December 2005

Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk

Heng Xu
National University of Singapore

Hock-Hai Teo
National University of Singapore

Bernard Tan
National University of Singapore

PREDICTING THE ADOPTION OF LOCATION-BASED SERVICES: THE ROLE OF TRUST AND PERCEIVED PRIVACY RISK

Heng Xu, Hock-Hai Teo, and Bernard C. Y. Tan
Department of Information Systems
National University of Singapore
Singapore
xuheng@comp.nus.edu.sg **teohh@comp.nus.edu.sg**
btan@comp.nus.edu.sg

Abstract

Location-based services (LBS) use positioning technology to provide individual users the capability of being constantly reachable and accessing network services while on the move. However, privacy concerns associated with the use of LBS may ultimately prevent consumers from gaining the convenience of anytime/anywhere personalized services. Understanding consumer's privacy concerns toward LBS is of increasing importance as mobile and positioning technologies develop and change with escalating speed. Drawing on the integrative social contract theory and the trust-risk model, we conducted an experiment study to examine the effects of LBS providers' interventions—third party privacy seals, P3P (Platform for Privacy Preferences Project) compliance, and device-based privacy enhancing features—on building consumer trust and reducing privacy risk. Results indicated that service providers' interventions including joining third party privacy seal programs and introducing device-based privacy enhancing features could increase consumers' trust beliefs and mitigate their privacy risk perceptions. However, the proposed P3P compliance did not have a direct impact on perceived privacy risk, influencing it only indirectly, through trust. The study reported here is novel to the extent that existing empirical research has not examined this complex set of interrelated issues in the L-commerce context. Implications for theory and practice are discussed, and suggestions for future research along the directions of this study are provided.

Keywords: Location-based services, L-commerce, privacy risk, trust

Introduction

Recently, the growing influence of location-based mobile commerce (L-commerce) has attracted significant attention. By bringing localization, personalization, and immediacy to users, emerging location-based services (LBS) applications have enormous potential for enhancing safety, utility, and mobility in our lives (Barnes 2003). According to the findings in a report from Allied Business Intelligence Inc. (ABI 2004), world LBS revenues are expected to increase from approximately US $500 million in 2004 to over US $3.6 billion by the end of the decade.

Unsurprisingly, the commercial potential and rapid growth of L-commerce have been accompanied by concerns regarding the collection and dissemination of consumer information by service providers and merchants. These concerns pertain to the confidentiality of accumulated consumer data and the potential risks that consumers experience over the possible breach of confidentiality (Beinat 200; Wallace et al. 2002). Location information often reveals the position of a person in real time, thus rendering the potential intrusion of privacy a more critical and acute concern. It was found that 24 percent of potential LBS users are seriously concerned about the privacy implications of disclosing their location together with other personal data (Beinat 2001). To the degree that privacy concern represents a major inhibiting factor in consumer's adoption of L-commerce, it is important

to respond to the call of "No L-commerce without L-privacy" (Gidari 2000) by identifying the mechanisms to reduce consumers' privacy risk perceptions.

The conceptual academic literature in consumer information privacy suggests that trust could play an important role in alleviating consumers' privacy risk perceptions (e.g., Caudill and Murphy 2000; Culnan and Bies 2003). Indeed, the privacy risk has been implicitly incorporated in the extant online trust literature. For instance, many trust researchers proposed various trust models in which the privacy policies and third party seals (e.g., BBBOnline and TRUSTe seal) are considered as the structural assurances built into a Web site that might affect trusting beliefs and trust related behaviors (e.g., Gefen et al. 2003; McKnight and Chervany 2002). However, the explicit involvement of privacy is frequently overlooked among these studies. Davison et al. (2003) feel it is "quite astonishing that a high proportion of the burgeoning literature on trust in the context of B2C [business-to-consumer] fails to control for privacy, fails to meaningfully consider it, or even completely overlooks it" (p. 344). This research, therefore, attempts to address this gap by integrating the trust literature into the theories of consumer information privacy to investigate the role of trust in reducing the privacy risk in the L-commerce context.

Drawing on the integrative social contract theory (Donaldson and Dunfee 1994, 1999) and trust literature (e.g., Jarvenpaa et al. 2000, McKnight and Chervany 2002), this study further proposes that building consumer trust and reducing privacy risk could be the products of several aspects of the LBS provider's interventions that are well within the control of the service provider. Some "weak" intervention mechanisms (i.e., market-driven and technology-driven mechanisms) are increasingly perceived as viable substitutes for "strong" intervention mechanisms (i.e., legally binding mechanisms) because legal mechanisms are usually more expensive to institute (Bakos and Dellarocas 2002; Pavlou and Gefen 2004). Accordingly, we focus on three popular weak mechanisms—specifically, third party privacy seals, P3P (Platform for Privacy Preferences Project) compliance, and device-based privacy enhancing features—as the trust building and privacy risk reduction strategies in the unclear and underdeveloped legal environment of L-commerce. In addition, by incorporating P3P compliance into the research model, the current study also addresses a debate in the privacy literature (Milne and Culnan 2002): *What is the appropriate role of P3P in assuring consumer privacy*? Although significant investments have been made in the development of P3P (Cranor 2002), there is much skepticism on the effectiveness of P3P in protecting consumer privacy from industry practice (Kaufman et al. 2002). To our best knowledge, few studies empirically test the relative effectiveness of P3P and hence we seek to address this void by investigating the extent to which P3P could alleviate privacy violation risks and build trust in the L-commerce context.

An experiment study was conducted in Singapore to examine the effects of three proposed interventions—third party privacy seals, P3P compliance, and device-based privacy enhancing features—on consumer trust beliefs and privacy risk perceptions. The study reported here is novel to the extent that existing empirical research has not examined this complex set of interrelated issues in the L-commerce context. The synthesis of privacy and trust literature streams may provide a rich understanding of the adoption of technologies that create personal vulnerabilities and, therefore, inform adoption research in the IS discipline. The findings are also potentially useful to privacy advocates, regulatory bodies, merchants, LBS providers, and device manufacturers to help shape or justify their decisions concerning L-commerce.

Theoretical Foundations and Hypotheses

The Integrative Social Contract Theory and Consumer Information Privacy

The conceptual academic literature in consumer privacy indicates that the integrative social contract theory (ISCT) is particularly appropriate for understanding the tensions between firms and consumers over information privacy (Caudill and Murphy 2000; Culnan 1995; Milne and Gordon 1993). ISCT posits that members of a given community or industry behave fairly if their practices are governed by *social contracts* (Donaldson and Dunfee 1994, 1999). In the context of information privacy, "a social contract is initiated, therefore, when there are expectations of social norms (i.e., generally understood obligations) that govern the behavior of those involved" (Caudill and Murphy 2000). When consumers provide personal information to a certain firm and the firm in turn offers some benefits to the consumer, one generally understood obligation accruing from entering into this social contract is that the firm will undertake the responsibility to manage the consumer's personal information properly (Caudill and Murphy 2000). This implied contract is considered breached if consumers are unaware that information is being collected, or if the firm divulges consumers' personal information to unauthorized parties, or if the firm uses consumers' personal information for other purposes without consumers' consent (Culnan 1995).

Thus, the social contract, dictating how the firm handles consumers' personal information, in an implicit form (*not* in an economic or a legal form), involves unspecified obligations, and requires consumers' trust on the firm's compliance to this social contract

(Caudill and Murphy 2000; Culnan and Bies 2003; Hoffman et al. 1999). The concept of social contract in the consumer privacy context means that consumers are willing to disclose personal information for certain benefits as long as they trust the firm that it would uphold its side of the social contract. Hence, the lack of consumer trust in customer-centric enterprises seems to be a critical barrier that hinders their efforts to collect personal information from consumers for the purpose of providing their services (Hoffman et al. 1999; McKnight and Chervany 2002). Consumer trust, therefore, may play an important role in reducing consumers' privacy risk perceptions.

Tapping the overwhelming privacy concern phenomenon in the e-service context, Featherman and Pavlou (2003) conceptualized perceived privacy risk as an important facet of perceived risk[1] and they generally defined it as the potential loss of control over personal information. In our context, following Featherman and Pavlou's definition, we defined perceived privacy risk as the expectation of losses associated with the release of personal information to the LBS provider. Since privacy risk is broadly regarded as the major inhibiting factor in the adoption of LBS (Beinat 2001; Gidari 2000; Wallace et al. 2002), we exclude *other* risk considerations (e.g., performance, financial, time, social, and psychological risks involved in using LBS) in this study. Rather, we explicitly focus on examining privacy risk involved in using LBS in that mobile communication and positioning technologies increasingly expand the ability for firms to collect, process, and exploit personal data and there is "no L-commerce without L-privacy" (Gidari 2000).

Trust, Privacy Risk, and Service Provider's Interventions

Trust is a crucial enabling factor in relations where there is uncertainty, interdependence, risk, and fear of opportunism (Mayer et al. 1995). In the context of e-commerce, because of the absence of proven guarantees that the e-vendor will not engage in harmful opportunistic behaviors, trust is crucial in helping consumers overcome their perceptions of uncertainty and risk (Jarvenpaa and Tractinsky 1999; McKnight and Chervany 2002). Trust, in this study, has been conceptualized as three specific beliefs that are utilized most often (e.g., McKnight et al. 2002; Pavlou and Gefen 2004): competence (ability of the trustee to do what the trustor needs), benevolence (trustee caring and motivation to act in the trustor's interests), and integrity (trustee honesty and promise keeping). To the extent that LBS are still in an early stage of diffusion when potential consumers do not yet have credible, meaningful information about, or have affective bonds with, the service providers, examining consumer trust is important because LBS providers need to engender sufficient trust to persuade first-time consumers to transact with them. According to McKnight et al. (2002), "the period during which a consumer visits and explores a vendor's Web site for the first time is clearly within the domain of initial trust" (p. 336). *Initial trust*, therefore, is the focus of this study and defined as the trust belief that a consumer holds toward an LBS provider during the period when she interacts with the service provider for the first time.

In McKnight and Chervany (2002), which tried to develop an initial trust formation model in the e-commerce context, *Web vendor interventions* are posited to have impacts on consumer trusting beliefs in the e-vendor. Web vendor interventions are defined as the actions a vendor may take to provide assurances to consumers about the vendor's site (McKnight and Chervany 2002). In the Internet context, these interventions could include privacy policy, third party privacy seals, interacting with customers, reputation building, links to other sites, and guarantees or other seals (McKnight and Chervany 2002). The interventions assure consumers that this particular vendor site is safe in spite of whatever deficiencies exist in the overall Web environment. "Over time, if such interventions become standard and actual practices, the overall Web may be widely perceived as a safer, more secure place, increasing institution-based trust" (McKnight and Chervany 2002, p. 51).

Following McKnight and Chervany, this study defines *the service provider privacy- and trust- related interventions* as the actions that a particular LBS provider may take to provide assurances to consumers about the service provider's efforts devoted to protect consumers' personal information. Since most permission-based LBS applications involve recruiting consumers by service registration or subscription via the Web channel, we included the trust-and privacy- related interventions covered by both Internet and LBS practices. In particular, this study examines three types of interventions: (1) third party privacy seals, (2) P3P compliance, and (3) device-based privacy enhancing features. The first two are the factors for which we draw on the interventions undertaken by the e-vendors in the Internet context. For the third, we draw on the intervention undertaken by the LBS provider in the LBS context. Although not an exhaustive list of all privacy- and trust- related interventions, the proposed three factors represent both popular market-driven institutional mechanisms (i.e., third party privacy seals), and technology-driven mechanisms (i.e., P3P compliance and device-based privacy enhancing features).

[1]Perceived risk is generally identified as having various facets (i.e., performance, financial, time, safety, social, and psychological loss) and all risk facets stem from performance risk (Cunningham 1967).

Third Party Privacy Seals

When applied to consumer privacy, ISCT suggests that a firm's collection of personal information is perceived to be fair when the consumer is vested with *voice* (Culnan and Bies 2003; Malhotra et al. 2004). In other words, consumers want to influence changes in a firm's policies that they find to be objectionable (Malhotra et al. 2004). Privacy seals of approval from third-parties (such as BBBOnline, Online Privacy Alliance, and TRUSTe) are essentially self-regulated institutional mechanisms where the consumer can be informed with the choices available regarding how the collected information is used, the safeguards in place to protect the information from loss, misuse, or alteration, and how the consumer can update or correct any inaccurate information. These seal programs should build consumers' trust beliefs toward the particular firm and reduce their privacy risk perceptions for two reasons. First, these institutional mechanisms could limit the firm's ability to behave in negative ways, allowing consumers to form and hold beliefs about expectations of positive outcomes (Johnson and Cullen 2002). As Gefen et al. (2003) explain, having a third party such as the reputable TRUSTe to vouch for a firm's trustworthiness should build trust in that such third party assurances have typically been one of the primary methods of building trust in business. Second, when violation occurs, these structures could provide mechanisms of voice and recourse for the betrayed (Johnson and Cullen 2002), which could create strong incentives for firms to refrain from opportunistic behavior and behave appropriately.[2] Empirical studies have shown that companies conforming to the privacy seal programs foster consumers' trust and confidence in revealing their personal information (e.g., Culnan and Armstrong 1999) and mitigate consumers' perceived privacy risks of disclosing their personal information (e.g., Xu and Teo 2004).

H1a: *The service provider's interventions with regard to joining third party privacy seal programs will reduce consumer's privacy risk perception.*

H1b: *The service provider's interventions with regard to joining third party privacy seal programs will increase consumer's trust belief.*

P3P Compliance

The Platform for Privacy Preferences Project (P3P)[3] is a protocol designed to provide a way for a Web site to encode its data-collection and data-use practices in a machine-readable format known as a *P3P policy* (Cranor 2002). P3P policies require the Web sites to use the P3P vocabulary to provide contact information for the legal entity making the representation of privacy statement, enumerate the types of data or data elements collected, explain how the data will be used, identify the data recipients, and include information about dispute resolution, about the Web address of a site's human-readable privacy policy, and about the way to opt out (Cranor 2002). Users could employ a P3P user agent (e.g., AT&T Privacy Bird) to evaluate whether an online company implements P3P-compliant privacy policy by configuring their privacy preferences using a series of check boxes (Cranor 2002). For example, users can choose to be notified, or not, when a site uses their information for whatever purposes. According to the level of agreement between the user's preferences and a Web site's policies, the Privacy Bird notifies the user by adjusting the representation of a small, cartoon-like bird icon situated peripherally in the browser's title bar.[4]

Privacy literature suggests that the factor of *awareness of privacy practices* could be used to address the bond of social contract between firms and consumers over information privacy (Malhotra et al. 2004). This awareness factor, referring to the degree to which a consumer is concerned about personal awareness of organizational information privacy practices (Malhotra et al. 2004), has been found to be associated with lower level of privacy risk perception (Phelps et al. 2000). Hence, a firm's P3P compliance might reduce the consumer's privacy risk perceptions through providing the transparency about how the firm used the consumer's personal information (Culnan and Bies 2003). The presence of the symbols notifying whether the site's privacy policies match consumer's personal privacy preferences should enhance the awareness of privacy practice and thus reduce privacy risk in that

[2]Taking TRUSTe as one example, any complaint raised against the licensees 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 United States (Benassi 1999).

[3]For details, see **http://www.w3.org/P3P/#what**.

[4]The cartoon-like bird icon displays a green "happy" bird icon at sites with P3P policies that match a user's privacy preferences, a red "angry" bird icon at sites with P3P policies that do not match a user's preferences, and a yellow "uncertain" bird icon at sites that do not have P3P encoded policies.

consumers could make sound decisions on whether to provide their personal information to the particular firm. Therefore, P3P is touted as reducing privacy risk perceptions by putting privacy policies where consumers can easily find them, explaining whether the policy differs from their preferences, and, most importantly, enabling consumers to act on what they see (Culnan and Bies 2003; Turner and Dasgupta 2003).

H2a: *The service provider's interventions with regard to P3P compliance will reduce consumer's privacy risk perception.*

P3P compliance should directly build consumer trust belief because it requires a firm to make a nontrivial investment of time and resources to implement and maintain P3P policy (Turner and Dasgupta 2003). This action should be interpreted as a signal that the firm is proactively addressing consumers' privacy concerns (Cranor 2002; Turner and Dasgupta 2003) and it will comply with the social contract by undertaking the responsibility to manage consumers' personal information properly. In other words, a particular LBS provider's P3P compliance may enable consumers to believe that the service provider cares about their information privacy needs (trusting belief—benevolence), and it is capable of protecting their personal information (trusting belief—competence).

H2b: *The service provider's interventions with regard to P3P compliance will increase consumer's trust belief.*

Device-Based Privacy Enhancing Features

To strengthen the bond of social contract between firms and consumers over information privacy, firms need to address the *data collection* issue in that marketers' collection of personal information would continue to be an important source of privacy concerns (Malhotra et al. 2004; Phelps et al. 2000). In the LBS context, the rapid development of mobile communication and device technologies provide the possibility of building privacy enhancing features into mobile devices. With a mobile device that supports the function of specifying privacy preferences for using LBS applications, mobile consumers are able to limit the amount of location information collected by the service providers in a timely fashion (Anuket 2003). Consumers can turn off the subscribed LBS just by clicking some buttons on their mobile devices anytime they want. Furthermore, device-based privacy enhancing features also allow consumers to control the degree of location information released to the service providers in space and time (Anuket 2003). For example, the user can specify that the service provider(s) can only send her a wireless advertising message if she is within 20 meters of those merchants, and/or with a time delay of 10 minutes within which the past locations of the subscriber may be pinpointed. These device-based privacy enhancing features could provide consumers with the capabilities to limit the amount of location information released to the service providers, and thus might reduce their privacy risk perceptions. Empirical evidence supported that perceptions of privacy invasion are lower when the individuals are provided with the technical features to control their personal information disclosure (Xu and Teo 2004; Zweig and Webster 2002).

H3a: *The service provider's interventions with regard to introducing device-based privacy enhancing features will reduce consumer's privacy risk perception.*

Introducing such device-based privacy-enhancing features, therefore, should directly build consumers' trust beliefs toward an LBS provider because of the nontrivial investment of time and resources made by the service provider to design and implement the device-based privacy-enhancing features. This action should be interpreted as a signal that the service provider is proactively addressing consumers' privacy concerns (Xu and Teo 2004) and it will comply with the social contract by undertaking the responsibility to manage consumers' personal information properly. In other words, a particular LBS provider's introduction of the privacy enhancing features to consumers may enable them to believe that the service provider cares about their information privacy needs (trusting belief—benevolence), and it is capable of protecting their personal information (trusting belief—competence).

H3b: *The service provider's interventions with regard to introducing device-based privacy enhancing features will increase consumer's trust belief.*

Trust, Privacy Risk, and Behavioral Intention

ISCT suggested that consumer trust may play an important role in reducing consumers' privacy risk perceptions (Caudill and Murphy 2000). The direct effect of trust on risk has been empirically supported in research on e-commerce (e.g., Jarvenpaa et

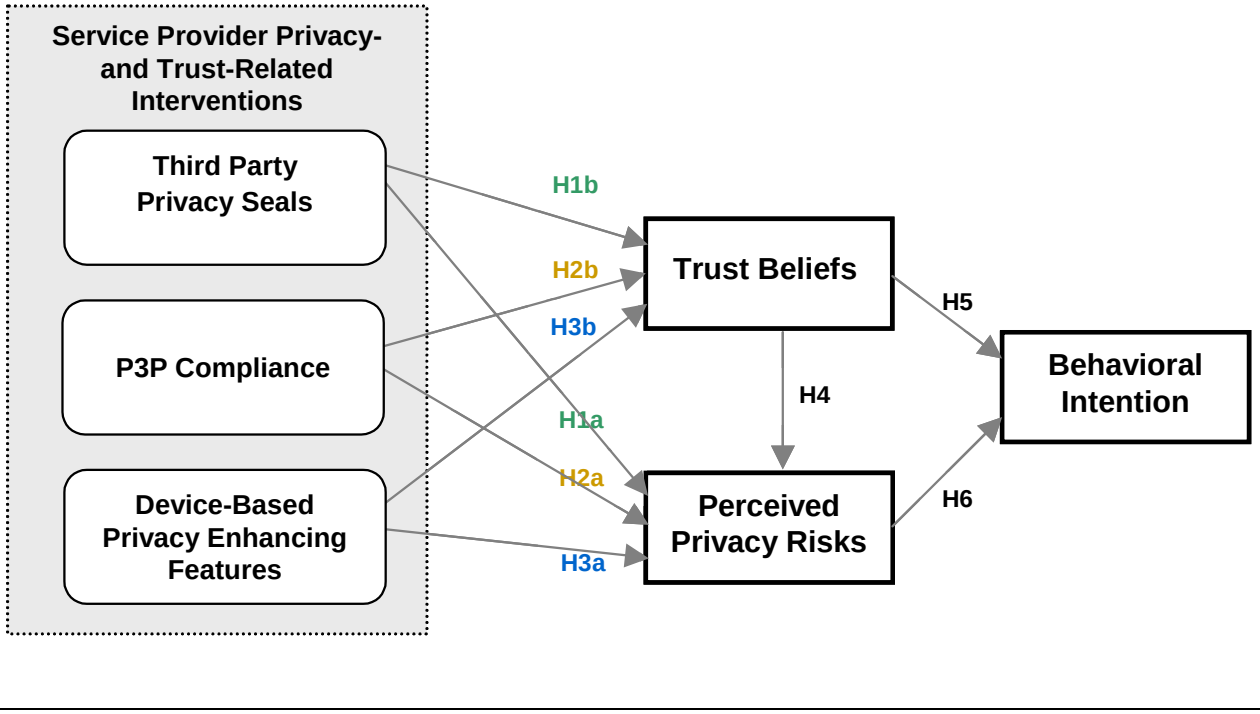


Figure 1. Research Model

al. 2000; Malhotra et al. 2004; Pavlou and Gefen 2004). Following the similar theoretical reasoning, when viewing perceived privacy risk as one facet of perceived risk, we expect that the more trust a consumer has in an LBS provider with regard to its information practice, the less likely she is to foresee the privacy risk associated with disclosing personal information to the service provider.

H4: *Trust beliefs will have a negative effect on privacy risk beliefs.*

Along the line of the theory of reasoned action (TRA) (Ajzen 1991), risk perception, viewed as the negative antecedent belief, and trust, viewed as the positive antecedent belief, are expected to affect a person's attitude that in turn influences a person's behavioral intention (Jarvenpaa et al. 2000). Empirical studies in e-commerce generally supported this expectation of the positive relationship between trust and behavioral intention (Gefen et al. 2003; Pavlou and Gefen 2004) and the negative relationship between risk perception and behavioral intention (Jarvenpaa and Tractinsky 1999; Pavlou and Gefen 2004). Accordingly, we expect that the same logic can be extended to our context.

H5: *Trust beliefs will have a positive effect on behavioral intention.*

H6: *Privacy risk beliefs will have a negative effect on behavioral intention.*

Figure 1 depicts the research model.

Control Variables

Prior research on adoption, consumer behavior, information privacy, and trust studies suggests that a number of additional factors should be included as control variables because of their potential influence on trust, privacy risk, and behavioral intention. They are *disposition to trust* (McKnight et al. 2002), *risk propensity* (Sitkin and Weingart 1995), *previous privacy experience* (Smith et al. 1996), *personal innovativeness* (Agarwal and Prasad 1998), and *coupon proneness* (Lichtenstein et al. 1990).

Research Method

An online field experiment was conducted. LBS in the experiment were operationalized as services offered to mobile phone users via short messaging services (SMS) based on the "cell-identification" technique employed by the network of telecom operators. One specific push-based LBS application—the mobile coupon (M-coupon) service was utilized as the scenario in this study because push-based LBS is more controversial in terms of consumers' concerns about privacy and authentication (Wallace et al. 2002). The M-coupon service usually involves recruiting customers by service registration and interest subscription: customers can register their mobile phone numbers and subscribe to a list of merchants who provide M-coupon services, based on their interests and preferred period of time for receiving coupons. Profiling information is then used to target the subscribers and their mobile phones will be sent related promotional information when they appear within the vicinity of the merchants.

Measures

As far as possible, constructs were adapted from existing measurement scales used in prior studies in adoption, information privacy, and trust in e-commerce to fit the LBS context where necessary. Appendix A summarizes the questions measuring each construct in this study.

Experiment Design and Manipulations

We used a 2 (with/without third party privacy seal) × 2 (with/without P3P compliance) × 2 (with/without device-based privacy enhancing feature) factorial experiment design. We varied the three privacy- and trust-related interventions—*third party privacy seal*, *P3P compliance*, and *device-based privacy enhancing features*—to construct multiple experiment scenarios. First, *third party privacy seal* was manipulated by providing a TRUSTe seal and a URL linked to the service provider's privacy policy on its Web site. A brief introduction explaining TRUSTe's mission was provided in the privacy policy. Second, *service provider's P3P compliance* was manipulated by asking the subjects to install a particular P3P user agent tool (i.e., AT&T Privacy Bird) to convey the fact that the service provider has complied with P3P policy for its information practices. An introduction explaining the purpose of using the AT&T Privacy Bird and how to use the Privacy Bird were provided to those subjects belonging to the P3P treatment group when they downloaded and installed the Privacy Bird. Finally, *device-based privacy enhancing feature* was manipulated by introducing a mobile device with an interactive graphical user interface for turning on/off the subscribed LBS anytime the user wants.

Subjects

A total of 176 responses were obtained among mobile phone users. We recruited the experiment subjects by posting announcements to a number of relevant forums or topics discussing mobile handsets and mobile applications on the major and reputable web portals in Singapore (i.e., Yahoo! Singapore Message Boards, Hardwarezone Forum, Can.com.sg Forum). 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. A lottery with three prizes (i.e., a 40G MP3 player, a speaker, and a cash prize) was included as incentive to participate in the experiment.[5] The invitees were assured that the results would be reported only in aggregate and that their anonymity would be assured. Specific demographic information is shown in Appendix B.

Experiment Procedure and Task

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. Then, as commonly used in marketing experiments that investigate consumer behavior, a cover story was provided to all subjects. They were told that one specific LBS application, the M-coupon service provided by Company A, would be soon introduced in the Singapore 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

[5]These three prizes included an iPod 40G MP3 player worth S$750, a JBL Creature speaker worth S$200, and a cash prize including S$100. These prices are framed in Singapore dollars. As of April 2005, one Singapore dollar = 61 U.S. cents.

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.[6] They were then asked to visit the site and other relevant information about the M-coupon service. The experimental system logged the accesses made by the subjects to all URLs to ensure that the subjects had actually viewed the manipulated condition. Finally, the subjects were asked to complete a post-session questionnaire regarding trust belief, perceived privacy risk, and behavioral intention in each specific scenario.

Data Analysis and Results

Control and Manipulation Check

Control checks were conducted by performing several one-way ANOVA tests to confirm that the random assignment of subjects to the eight experimental conditions was successful.[7] To ensure that study participants attended to their assigned intervention conditions, manipulation checks were performed. The manipulations on *device-based privacy enhancing features*, *third party seal*, and *P3P compliance* were checked against several true/false questions in the post-session questionnaire. Subjects who did not correctly answer these questions were dropped from the subsequent analyses. This resulted in 163 valid data sets.

PLS Analyses

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold (1982), was used for data analysis for three reasons. First, it is not contingent upon data having multivariate normal distributions and interval scales (Fornell and Bookstein 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 (Fornell and Bookstein 1982). Therefore, we believe that PLS is more suitable for this exploratory study.

Testing the Measurement Model

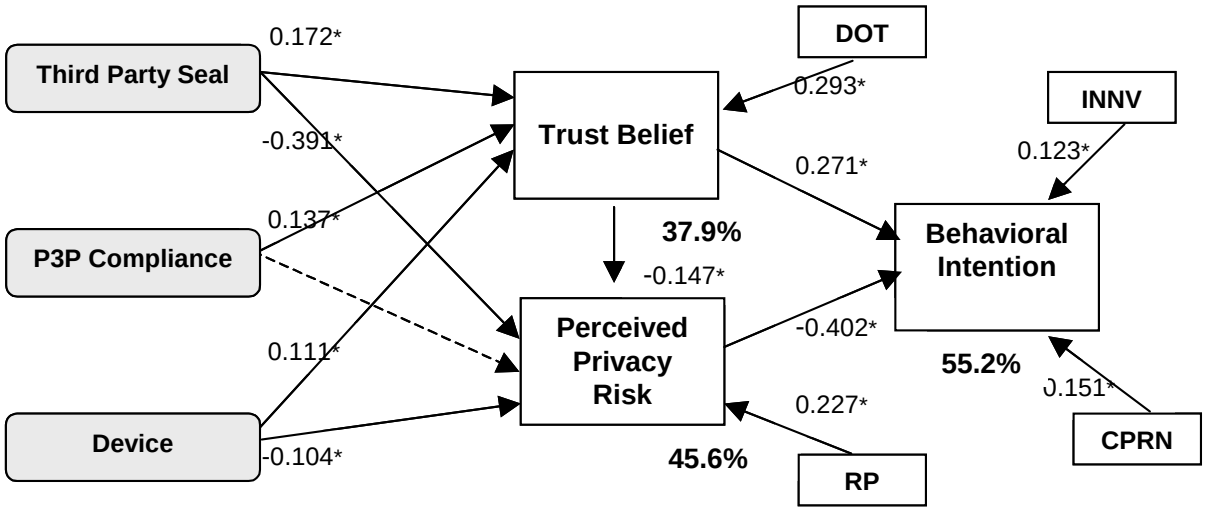
The measurement model was evaluated by examining the convergent and discriminant validity of the research instrument. Three tests are used to determine the convergent validity: reliability of questions, the composite reliability of constructs, and the average variance extracted by constructs. Appendix A presents the assessment of the measurement model. Given that all questions had reliability scores above 0.55 (Falk and Miller 1992), and most questions had reliability scores above 0.707, the questions measuring each construct had adequate reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7 while the average variances extracted for these constructs were all above 50 percent and the Cronbach's alphas were also all higher than 0.7. Hence, convergent validity was established. 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. Appendix C 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.

Testing the Structural Model

After establishing the validity of the measures, we tested the structural paths in the research model by applying bootstrapping technique in PLS. Figure 2 depicts the structural model inclusive of all significant control variables. Our structural model could explain 37.9 percent of the total variability of trust belief, 45.6 percent of perceived privacy risk, and 55.2 percent of the behavioral intention. The hypotheses were evaluated according to the size, sign, and significance of the path coefficients. With the exception of the path from P3P compliance to perceived privacy risk, all of the path coefficients shown in Figure 2 were with

[6]Due to space limitations, we did not provide the screen shot for the experiment details, which can be requested from the authors.

[7]There were no significant differences among the eight experimental conditions in terms of gender ($F = 1.616$, p = ns), age ($F = 0.733$, p = ns), education ($F = 0.656$, p = ns), income ($F = 1.271$, p = ns), mobile phone usage ($F = 0.800$, p = ns), mobile application usage ($F = 0.614$, p = ns), SMS usage ($F = 1.407$, p = ns), Internet usage ($F = 0.599$, p = ns), prior privacy-related knowledge ($F = 0.356$, p = ns), disposition to trust ($F = 0.483$, p = ns), risk propensity ($F = 0.601$, p = ns), personal innovativeness ($F = 1.334$, p = ns), and coupon proneness ($F = 0.208$, p = ns).



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

DOT = Disposition to Trust; RP = Risk Propensity; INNV = Personal Innovativeness; CPRN = Coupon Proneness

Figure 2. Results of PLS Analyses

the expected sign, and significant at the 0.05 level. Therefore, all of the hypotheses except H2a were supported. Among the control variables, disposition to trust had a significant effect on trust belief, and risk propensity significantly affected perceived privacy risk. Coupon proneness and personal innovativeness were shown to have significant effects on behavioral intention.

Discussions and Conclusions

Discussion of Findings

This study developed and empirically tested a model to investigate the roles of *trust belief* and *privacy risk belief* in the LBS usage adoption. Consistent with ISCT, the results show that consumers' trust beliefs could help mitigate their privacy risk perceptions and increase their intentions to disclose personal information for using LBS. Furthermore, this study shows that the service provider's interventions including joining third party privacy seal programs and introducing device-based privacy enhancing features could increase consumers' trust beliefs and mitigate their privacy risk perceptions. However, the proposed P3P compliance did not have a direct impact on perceived privacy risk, influencing it only indirectly, through trust.

A plausible explanation for this unexpected finding is that consumers' privacy risk perceptions are affected by the level of *enforcement* provided by the interventions (e.g., third party assurance). Although P3P provides users with the privacy optionsof *notice* (i.e., notifying users whether a Web site's privacy policy conflicts with their privacy preferences) and *choice* (i.e., allowing users to make sound decisions on whether to provide personal information based on the user agent's notice), P3P lacks the *enforcement* mechanism to ensure sites act according to their privacy policies. Hence, it seems that the use of P3P in the absence of risk assurance mechanisms shifts the onus primarily onto the individual user to protect herself. This may explain the insignificant effect of P3P compliance on perceived privacy risk in this study.

However, the other privacy enhancing technique (PET)—device-based privacy enhancing features, also lacking third party assurance mechanisms—was shown to have significant effects on perceived privacy risk. The possible explanation for this finding could be due to the underlying *control* mechanism as revealed in Xu and Teo (2004). With the aid of device-based privacy enhancing features to exert direct control over their personal information, consumers could control the amount of location information released to the service providers and hence they would especially feel greater autonomy (Yamaguchi 2001).

Consequently, the control assurance provided by the device-based privacy enhancing features would lead to lower privacy invasion risk (Xu and Teo 2004). In contrast, although P3P is touted as one of the PETs to "provide consumers with greater control over the disclosure of their personal information" (Culnan and Bies 2003), it actually provided little assurance of control to consumers. For instance, when the "angry" red bird icon appeared at those sites that do not match users' privacy preferences, the only choice offered to the users is either to give up their privacy needs to use the Web services *or* to give up their needs of using the Web services. Future research could be directed to further explore the relative effects of these two PETs (i.e., P3P and device-based privacy enhancing features) by integrating the psychological control theories with the trust-risk framework.

Examining the relative importance of institution-based (i.e., third party seals) versus technology-based interventions (i.e., P3P compliance and device) in building trust and reducing privacy risk, we found that third party seal programs have by far the most influence. There is perhaps nothing surprising in this finding since institution-based mechanisms especially the structural assurance through third party guarantees, have been consistently found to have positive impacts on the development of trust in e-vendors (e.g., Gefen et al. 2003; Pavlou and Gefen 2004). This result echoes and supports the current trends in the United States for a self-regulatory approach to rely on the private sectors to add structural assurances (e.g., TRUSTe privacy seal and other trade association membership). Given their importance in building trust and mitigating privacy risk, institution-based mechanisms warrant further research.

Limitations and Future Research

Although the data generally supported the proposed model, we need to mention some characteristics of our study that may limit the ability to generalize from these results. First, the subjects were recruited from a number of relevant forums or topics on three major web portals in Singapore. Thus our sample comprised a subpopulation of potential mobile consumers (i.e., those mobile users who were also interested in participating in the online forums discussing mobile handsets and mobile applications). Further research using our method should be conducted among different groups of constituents with different demographics on the mobile market. Second, this study was conducted in Singapore; therefore, care must be taken when generalizing these findings to consumers in other social, economic, and cultural environments, and future research should attempt to replicate this study in other countries. As privacy attitudes and trust beliefs may be culturally dependent (Johnson and Cullen 2002; Milberg et al. 2000), this study might limit the generalizability of our results to the Asia-Pacific context. Finally, the scenario used in the study represents an over-simplification of LBS, which may limit the generalizability of our findings. Future work could also be directed to look into the applicability of our findings to different LBS applications. The challenge is to continue improving the experiment design, which could be a scenario where consumers are, in reality, on the move. Field research along the directions of this study could certainly contribute toward fostering the acceptance of LBS.

Implication and Conclusion

Our research model was originally developed to reflect recent changes in an individual's views on the privacy invasion risk because of the rapid development of wireless network and positioning technologies. Nevertheless, it is important to note that this model is strongly rooted in a general conceptual framework drawing on ISCT. Therefore, under an assumption that the essence of privacy concerns lies in a social contract, our model is likely to be applicable to a variety of privacy-related contexts. Our posited predictors explain 55.2 percent of the variance in the behavioral intention, suggesting that the ISCT and trust theories serve as a useful theoretical foundation in the information privacy context. Additionally, the present study highlights the roles of service providers' trust- and privacy- related interventions in building trust and mitigating privacy risk, which have important implications for the LBS industry where the legal environment is not yet sound. Our initial finding that P3P could not have a direct impact on perceived privacy risk, influencing it only indirectly through trust, suggests the need for future studies to understand the nature and effects of P3P fully. For instance, it is very possible that P3P might moderate the relationship between the third party seal and perceived privacy risk. In other words, although P3P did not have a direct impact on mitigating privacy risk, it might have an impact on reducing perceived privacy risks in conjunction with third party seal. In that the objective of the study was to explore the relative effectiveness of the three proposed service providers' interventions on building trust and mitigating privacy risk, examining the interaction effects of these service providers' interventions was beyond the scope of this study.

From a practical perspective, this study shows that privacy invasion risk and trust belief are the important factors in the interaction of the consumer with an LBS provider. In this aspect, this study provides some insights into the different approaches that could be used by an LBS provider to build consumer trust and reduce privacy risk perceptions. First, this study shows that incorporating institution-based structural assurances (e.g., third party privacy seals) into the management of information practices is an important

method for increasing consumers' trust beliefs and reducing their privacy risk perceptions. Second, it is important for LBS providers to collaborate with mobile device manufacturers to develop improved devices with user-friendly interfaces for specifying privacy preferences to counter privacy risk perceptions and enhance consumer trust. Third, although the service provider's P3P compliance could enhance consumer trust, it does not provide a means for reassuring that the service provider's information practices comply with certain accepted and required standards, which is what the third party privacy seal programs attempt to do. Thus, another important factor in reducing consumers' privacy risk perceptions will be the extent to which the service provider could shape perception and engender belief that its privacy policy accurately reflects the service provider's information collection and using practices.

Trust could play a primary role in promoting the use of LBS applications, especially in the absence of familiarity with L-commerce phenomenon and well-established legal resources. Having highlighted the roles of some market-driven and technology-driven mechanisms in trust building and privacy risk reduction, this study provides preliminary empirical support to understand the privacy issues from the social contract perspective. Using the groundwork laid down in this study, future research along various possible directions could contribute significantly to extending our theoretical understanding and practical ability to foster the acceptance of L-commerce.

References

ABI. "Location Based Services Making a Humble Comeback, Declares ABI Research," Allied Business Intelligence Inc., April 27, 2004 (available online at **http://www.abiresearch.com/home.jsp**).

Agarwal, R., and Prasad, J. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," *Information Systems Research* (9:2), 1998, pp. 204-215.

Ajzen, I. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50), 1991, pp. 179-211.

Anuket, B. *User Controlled Privacy Protection in Location-Based Services*, Unpublished Master's Thesis, University of Maine, Orono, ME, 2003.

Bakos, Y., and Dellarocas, C. "Cooperation without Enforcement? A Comparative Analysis of Litigation and Online Reputation as Quality Assurance Mechanisms," in *Proceedings of 23rd International Conference on Information Systems*, L. Applegate, R. Galliers, and J. I. DeGross (Eds.), Barcelona, Spain, 2002, pp. 127-142.

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 (available online at **http://www.geodan.nl/nl/geodan/nieuws/pdf/GeoInformatics_sept_2001_LBSandPrivacy.pdf**).

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

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.

Cranor, F. L. *Web privacy with P3P*, O'Reilly, Sebastopol, CA, 2002.

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), January-February 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.

Cunningham, S. "The Major Dimensions of Perceived Risk," in *Risk Taking and Information Handling in Consumer Behavior*, D. F. Cox (Ed.), Harvard University Press, Cambridge, MA, 1967.

Davison, M. R., Clarke, R., Smith, H. J., Langford, D., and Kuo, F-Y. "Information Privacy in a Globally Networked Society: Implications for IS Research," *Communications of the Association for Information Systems* (12), 2003, pp. 341-365.

Donaldson, T., and Dunfee, W. T. *Ties that Bind: A Social Contracts Approach to Business Ethics*, Harvard Business School Press, Cambridge, MA, 1999.

Donaldson, T., and Dunfee, W. T. "Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory," *Academy of Management Review* (19), April 1994, pp. 252-284.

Donthu, N., and Gilliland, D. "The Infomercial Shopper," *Journal of Advertising Research* (36), March-April 1996, pp. 69-76.

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

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

Fornell, C., and Bookstein, F. L. "Two Structrual Equation Models: LISREL and PLS Applied to Customer Exit-Voice Theory," *Journal of Marketing Research* (19:11), 1982, pp. 440-452.

Gefen, D., Karahanna, E., and Straub, D. W. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), March 2003, pp. 51-90.

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

Hoffman, D. L., Novak, T., and Peralta, M. A. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2), 1999, pp. 129-139.

Jarvenpaa, S. L., and Tractinsky, N. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer Mediated Communications* (5:2), 1999, pp. 1-35.

Jarvenpaa, S. L., Tractinsky, N., and Vitale, M. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:12), 2000, pp. 45-71.

Johnson, L. J., and Cullen, B. J. "Trust in Cross-Cultural Relationships," in *The Blackwell Handbook of Cross-Cultural Management*, M. J. Gannon and K. L. Newman (Eds.), Blackwell, Oxford, UK, 2002, pp. 335-360.

Kaufman, J. H., Edlund, S., Ford, A. D., and Powers, C. "Ubiquitous WWW: The Social Contract Core," *Proceeding of the 11th International Conference on World Wide Web*, Honolulu, HI, ACM Press, 2002, pp. 210-220 (available online through ACM Digital Library, **http://portal.acm.org/**).

Lichtenstein, D. R., Netemeyer, G. R., and Burton, S. "Distinguishing Coupon Proneness from Value Consciousness: An Acquisition-Transaction Utility Theory Perspective," *Journal of Marketing* (54), July 1990, pp. 54-67.

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

Mayer, R. C., Davis, J. H., and Schoorman, F. D. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), 1995, pp. 709-734.

McKnight, D. H., and Chervany, N. L. "What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology," *International Journal of Electronic Commerce* (6:2), 2002, pp. 35-59.

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.

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 Culnan, J. M. "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U. S. Web Surveys," *The Information Society* (18), 2002, pp. 345-359.

Milne, G. R., and Gordon, E. M. "Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework," *Journal of Public Policy and Marketing* (12:2), Fall 1993, pp. 206-215.

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

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.

Sitkin, S. B., and Weingart, L. R. "Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity," *Academy of Management Journal* (38:6), 1995, pp. 1573-1592.

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.

Turner, C. E., and Dasgupta, S. "Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals," *Information Systems Management* (Winter), 2003, pp. 8-18.

Venkatesh, V., Morris, G. M., Davis, G. B., and Davis, F. D. "User Acceptance of Information Technology: Toward A Unified View," *MIS Quarterly* (27:3), 2003, pp. 425-478.

Wallace, P., Hoffmann, A., Scuka, D., Blut, Z., and Barrow, K. *i-Mode Developer's Guide*, Addison-Wesley, Boston, 2002.

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," in *Proceedings of the 25th Annual International Conference on Information Systems*, R. Agarwal, L. Kirsch, and J. I. DeGross (Eds.), Washington, DC, December 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 A. Psychometric Properties of the Measurement Model

Measures of Constructs and Sources	LD	CR	CA	AVE
Trust Belief (TRUST): (Jarvenpaa et al. 2000; McKnight et al. 2002)		0. 927	0. 894	0. 762
Company A…				
is competent and effective in handling my personal information that I would provide.	0. 735			
would keep my best interests in mind when dealing with my personal information.	0. 890			
would fulfill its promises related to customers' personal information.	0. 930			
is in general trustworthy regarding the usage of my personal information.	0. 922			
Perceived Privacy Risk(RISK): (Jarvenpaa et al. 2000; Malhotra et al. 2004)		0. 913	0. 882	0. 725
There would be too much uncertainty associated with giving my personal information to Company A.	0. 814			
Providing Company A with my personal information would involve many unexpected problems.	0. 884			
It would be risky to disclose my personal information to Company A.	0. 885			
There would be high potential for loss with disclosing my personal information to Company A.	0. 821			
Intention to Use LBS (INT): (Venkatesh et al. 2003)		0. 970	0. 952	0. 914
I am very likely to disclose my personal information to use M-coupon service.	0. 934			
I predict I would provide my personal information to Company A to use M-coupon service.	0. 966			
I intend to disclose my personal information to use M-coupon service.	0. 968			
Personal Innovativeness (INNV): (Agarwal and Prasad 1998)		0. 888	0. 819	0. 669
If I heard about a new information technology, I would look for ways to experiment with it.	0. 905			
Among my peers, I am usually the first to try out new information technologies.	0. 855			
In general, I am hesitant to try out new information technologies.	0. 600			
I like to experiment with new information technologies.	0. 876			
Coupon Proneness (CPRN): (Lichtenstein et al. 1990)		0. 872	0. 818	0. 633
I enjoy collecting coupons.	0. 782			
Beyond the money I save, redeeming coupons gives me a sense of joy.	0. 866			
I enjoy using coupons, regardless of the amount I save by doing so.	0. 835			
I am more likely to buy brands for which I have a coupon.	0. 687			
Disposition to Trust (DOT): (McKnight et al. 2002)		0. 863	0. 804	0. 613
Most of the time, people care enough to try to be helpful, rather than just looking out for themselves.	0. 777			
Most people are honest in their dealings with others.	0. 879			
Most professionals are very knowledgeable in their chosen field.	0. 782			
I usually trust people until they give me a reason not to trust them.	0. 680			
Risk Propensity (RP): (Donthu and Gilliland 1996)		0. 871	0. 783	0. 693
I would rather be safe than sorry.	0. 820			
I am cautious in trying new/different products.	0. 827			
I avoid risky things.	0. 850			
Previous Privacy Experience (**PPRV**): (Smith et al. 1996)		0. 874	0. 791	0. 700
How often have you personally experienced incidents whereby your personal information was used by some service provider or e-commerce website without your authorization?	0. 842			
How often have you personally been the victim of what you felt was an improper invasion of privacy?	0. 908			
How much have you heard or read during the last year about the use and potential misuse of consumer's personal information without consumer's authorization by some service provider or e-commerce website?	0. 752			

(**LD**: Loading, **CR:** Composite Reliability; **CA:** Cronbach's Alpha; **AVE:** Average Variance Extracted)

Appendix B. Respondent Profile (n = 163)

Variables	Category	Frequency	Variables	Category	Frequency
Gender	Male Female	90 (55.2%) 73 (44.8%)	**Personal Annual Income**	< S$24,000 S$24,001-S$48,000 S$48,001- S$60,000 S$60,001- S$72,000 >S$72,001 Undisclosed	34 (20.8%) 65 (39.9%) 40 (24.5%) 12 (7.4%) 8 (5.0%) 4 (2.4%)
Education	High School Diploma Bachelor Master	4 (2.5%) 59 (36.2%) 74 (45.3%) 26 (16.0%)			
Age	20-24 25-29 30-34 35-39 40-49	33 (20.2%) 65 (39.9%) 28 (17.2%) 21 (12.9%) 16 (9.8%)	**Internet Usage**	One time each week Several times each week Once per day Several times each day	3 (1.8%) 7 (4.3%) 19 (11.7%) 134 (82.2%)
Mobile Phone Ownership	Less than12 months 12 to 24 months 25 to 36 months More than 3 years	21 (12.9%) 22 (13.5%) 19 (11.6%) 101 (62.0%)	**Mobile Application Usage for the past 6 months**	Never Below 10 times 10 to 29 times 30 to 49 times 50 times and above	40 (24.5%) 85 (52.1%) 27 (16.6%) 5 (3.1%) 6 (3.7%)
Prior Privacy-Related Knowledge	Know TRUSTe Know Cookie Know SSL Know P3P	85 (52.1%) 149 (91.4%) 107 (65.6%) 23 (14.1%)	**Monthly SMS Usage**	Below 50 messages 51 to 99 messages 100 to 300 messages More than 300 messages	33 (20.2%) 37 (22.7%) 51 (31.3%) 42 (25.8%)

Appendix C. Discriminant Validity of Constructs

	INT	TRUST	RISK	DOT	RP	PPRV	CPRN	INNV
INT	0. 956							
TRUST	0. 478	0. 873						
RISK	-0. 592	-0. 310	0. 852					
DOT	0. 161	0. 311	-0. 057	0. 783				
RP	-0. 232	-0. 061	0. 185	-0. 077	0. 832			
PPRV	0. 038	0. 003	0. 206	-0. 132	-0. 059	0. 836		
CPRN	0. 361	0. 329	-0. 361	0. 187	-0. 096	0. 009	0. 795	
INNV	0. 270	0. 258	0. 095	0. 300	-0. 179	-0. 013	0. 168	0. 818

Note: Diagonal elements are the square root of average variance extracted (AVE), which, for discriminant validity, should be larger than interconstruct correlations (off-diagonal elements).