxy control* is an attempt to align oneself with a powerful force in order to gain control through powerful others when people do not have enough skills, resources, and power to bring about their desired outcome or avoid an undesired outcome in the environment (Yamaguchi 2001). For example, in the situation of third-party interventions in which intermediaries are called upon to regulate the

relationships between parties with potential or actual conflict of interests, people can gain a desired outcome with the help of those intermediaries without acting agentically (i.e., proxy control).

Assuring Information Privacy: Three Mechanisms

The privacy literature describes three mechanisms for alleviating privacy concerns: privacy-enhancing technology, industry self-regulation, and government legislation (Banisar 2000; Culnan and Bies 2003; Fischer-Hüber 2000). Privacy-enhancing technology comprises tools that allow consumers to protect their information privacy by directly controlling the flow of their personal information to others (Burkert 1997), such as LBS providers. As is evident, with privacy-enhancing technology, the agent of control is the self; and the effects of this mechanism arise due to the opportunity for personal control. 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. Seals of approval from trusted third-parties (such as Online Privacy Alliance and TRUSTe) are one example of the mechanism that was created to provide third-party assurances to consumers based on a voluntary contractual relationship between firms and the seal provider. On behalf of consumers, these third parties act as the control agents for consumers to exercise proxy control over the collection and use of personal information. Finally, government legislation is the other commonly used approach for assuring proxy control, which relies on the judicial and legislative branches of a government for protecting personal information (Swire 1997). For instance, the United States has sector-specific privacy laws that apply to industry sectors and specific issues (Culnan and Bies 2003). Privacy laws exist that apply to specific populations of people (e.g., children) or specific types of personal information (e.g., health and financial information). On behalf of consumers, these laws exercise proxy control that regulates the collection and use of personal information.

The following sub-sections develop the hypotheses about the relationships between privacy assurance mechanisms and perceived control, and elaborate on the reasoning supporting the causal relationships among these constructs in the research model.

Personal Control through Privacy Enhancing Technologies

When consumers exercise personal control through privacy-enhancing technology, they are striving for primary control over their environment (Weisz et al. 1984). Such a mechanism empowers consumers with primary control over how their personal information may be gathered by LBS providers. For instance, to assuage employee perceptions of privacy invasion in the workplace, monitoring systems have been designed with features that allow employees to decide when their images can be displayed (Zweig and Webster 2002). When employees are provided the means to delay or prevent performance monitoring, their perception of personal control increases (Stanton 1996). Hence, when consumers are able to control the disclosure of their personal information to LBS providers using privacy-enhancing technology, their level of perceived control is likely to increase. Therefore, we hypothesize:

> **H1:** *The availability of personal control through privacy-enhancing technology is positively related to consumers' perceived control over their personal information.*

Proxy Control through Industry Self-Regulation

For industry self-regulation to effectively assure proxy control over information privacy, firms need to voluntarily adopt and implement privacy policies that are based at a minimum on Fair Information Practices (Culnan and Bies 2003). Third party intervention, therefore, has been employed in self-regulation to provide legitimacy and trustworthiness to companies through membership or seals of approval (such as Online Privacy Alliance, and TRUSTe[1]) that are designed to confirm adequate privacy compliance. The literature on institutional structures (e.g.,McKnight et al. 1998; Pavlou and Gefen 2004) may help explain the positive effects of industry self-regulation in enhancing control perceptions for two reasons. First, the self-regulatory structures built into the firm's web site, such as the privacy policy and privacy seal could assure people that everything in the setting is as it ought to be (McKnight et al. 1998), allowing consumers to form and hold beliefs about their proxy control over personal

[1] See TRUSTe at http://www.truste.org/, and Online Privacy Alliance at http://www.privacyalliance.org/ for examples.

information. Second, when violation occurs, these structures could provide the means of recourse for the aggrieved, thereby creating strong incentives for firms to refrain from opportunistic behavior and behave appropriately (Benassi 1999)[2]. Hence, having a third party like the reputable TRUSTe to vouch for a firm's trustworthiness should enable consumers to believe that they are able to exercise proxy control over their personal information.

> **H2:** *The availability of proxy control through industry self-regulation is positively related to consumers' perceived control over their personal information.*

Proxy Control through Government Legislation

Prior studies have reported a strong link between government legislation and consumer perception of control over the use of their personal information (Culnan and Armstrong 1999). Some scholars have even suggested that the legal system is the most powerful mechanism for the exercise of proxy control because it requires that offenders be punished in order to maintain its deterrent effectiveness (Spiro and Houghteling 1981). With government legislation, illegal behavior can be deterred through threat of punishment (Tittle 1980). Recognizing the deterrent value of a legal system, consumers tend to believe that LBS providers would abide by the law (Tittle 1980), and would therefore collect and use personal information appropriately. In other words, through government legislation, consumers can exercise proxy control over the collection and use of their personal information by LBS providers. Government legislation is also effective for resolving conflicts that may occur. Thus, in the presence of relevant government legislation, consumers are likely to perceive a higher level of control. Therefore, we hypothesize:

> **H3:** *The availability of proxy control through government legislation is positively related to consumers' perceived control over their personal information.*

The Moderating Role of Self-Construal

The information flow between individuals and other entities can be viewed as a boundary regulation process (Altman 1975). Such boundary regulation process is "a process of give and take among various entities – from individuals to groups to institutions – in ever-present and natural tension with the simultaneous information need" (Palen and Dourish 2003, p.129). There has been a rich research tradition of linking privacy to the *self* in social psychology (Altman 1974; Altman 1975; Foddy and Finighan 1980). It was suggested that the function of privacy has its psychological root "inside" the self (Altman 1974). In a hierarchical model of functions of privacy proposed by Altman (1975), creating self-identity is conceived of the ultimate goal of privacy. Westin (1967, p.39) also describes the major function of privacy as "… an instrument for achieving individual goals of self-realization".

Social cognition research on the self has developed a variety of theoretical constructs to explain the complex nature of self-related behavior. One important aspect of the self conceptualization is related to schematic self-aspects – *self-construal* (Markus 1977; Singelis 1994). Self-construal reflects the extent to which individuals view themselves either as a separate individual (independent aspects of self) versus as part of a group lead to a particular self-construal (interdependent aspects of self). In this study, we believe that privacy assurance mechanisms become linked to self-construal when the mechanisms are able to help individuals achieve privacy goals that are motivated by the self. Specifically, we examine how the effects of three privacy assurance mechanisms on perceived control may differ depending upon a consumer's self-construal.

The two selves (independent and interdependent) may coexist within every individual and in any culture but individuals may differ in the relative strength of these two selves on a chronic basis (due to social or cultural surroundings), or on a temporarily accessible basis (due to primed or contextually activated self) (Hong et al. 2000; Markus and Kitayama 1991). In this study, we focus on differences in self-construal due to chronic tendencies. Since independent-selves perceive themselves as and strive to be independent, they should perceive themselves as volitional actors and be motivated by contexts fostering personal agency (Markus and Kitayama 1991). Therefore,

---

[2] Taking TRUSTe as an example, any complaint raised against a licensee will result in reviews and inquiries by TRUSTe, and an escalated investigation will be conducted if the initial inquiries do not result in a satisfactory resolution to the complaint. Depending on the severity of the violation, the escalated investigation could lead to a compliance review by a CPA firm of the web site, termination as a licensee of TRUSTe and revocation of the trustmark, or referral to the appropriate law authority which may include the appropriate attorney general's office, the FTC, or the Consumer Protection Agency in the US (Benassi 1999).

people who value independent self are more personally agentic (Hernandez and Iyengar 2001) and hence prefer to exercise direct personal control over their personal information through technology-based mechanisms. In contrast, people with interdependent self-construals focus on aspects of self shared with some subset of others and perceive themselves as being interconnected with and interrelated to others in their social context (Markus and Kitayama 1991). Interdependent-selves should therefore, perceive their surroundings in terms of powerful others that are vital, influential and liable (Hernandez and Iyengar 2001) and will be particularly motivated by contexts that allow proxy agency (in which they align with powerful others). Therefore, people who value interdependent-self are more proxy agentic and hence prefer proxy control.

H4: *The positive impact of technology based mechanism on perceived control should be stronger for the independent-self than for the interdependent-self.*

H5: *The positive impact of industry self-regulation based mechanism on perceived control should be stronger for the interdependent-self than for the independent-self.*

H6: *The positive impact of government legislation based mechanism on perceived control should be stronger for the interdependent-self than for the independent-self.*

Perceived Control and Privacy Concerns

Some researchers have equated the concept of privacy with control. Johnson (1974), for instance, defined privacy as "secondary control in the service of need-satisfying outcome effectance" (p. 91). Goodwin (1991) defined consumer privacy by two dimensions of control: control over information disclosure and control over unwanted physical intrusions into the consumer's environment. However, many researchers reason that control is actually one of the factors that shape privacy and that privacy is not control *per se* (Laufer and Wolfe 1977; Margulis 2003a; 2003b). For instance, Laufer and Wolfe (1977) conceptualized control as a mediating variable in the privacy system by arguing that "a situation is not necessarily a privacy situation simply because the individual perceives, experiences, or exercises control" (p. 26). Conversely, the individual may not perceive s/he has a control, yet the environmental and interpersonal elements may create perceptions of privacy (Laufer and Wolfe 1977). Therefore, privacy should be more than control and control might be one of the factors which determine privacy state. These considerations suggest that perceived control over disclosure and subsequent use of personal information is a separate construct from privacy concerns and that the two constructs are negatively related. Prior research has shown that, in general, individuals will have fewer privacy concerns when they have a greater sense that they control the disclosure and subsequent use of their information (Milne and Boza 1999). Therefore, in this study, we hypothesize that perceived control over personal information is an antecedent to privacy concerns and we expect a similar negative relationship between perceived control and privacy concerns in the LBS context.

H7: *There is a negative relationship between perceived control and privacy concerns.*

Control Variables

Prior research on privacy identifies a number of factors that may impact perceived control or privacy concerns. We include these factors as covariates in the study to isolate the effects of the privacy enhancing mechanisms. Specifically, we exclude variance accounted for by prior experience with mobile applications (Sheehan and Hoy 2000), desire for information control (Phelps et al. 2000), trust propensity (McKnight et al. 2002) and previous privacy experience (Culnan 1995).

Research Method

We conducted an experiment to test the research hypotheses. The experimental approach, which allows for precision of measurement and control over extraneous sources of variance, is particularly appropriate in the context of this study. A push-based LBS application (mobile coupon service) was utilized because LBS providers with push-based applications tend to be more aggressive in promoting their services through active tracking of consumer information, thereby resulting in greater privacy concerns among consumers (Wallace et al. 2002). Details of the experiment design are provided below.

Operationalization of Variables

To the extent possible, we adapted constructs from measurement scales used in prior studies to fit the LBS context. Items measuring *perceived control* were based on the work of Reed et al. (1993) in the context of health psychology. The wording was adapted to focus on perceived control over personal information. Drawing on Smith et al. (1996), we operationalized *privacy concerns* as a reflective construct encompassing four areas of consumers' concerns about information privacy practices: collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. We selected one item from each of the four perspectives of the information privacy concern instrument developed by Smith et al.(1996). With regard to control variables, *previous privacy experience* was measured with three questions adapted from Smith et al. (1996), *desire for information control* was assessed with three questions adapted from Phelps et al. (2000), *trust propensity* was measured with three questions taken from McKnight et al. (2002) and *prior experience in using mobile applications* was measured with questions on the number of times in the previous year the subjects had used a mobile application. We used the Singelis (1994) scales for independence and interdependences to identify participants who are high on one type of self-construal, but low on the other.

Manipulation

We used a 2 (with/without technology) × 2 (with/without self-regulation) × 2 (with/without legislation) factorial experiment design. We varied the three control assurance mechanisms—*technology*, *self-regulation*, and *legislation* to construct multiple experiment scenarios. We carried out two pilot tests to ensure that the manipulation was anchored at the appropriate level to be able to detect differences, to modify and finalize the instrument, and to refine the experimental procedures and instructions.

Privacy-enhancing technologies are available for mobile devices in many forms: for example, consumers can now limit the amount of location information collected by LBS providers (Anuket 2003) by simply turning off the LBS with a click on a button on the mobile communication device anytime and anywhere. Some devices also allow consumers to specify the accuracy of location information to be released to LBS providers (Anuket 2003). Therefore, in the experiment, we manipulated privacy-enhancing technology by providing subjects with an interactive graphical interface of a mobile communication device that allows them to restrict their location information released to the LBS provider.

With industry self-regulation, LBS providers handle personal information based on their privacy policy, with trusted third parties acting as an assurance against violations. For example, the Wireless Location Industry Association has established guidelines to govern the use of personal information linked to location and prescribed responsible practices for businesses in the industry (WLIA 2001). A well-known trusted third party, TRUSTe has a set of wireless privacy principles and implementation guidelines for LBS providers to safeguard privacy of personal information (TRUSTe 2004). LBS providers who adhere to these principles and guidelines are awarded the TRUSTe seal, which adds credibility to their privacy practices. When violations occur, this seal may be revoked. Because TRUSTe seal is applicable for LBS providers, industry self-regulation was manipulated by showing subjects a TRUSTe seal with a URL link to the privacy policy of the LBS providers. 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.

An increasing number of countries are formulating laws to safeguard privacy of personal information. In the United States, privacy legislation has received a boost from the E911 Phase II obligations. US legislation (Wireless Communications and Public Safety Act of 1999) requires that location related customer information be limited during disclosure (under the Communication Act of 1996). The US Congress amended Section 222 to explicitly require "express prior authorization" before LBS consumers can be deemed to have consented to the use, disclosure, or access to wireless location information[3]. Similar action was taken by the European Commission in a directive (COM (2000) 385) which explicitly requires location information to be used only with the consent of consumers and only for the duration necessary to provide the specific services. Further, consumers have to be provided with simple means to temporarily deny the collection and use of their location information. Therefore, in the experiment, we manipulated government legislation by informing the subjects that LBS transactions were governed by privacy

[3] See Title 47 U.S.C. 222 (h) (1), available at http://www4.law.cornell.edu/uscode/47/222.html

protection laws which cover the collection and use of their personal information. Subjects were also presented with a news item related to recent enforcement of the privacy legislation has.

Procedure and Task

At the start of each experimental session, the subjects were told that all the instructions were provided online and that they should read the instructions carefully and complete the experiment independently. After logging into our Web-based experiment system, all subjects began the experiment by answering a pre-session questionnaire about their personal information as a form of control check. Next, as commonly used in marketing experiments that investigate consumers' behavior, a cover story was provided to all the subjects. They were told that one specific LBS application—Mobile Coupon (M-Coupon) service provided by Company A would be soon introduced in the market, and their feedback would be very important for the evaluation of such service. Next, our Web-based experiment system generated the scenarios randomly so that each respondent has an equal and independent chance of being put into any of the eight scenarios. The subjects were presented with the introduction of the M-Coupon service that was described in the form of a real company web site to ensure realism. They were then asked to visit the site and other relevant information about M-Coupon service. The experimental system logged the accesses made by the subjects to all the URLs to ensure that the subjects had actually viewed the manipulated condition. After task completion, we measured various research constructs through a survey. Subjects took an average of 25-30 minutes to complete the experiment.

Subjects

A total of 208 responses were obtained among mobile phone users. We recruited the experiment subjects by posting announcements to a number of relevant forums or topics on mobile devices and mobile applications on the major web portals based in Singapore. Our postings explained who we were and what we were trying to do (i.e., the purpose of this study) and invited subjects' participation. The respondents were asked to click on the URL link provided in the posted message, which linked to the online experiment. To motivate subject participation with the experiment, a lottery with four prizes was offered to all the participants. These prizes included a high-end mobile phone, a MP3 Player, a Bluetooth headset and S$300 cash.

The respondents did not differ from a nationally representative sample in terms of gender ratio and mobile phone usage[4]. However, the respondents' education and household income were higher than the national average. Having a more educated and wealthier population may imply that the subject group may be more worried about information misuse and they have more to lose financially should they experience privacy breach incidents.

Data Analysis and Results

Control and Manipulation Checks

We performed control checks on subjects' characteristics (i.e., trust propensity and previous privacy experience) and other variables which might be confounded with perceived control (i.e., desired control and preference for control assurance). Several ANOVA tests were performed to confirm that the random assignment of subjects to the eight experimental conditions was successful. To ensure that participants attended to their assigned experimental conditions, manipulation checks were included in the post-session questionnaire. The manipulations on *technology*, *self-regulation* and *legislation* were checked against true/false questions. Specifically, for the *technology* treatment, the subjects were asked whether they could use a software tool installed on the mobile phone to turn off the subscribed M-Coupon service anytime when they want to. For the *self-regulation* treatment, the subjects were asked whether there was a TRUSTe logo on Company A's privacy statement. For the *legislation* treatment, the subjects were asked whether there was a *Privacy and Wireless Communications Protection Act* to protect their privacy in

[4] Please refer to *Singapore Statistics – Key Annual Indicators*, available at http://www.singstat.gov.sg/stats/keyind.html#econind

LBS. Subjects who did not correctly answer above questions were dropped from the subsequent analyses. This resulted in 179 valid data sets.

Partial Least Squares (PLS)

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold (1982) , was used for data analysis. PLS possesses many advantages over traditional statistical methods such as regression. First, it is not contingent upon data having multivariate normal distributions and interval scales (1982). This makes PLS suitable for handling manipulated constructs. Second, PLS has the ability to simultaneously test the measurement model and the structural model. This will provide a more complete analysis for the inter-relationships in the model. Third, it is generally more appropriate for testing theories in the early stages of development (Bagozzi and Fornell 1982). Since this study is an early attempt to examine the moderating role of self-construal on affecting perceived control and privacy concerns, PLS is more suitable for this exploratory study.

Evaluating the Measurement Model

The measurement model was evaluated by examining the convergent and discriminant validity of the research instrument. Convergent validity is the degree to which different attempts to measure the same construct agree (Bagozzi and Fornell 1982). We evaluated convergent validity using reliability of items, composite reliability of constructs, average variance extracted by constructs, and Cronbach's alpha of constructs. The reliability of an item is its loading on the intended construct. In this study, the loadings all exceed 0.707 (see appendix), indicating adequate reliability (Falk and Miller 1992). The composite reliability of all constructs exceeds 0.7. The average variance extracted by all constructs is above 0.5, and Cronbach's alpha for all constructs also exceeds 0.7. These results point to adequate convergent validity for the measures (see Table 1).

Discriminant validity is the degree to which measures of different constructs are distinct (1978). To test discriminant validity, 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. Table 1 reports the results of discriminant validity which is checked by comparing the diagonal to the non-diagonal elements. All items fulfilled the requirement of discriminant validity.

Table 1. Properties of Measurement Scales

Constructs	CR	CA	AVE	Discriminant Validity				
				1	2	3	4	5
1. Perceived Control (PCTL)	.94	.93	.75	.75				
2. Privacy Concerns (PCON)	.95	.95	.79	-.32	.79			
3. Trust Propensity (TP)	.84	.75	.64	.02	-.03	.64		
4. Desire for Information Control (DC)	.96	.95	.88	.01	.01	.01	.88	
5. Previous Privacy Experience (PPRE)	.87	.78	.70	.02	.04	.01	.02	.70

Notes. CR = composite reliability; CA = Cronbach's Alpha; AVE = average variance extracted.

Evaluating the Structural Model

Following the analysis method adopted in Escalas and Bettman (2005), we split the dataset into two subsets according to self-construals. Participants completed the entire Singelis (1994) scales for independent (12 items, α = .84) and interdependent (12 items, α = .79) chronic self-concepts. Based on median splits, participants were divided into high and low groups for each self-construal type. Participants who were high in independent and low in interdependent were considered to be schematic on independence, while participants who were high in interdependence and low in independence were considered to be schematic on interdependence (Escalas and Bettman 2005). Participants who were high on both or low on both scales were eliminated from the dataset, leaving

a total of 141 participants. We tested the structural paths separately for independent and interdependent participants by applying bootstrapping technique in PLS. Figures 1a and 1b depict the results. The hypotheses were evaluated according to the size, sign, and significance of the path coefficients. All the path coefficients shown in Figures 1a and 1b were with the expected sign, and significant at the 0.05 level.

For both independent and interdependent participants, the positive effects of privacy-enhancing technology, industry self-regulation and government legislation were significant. Therefore, the hypotheses H1, H2, and H3 were supported. Perceived control was a significant predictor of privacy concerns (H7) for both independent and interdependent participants.

Hypotheses related to the moderating effects of self-construals (H4, H5 and H6) were tested with the approach suggested in Carte and Russell (2003) and Duxbury and Higgins (1991). After confirming that inter-item covariance matrices within the construct of perceived control were equal (Box's $M = 5.51$, $F = 0.55$, $p = 0.86$), we proceeded to test the moderating effects of self-construals using the PLS-generated path coefficients and their standard errors. The results of these tests are shown in Table 2. In support of H4, the relationship between technology and perceived control was stronger for the independent participants (t (139) =3.93, $p< 0.01$)[5]. H5 stated that the positive relationship between industry self-regulation and perceived control would be stronger for interdependent participants. This was supported by the data (t (139) = 6.81, $p< 0.01$). Results also showed that the positive relationship between government and perceived control was stronger for interdependent participants (t (139) = 3.21, $p< 0.01$) and thus H6 was supported.

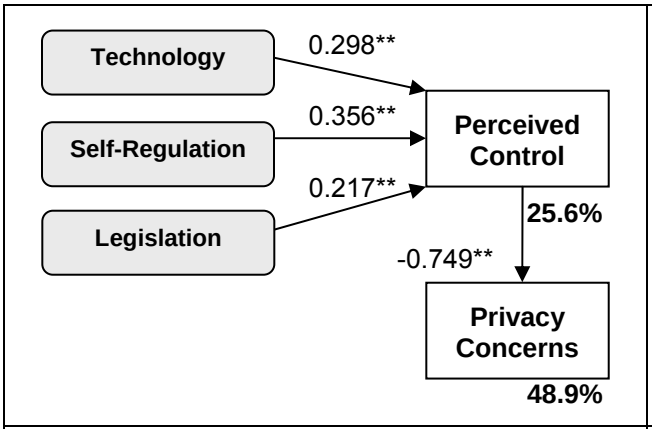

Figure 1a. PLS Results (independent self) n= 63

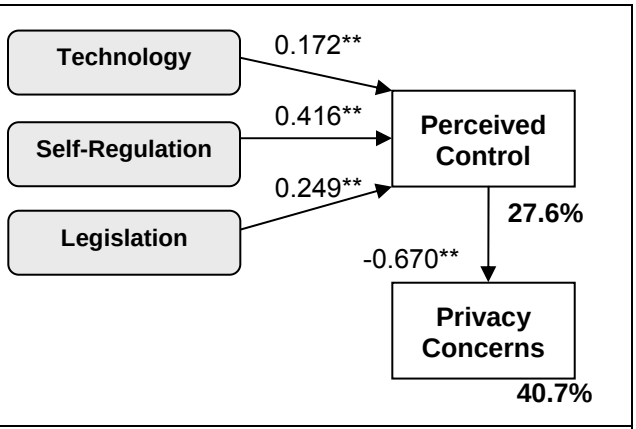

Figure 1b. PLS Results (interdependent self) n= 78

Note: Variance explained in **bold**, * Significant at $p < 0.05$, ** Significant at $p < 0.01$

Table 2. Results on Moderating Impact of Self-Construal

Path	Coefficient		*t*	Supported
	Independent	Interdependent		
H4: Technology → Perceived Control	0.298	0.172	3.93	Yes
H5: Industry Self-Regulation → Perceived Control	0.356	0.416	6.81	Yes
H6: Government Legislation → Perceived Control	0.217	0.249	3.21	Yes

[5] The following test of the difference between path coefficients was suggested in Chin (2004):

$$\frac{coeff_1 - coeff_2}{\sqrt{\frac{(n_1-1)}{(n_1+n_2-2)} \times SE_1^2 + \frac{(n_2-1)}{(n_1+n_2-2)} \times SE_2^2} \times \sqrt{\frac{1}{n_1}+\frac{1}{n_2}}}$$

follows a t distribution with (n_1+n_2-2) degrees of freedom. SE_i is the standard error of the coefficient.

Discussion and Conclusion

The overall goal of this study is to further illuminate the effects of different privacy assurance mechanisms on consumers' privacy concerns. We theorized that such effects were exhibited through the mediation by perceived control, and developed arguments in support of the moderating effects of self-construal. The evidence from this study provides empirical support that perceived control is one of the key factors which provide higher degree of explanation for privacy concern. Perceived control can be shaped by providing consumers with personal control through privacy-enhancing technology, proxy control through industry self-regulation and government legislation. With the recognition of the diversity of users, this study generates further insights into the issue of how privacy concerns could be alleviated through different mechanisms for different individuals.

Our results demonstrate the utility of the self-construal construct for predicting individuals' control perceptions of their personal information. We found that consumers who value independent-self are more personally agentic and hence prefer to retain personal control through technology-based mechanisms. But the more people believe that their surroundings in terms of powerful others that are vital, influential and liable, the more they prefer to retain proxy control through industry self-regulation and government legislation. The results indicate that, with the rapid advancement of ubiquitous computing technology and social conditions, the availability of diverse privacy assurance approaches to accommodate the interests of each individual or broad group of users would be very important.

There are several limitations in this study that present useful opportunities for further research. First, this study was conducted in Singapore where people are acculturated with both Western and Eastern social beliefs and values. Thus, care must be taken when generalizing these findings to consumers in other social and cultural environments. It would be worthwhile to replicate the study in cultures that either are more diverse (e.g., U.S.A.) or more homogeneous (e.g., Japan). Second, we employed a manipulation of privacy-enhancing technology that is simple but commonly used, i.e., allowing consumers to turn off their LBS. As technology advances, more options for personal control would naturally become available to consumers of LBS. For example, consumers may have options to transmit only partial or delayed location information to LBS providers. Future research can investigate whether partially restricting the flow of personal information to LBS providers yields the same impact as totally stopping the flow of personal information in terms of raising perceived control.

Finally, although this study was conducted in an LBS context, the theoretical framework may be applicable to other contexts where technology advances have raised the specter of privacy concerns. For instance, there have been very rapid technology advances in sensor networks and surveillance systems which also involve the collection and use of large volumes of personal information of consumers. It will become increasingly important for these technology promoters and vendors to understand how to alleviate privacy concerns. The theoretical framework developed here can be tested in such other technology contexts to assess its applicability.

In conclusion, advances in technology will continue to produce new mobile services for consumers. While these new mobile services can potentially improve the way we work, live, and play, such improvements typically come with the negative consequences of losing information privacy. Using the groundwork laid in this study as a foundation, scholars can continue to pursue this line of research to make further progress on theoretical developments on the topic of information privacy.

References

ABI. 2004. Location Based Services Making a Humble Comeback Declares ABI Research. Allied Business Intelligence Inc. Retrieved April 16, 2007, http://www.directionsmag.com/press.releases/index.php?duty=Show&id=9222&trv=1.

Altman, I. "Privacy: A Conceptual Analysis," in: *Man-Environment Interactions: Evaluations and Applications: Part 2*, D.H. Carson (ed.), Environmental Design Research Association, Washington, DC, 1974, pp. 3-28.

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

Anuket, B. 2003. User Controlled Privacy Protection in Location-Based Services. Unpublished Master's Thesis, Department of Spatial Information Science and Engineering, University of Maine, Orono, ME. Retrieved April 16, 2007, http://library.umaine.edu/theses/pdf/BhaduriA2003.pdf.

Bagozzi, R.P., and Fornell, C. "Theoretical Concepts, Measurement, and Meaning," C. Fornell (ed.), Praeger Publishers, Westport, CT, 1982.

Bandura, A. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37) 1982, pp 122-147.

Banisar, D. "Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments," Electronic Privacy Information Centre, Washington, D.C.

Barnes, J.S. "Known by the Network: The Emergence of Location-Based Mobile Commerce," in: *Advances in Mobile Commerce Technologies*, E.-P. Lim and K. Siau (eds.), Idea Group Publishing, Hershey, PA, 2003, pp. 171-189.

Beinat, E. "Privacy and Location-based: Stating the Policies Clearly," *GeoInformatics*), September 2001, pp 14-17.

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

Beresford, R.A., and Stajano, F. "Location Privacy in Pervasive Computing," *IEEE Pervasive Computing* (1) 2003, pp 46-55.

Burkert, H. "Privacy-enhancing technologies: typology, critique, vision," in: *Technology and Privacy: the New Landscape*, P. Agre and M.Rotenberg (eds.), MIT Press, Cambridge, MA, 1997.

Carte, A.T., and Russell, J.C. "In Pursuit of Moderation: Nine Common Errors and Their Solutions," *MIS Quarterly* (27:3) 2003, pp 479-501.

Caudill, M.E., and Murphy, E.P. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing* (19:1) 2000, pp 7-19.

Culnan, M.J. "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing* (9), Spring 1995, pp 10-19.

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

Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp 323-342.

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

Duxbury, E.L., and Higgins, A.C. "Gender Differences in Work-Family Conflict," *Journal of Applied Psychology* (76:1) 1991, pp 60-74.

Escalas, J.E., and Bettman, J.R. "Self Construal, Reference Groups, and Brand Meaning," *Journal of Consumer Research* (32:Dec) 2005, pp 378-389.

Falk, R.F., and Miller, N.B. *A Primer for Soft Modeling* The University of Akron Press, Akron, Ohio, 1992.

FCC. 2004. Wireless Enhanced 911. Federal Communications Commission. Retrieved April 16, 2007, http://www.fcc.gov/911/enhanced/

Fischer-Hüber, S. *IT-Security and Privacy* Springer-Verlag, Berlin Heidelberg, 2000.

Foddy, W.H., and Finighan, W.R. "The concept of privacy from a symbolic interaction perspective," *Journal for the Theory of Social Behavior* (10:1) 1980, pp 1-17.

Gidari, A. "No 'L-Commerce' Without 'L-Privacy': Fair Location Information Practices for Mobile Commerce," in: *paper presented at L-Commerce 2000-The Location Services & GPS Technology Summit*, Washington, D.C., 2000.

Goodwin, C. "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing* (10:1) 1991, pp 149-166.

Hernandez, M., and Iyengar, S.S. "What Drives Whom? A Cultural Perspective on Human Agency," *Social Cognition* (19:3) 2001, pp 269-294.

Hong, Y.-Y., Morris, M., Chiu, C.Y., and Benet-Martinez, V. "Multicultural Minds: A Dynamic Constructivist Approach to Culture and Cognition," *American Psychologist* (55:July) 2000, pp 709–720.

Johnson, C.A. "Privacy as Personal Control," in: *Man-Environment Interactions: Evaluations and Applications: Part 2*, D.H. Carson (ed.), Environmental Design Research Association, Washington, D.C., 1974, pp. 83-100.

Junglas, I.A., and Waston, R.T. "U-Commerce: A Conceptual Extension of E-Commerce and M-Commerce," Proceedings of 24th Annual International Conferences on Information Systems (ICIS 2003), Seattle, United States, 2003b, pp. 667-677.

Langer, E.J. "The Illusion of Control," *Journal of Personality and Social Psychology* (32) 1975, pp 311-328.

Laufer, R.S., and Wolfe, M. "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues* (33) 1977, pp 22-41.

Levy, S. 2004. A Future With Nowhere to Hide? Newsweek (June 7 issue). Retrieved April 16, 2007, http://www.msnbc.msn.com/id/5086975/site/newsweek/.

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

Margulis, T.S. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2) 2003a, pp 243-261.

Margulis, T.S. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59:2) 2003b, pp 411-429.

Markus, H. "Self-schemata and processing information about the self," *Journal of Personality and Social Psychology* (35:August) 1977, pp 63-78.

Markus, H.R., and Kitayama, S. "Culture and the Self: Implications for Cognition, Emotion, and Motivation," *Psychological Review* (98:April) 1991, pp 224–253.

McKnight, D.H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3) 2002, pp 334-359.

McKnight, D.H., Cummings, L.L., and Chervany, N.L. "Initial Trust Formation in New Organizational Relationships," *Academy of Management Review* (23:3) 1998, pp 472-490.

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

Milne, G.R., and Boza, M.-E. "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1), Winter 1999, pp 5-24.

Milne, G.R., and Rohm, A. "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy and Marketing* (19:2) 2000, pp 238-249.

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

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

Orwell, G. *1984, San Diego: Harcourt Brace Jovanovich Publishers, 1984. Originally published as Nineteen Eighty-Four* Martin Secker & Warburg, London, 1949.

Palen, L., and Dourish, P. "Unpacking "privacy" for a networked world," Proceedings of the SIGCHI conference on Human factors in computing systems, ACM Press, Ft. Lauderdale, Fl., 2003, pp. 129-136.

Pavlou, P.A., and Gefen, D. "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research* (15:1) 2004, pp 37-59.

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

Rao, B., and Minakakis, L. "Evolution of Mobile Location-Based Services," *Communications of ACM* (46:12), December 2003, pp 61-65.

Reed, G.M., Taylor, S.E., and Kemeny, M.E. "Perceived Control and Psychological Adjustment in Gay Men with AIDS," *Journal of Applied Social Psychology* (23:10) 1993, pp 791-824.

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

Singelis, T.M. "The Measurement of Independent and Interdependent Self-Construals," *Personality and Social Psychology Bulletin* (20:October) 1994, pp 580-591.

Skinner, E.A. "A Guide to Constructs of Control," *Journal of Personality and Social Psychology* (71) 1996, pp 549-570.

Skinner, E.A., Chapman, M., and Baltes, P.B. "Control, Means-Ends, and Agency Believes: A New Conceptualization and its Measurement During Childhood," *Journal of Personality and Social Psychology* (54) 1988, pp 117-133.
Smith, H.J., Milberg, J.S., and Burke, J.S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp 167-196.
Spiro, W.G., and Houghteling, L.J. *The Dynamics of Law*, (2nd ed.) Harcourt Brace Jovanovich, New York, 1981.
Stanton, J.M.B.-F., J. L. "Effects of electronic performance monitoring on personal control, task satisfaction, and task performance," *Journal of Applied Psychology* (81) 1996, pp 738-745.
Stone, E.F., Gueutal, G.H., Gardner, D.G., and McClure, S. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* (68:3) 1983, pp 459-468.
Swire, P.P. "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," in: *Privacy and Self-Regulation in the Information Age*, W.M. Daley and L. Irving (eds.), Department of Commerce, U.S.A., Washington, D.C., 1997, pp. 3-19.
Tittle, C.R. *Sanctions and Social Deviance: The Question of Deterrence* Praeger, New York, 1980.
TRUSTe. 2004. TRUSTe Plugs into Wireless: TRUSTe's Wireless Advisory Committee Announces First Wireless Privacy Standards. Retrieved April 16, 2007, http://www.truste.org/articles/wireless_guidelines_0304.php
USC. 2007. Online World As Important to Internet Users as Real World? Center for the Digital Future, Annenberg School for Communication, University of Southern California. Retrieved April 16, 2007, http://www.digitalcenter.org/pdf/2007-Digital-Future-Report-Press-Release-112906.pdf.
Wallace, P., Hoffmann, A., Scuka, D., Blut, Z., and Barrow, K. *i-Mode Developer's Guide* Addison-Wesley, Boston, Mass, 2002.
Weisz, J.R., Rothbaum, F.M., and Blackburn, T.C. "Standing out and standing in: The psychology of control in America and Japan," *American Psychologist* (39:9) 1984, pp 955-969.
Westin, A.F. *Privacy and Freedom* Atheneum, New York, 1967.
WLIA "Draft WLIA Privacy Policy Standards (first version)," Wireless Location Industry Association.
Wold, H. "Soft Modeling: The Basic Design and Some Extensions," in: *Systems Under Indirect Observations: Part 2*, K.G. Joreskog and H. Wold (eds.), North-Holland, Amsterdam, 1982, pp. 1-54.
Xu, H., and Teo, H.H. "Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective," Proceedings of the Twenty-Fifth Annual International Conference on Information Systems (ICIS 2004), Washington, D. C., United States, 2004, pp. 793-806.
Yamaguchi, S. "Culture and Control Orientations," in: *The Handbook of Culture and Psychology*, D. Matsumoto (ed.), Oxford University Press, New York, 2001, pp. 223-243.
Zweig, D., and Webster, J. "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23) 2002, pp 605-633.

Appendix:

Item Loadings for Major Constructs

Privacy Concern (PCON)	
PCON1 (.74)	I am concerned that the company is collecting too much personal information about me.
PCON2 (.92)	I am concerned that the company may not take measures to prevent unauthorized access to my personal information.
PCON3 (.88)	I am concerned that the company may keep my personal information in a non-accurate manner in their database.
PCON4 (.91)	I am concerned that the company may share my personal information with other parties without getting my authorization.
PCON5 (.97)	Overall, I feel unsafe about providing personal information to the company to use the LBS service.
Perceived Control (PCTL)	
PCTL1 (.89)	How much control do you feel you have over the amount of your personal information collected by the company?
PCTL2 (.90)	How much control do you feel you have over who can get access your personal information?
PCTL3 (.76)	How much control do you feel you have over your personal information that has been released?
PCTL4 (.85)	How much control do you feel you have over how your personal information is being used by the company?
PCTL5 (.92)	Overall, how much in control do you feel you have over your personal information provided to the company?