The Role of Push–Pull Technology in Privacy Calculus: The Case of Location-Based Services

HENG XU, HOCK-HAI TEO, BERNARD C.Y. TAN, AND RITU AGARWAL

HENG XU is an Assistant Professor of Information Sciences and Technology (IST) at Pennsylvania State University, where she directs the Privacy Assurance Lab (PAL), an interdisciplinary research group working on a diverse set of projects related to understanding and assuring information privacy. She is also the associate director of the Center for Cyber-Security, Information Privacy, and Trust at the College of IST. She received her Ph.D. in information systems in December 2005. Her Ph.D. dissertation, "Privacy Considerations in the Adoption of Location-Based Services," was named runner-up in the 2006 ACM SIGMIS Doctoral Dissertation Award Competition. Her research interests include information privacy and security, human–computer interaction, and technology innovation adoption. Her work has been published or accepted for publication in the *Journal of Management Information Systems, DATA BASE for Advances in Information Systems, Electronic Commerce Research and Applications, Electronic Markets,* and *International Journal of Mobile Communications.*

HOCK-HAI TEO is an Associate Professor of Information Systems and Head of the Department of Information Systems at the School of Computing, National University of Singapore. Prior to his current appointment as Head of Department, Dr. Teo served as Vice Dean, Corporate Communications from August 2007 to August 2008. His research interests are in the areas of IT innovation adoption, assimilation and effects, information privacy, electronic market institutions, and virtual communities. Dr. Teo's research has been published in journals such as the *Journal of Management Information Systems, MIS Quarterly, ACM Transactions on Computer–Human Interactions, IEEE Transactions on Engineering Management, International Journal of Human–Computer Studies,* and *Information and Management* and has been presented at numerous international conferences, including the *International Conference on Information Systems.* He is currently serving on the editorial board of *Information Systems Research, MIS Quarterly,* and *IEEE Transactions on Engineering Management.* Dr. Teo is also the senior editor of the *DATA BASE for Advances in Information Systems.* He won the *MIS Quarterly* Reviewer of the Year (2004) award.

BERNARD C.Y. TAN is Professor of Information Systems and Associate Provost at the National University of Singapore (NUS). He received his Ph.D. in information systems from NUS. He has been a Visiting Scholar in the Graduate School of Business at Stanford University and the Terry College of Business at the University of Georgia. He is the President of the Association for Information Systems. His current research interests are knowledge management, virtual communities, and information privacy. His research has been published in journals such as *ACM Transactions on Computer–Human Interaction, ACM Transactions on Information Systems, IEEE Transactions on Engineering*

Journal of Management Information Systems / Winter 2009–10, Vol. 26, No. 3, pp. 135–173.

0742–1222 / 2010 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222260305

Management, Information Systems Research, Journal of Management Information Systems, Journal of the AIS, Management Science, and *MIS Quarterly.* He has served on the editorial boards of *MIS Quarterly* (senior editor), *Journal of the AIS* (senior editor), *IEEE Transactions on Engineering Management* (department editor), *Management Science,* and *Journal of Management Information Systems.*

Ritu Agarwal is a Professor and Robert H. Smith Dean's Chair of Information Systems at the Robert H. Smith School of Business, University of Maryland, College Park. She is also the founder and director of the Center for Health Information and Decision Systems at the Smith School. Her current research focuses on the use of IT in health-care settings, technology-enabled transformations in various industrial sectors, and consumer behavior in technology-mediated settings. Dr. Agarwal has published more than 75 papers on IT management topics in *Information Systems Research, Journal of Management Information Systems, MIS Quarterly, Management Science, Communications of the ACM, Decision Sciences, IEEE Transactions,* and *Decision Support Systems.* She has served as a senior editor for *MIS Quarterly* and *Information Systems Research.*

Abstract: Location-based services (LBS) use positioning technologies to provide individual users with reachability and accessibility that would otherwise not be available in the conventional commercial realm. While LBS confer greater connectivity and personalization on consumers, they also threaten users' information privacy through granular tracking of their preferences, behaviors, and identity. To address privacy concerns in the LBS context, this study extends the privacy calculus model to explore the role of information delivery mechanisms (pull and push) in the efficacy of three privacy intervention approaches (compensation, industry self-regulation, and government regulation) in influencing individual privacy decision making. The research model was tested using data gathered from 528 respondents through a quasi-experimental survey method. Structural equations modeling using partial least squares validated the instrument and the proposed model. Results suggest that the effects of the three privacy intervention approaches on an individual's privacy calculus vary based on the type of information delivery mechanism (pull and push). Results suggest that providing financial compensation for push-based LBS is more important than it is for pull-based LBS. Moreover, this study shows that privacy advocates and government legislators should not treat all types of LBS as undifferentiated but could instead specifically target certain types of services.

Key words and phrases: compensation, distributive justice, government regulation, industry self-regulation, information delivery mechanisms, location-based services (LBS), privacy calculus, procedural justice.

In the new wireless era, we can go anywhere and still maintain intimate contact with our work, our loved ones and our real-time sports scores. To see how this might work, check out Worktrack, a tracking system used by a company in the heating and air-conditioning business. Workers have cell phones equipped with Global Positioning System (GPS) that pinpoint their locations to computers in the back office. Their peregrinations can be checked against the "Geo Fence" that employers draw up, circumscribing the area where their work is situated.

> If they're not in the right working area, a notification will be sent to the back office. Worktrack is only one of many services devoted to tracking humans. Parents use similar schemes to make sure their kids are safe; our buddies use location-based "friend-finder" services to make social lives more efficient and pleasurable. Sooner or later, the persistent connectedness may well lead us toward a future where our cell phones tag and track us like FedEx packages. Here's a new battle cry for the wireless era: Don't Geo-Fence me in. [45]

Recent advances in mobile communication technologies are spearheading the next generation of itinerant e-commerce applications. The development of positioning technologies, such as GPS and cellular triangulation techniques, has not only provided consumers with unprecedented accessibility to network services while on the move, but also enabled the localization of services [8, 61]. In the literature, commercial location-sensitive applications and services that utilize geographical positioning information to provide value-added services are generally termed *location-based services* (LBS) [6, 8]. These services include emergency and safety-related services, location-sensitive billing, entertainment, navigation, asset tracking, directory and city guides, traffic updates, and location-based advertising [6]. By bringing locatability and personalization to users, emerging LBS applications potentially offer significant value by placing information, transactions, and entertainment in a location-specific context [8].

The growth trajectory of LBS is striking. According to a recent report from Allied Business Intelligence Inc., LBS revenues are expected to reach an annual global total of $13.3 billion by 2013, up from an estimated $515 million during 2007 [53]. Unsurprisingly, the commercial potential and rapid growth of LBS have been accompanied by concerns over the collection and dissemination of personal information by service providers and merchants. The concerns center on the confidentiality of accumulated consumer location data and other personal information, and the potential risks that consumers experience over the possible breach of confidentiality [41]. Location information often reveals the position of a person in real time, rendering the potential intrusion of privacy a critical and acute concern. Indeed, the Big Brother imagery [55] looms in the popular press where LBS are discussed [45]. To the degree that privacy concerns represent a major inhibiting factor in the adoption of LBS [41], we respond to the call of *no LBS without L-privacy* [34] by theoretically developing and empirically testing a model that addresses privacy issues in the context of LBS usage.

Individual privacy decision making is often described in terms of a *calculus* where personal information is given in return for certain benefits [44, 67]. We extend the privacy calculus framework by modeling three privacy intervention approaches (compensation, industry self-regulation, and government regulation) as important variables that exert direct effects on the privacy calculus. We theoretically link these privacy intervention approaches with two types of justice provisions, and argue that justice provisions, through the forms of compensation, industry self-regulation, and government regulation, influence the outcomes of the privacy calculus. We manipulate these privacy intervention approaches in a quasi-experimental survey study and examine their effects on the privacy calculus in two types of information delivery mechanisms. In particular, we study pull-based LBS, where consumers initiate requests

for information and services based on their locations, and push-based LBS, where positioning technologies autonomously and proactively push information and services to consumers' mobile devices based on their locations. We propose that the effects of the three privacy intervention approaches on an individual's privacy calculus vary based on the type of information delivery mechanism (pull or push).

The current study contributes to existing privacy literature in several important ways. First, in contrast to most privacy research that was conducted in the Internet context (e.g., [29, 48]), we develop and empirically test a research model in an understudied LBS context. Such a new ubiquitous computing environment offers consumers relatively higher levels of reachability and accessibility over the communication and exchange process than has been the case with the Internet [39]. Accordingly, privacy concerns in such contexts become particularly salient as merchants and service providers may have access to a large volume of potentially sensitive consumer information. Second, following the call by Chan et al. [15], this research explores the role of one particular technological attribute (information delivery mechanisms) in the theoretical development surrounding privacy. Particularly, we attempt to show if and to what extent the effects of privacy intervention strategies on privacy calculus are dependent upon different information delivery mechanisms (pull and push). Third, although scholarly efforts have been devoted to identify the dimensions of justice in the information privacy context (e.g., [27, 43, 66]), few studies have identified approaches to justice provision and examined the efficacies of these approaches. To address this gap, we theoretically differentiate three privacy intervention approaches (compensation, industry self-regulation, and government regulation) based on the types of justice components they provide.

Theoretical Foundations

THE CALCULUS PERSPECTIVE OF INFORMATION PRIVACY interprets the individual's privacy interests as an exchange where individuals disclose their personal information in return for certain benefits. We extend this perspective by integrating it with justice theory to study the efficacy of three privacy intervention strategies (compensation, industry self-regulation, and government regulation) in influencing perceptions of privacy benefits/risks. By theoretically linking three privacy intervention approaches with two types of justice provisions, we propose that the conventional understanding of privacy as a calculus can be explained within the framework of justice theory: on one hand, consumers may evaluate the fairness of the distribution of outcomes, which includes the tangible consequences of the information disclosure to both themselves and firms; on the other hand, they may attend to and evaluate the fairness of the manner in which they were treated in the information exchange.

Using the Calculus Perspective to Understand Information Privacy

Information privacy refers to the ability of the individual to control the terms under which personal information is acquired and used [73]. Although ostensibly the no-

tion of privacy appears straightforward, there are a great many ways in which the literature in diverse fields such as law, marketing, political science, psychology, and social sciences has treated this concept [49, 67]. Within the robust body of research that attempts to understand the nature of consumer privacy, it has been found that the *calculus* perspective of privacy is "the most useful framework for analyzing contemporary consumer privacy concerns" [27, p. 326]. This calculus perspective is especially evident in empirical studies of consumer privacy concerns (e.g., [23, 29, 36, 38, 52]). According to these studies, consumers perform a risk–benefit analysis of all the factors related to a particular information disclosure situation in order to assess privacy concerns. In contrast to most prior research that was conducted to apply the privacy calculus framework in the direct marketing or conventional Web context, we empirically test and extend the calculus model in an understudied LBS context. In a context marked by ubiquity and uniqueness where individuals engage more devices and systems in a real-time fashion [39], privacy concerns become particularly salient as service providers may have access to a larger volume of potentially sensitive information. Thus, the use of LBS often demands that individuals be continually engaging in a dynamic adjustment process in which privacy risks are weighed against benefits of information disclosure, rendering the privacy calculus very significant and highly relevant in this context.

Consistent with the core ideas of privacy calculus, exchange theory [5] may further help predict how individuals make decisions regarding the disclosure of personal information [27]. This theory describes the utilitarian exchange as an interaction whereby goods are given in return for money or other goods [5, p. 36], which is considered as the "first exchange" [27, p. 326]. The concept of the "second exchange" has been introduced by Culnan and Bies [27, p. 326] to explain the privacy calculus, whereby consumers' personal information is given in return for value such as higher-quality service and personalized offers or discounts [27]. Applying the second exchange framework to the LBS context, we may interpret information disclosure in LBS as an exchange where consumers disclose their personal information and location data in return for value such as locatability and personalization provided by LBS providers. Specifically, consumers behave as if they are performing a risk–benefit analysis (i.e., privacy calculus) in assessing the outcomes they would receive as the result of providing personal information to LBS providers. We further integrate the privacy calculus model with justice theory to argue that the outcomes of risk–benefit analysis of personal information disclosure, at the individual level, could be differentiated according to the extent to which justice provisions are manifested in privacy interventions.

Using Justice Theory to Understand Information Privacy

Much has been written on the notion of justice or fairness, from a wide variety of disciplines, including ethics, economics, management, sociology, and psychology, resulting in a plethora of definitions and uses of the concept (see [20] for a review). Recently, justice theory has seen a popular return in the privacy literature [3, 27, 62]. Accordingly, scholarly efforts have been devoted to theoretical development

for analyzing privacy through a justice theoretical lens (e.g., [27, 43, 66]). A general conclusion from this stream of research is that the fairness perceptions of a firm's information practices can have a major positive effect on consumers' privacy decision making [26]. Specifically, the presence of justice, with the concerns for fairness, transparency, and accountability for privacy protection actions, provides consumers with the tangible processes and psychological benefits such as confidence and control that lead to a positive outcome of their privacy calculus and a greater willingness to disclose personal information [27].

However, in the justice literature, there remains considerable debate as to the dimensionality of justice. Arguments have been made that justice consists of anywhere between one single underlying dimension [22] and up to five dimensions, including distributive, procedural, interactional, interpersonal, and informational justice [10, 27, 35, 66]. To address these confusions, Colquitt et al. [20] conducted a meta-analytic review of 25 years of justice research and concluded that the various components of justice reflect two underlying dimensions—namely, distributive justice and procedural justice. In a more recent article on identifying dimensions of justice in the privacy context, Ashworth and Free [3] echoed this conclusion by suggesting that distributive justice and procedural justice fundamentally reflect consumers' privacy concerns (see [3] for a review).[1] They further argued that "the other components of justice [such as interactional justice] in the literature reflect the same underlying concern as that voiced for procedural justice" [3, p. 113].

Consequently, we focus on distributive justice and procedural justice in this research: (1) *distributive justice* refers to the perceived fairness of outcomes that one receives from providing personal information, and (2) *procedural justice* refers to the perceived fairness of the procedures that are enacted for information collection and use. In our research model, distributive justice provisions, predicting individuals' attitudes toward material outcomes of an exchange [3], are mapped as the *compensation* which raises material outcomes of personal information disclosure. We argue that providing financial compensation constitutes an extra consumer outcome and an additional firm input, which is likely to increase the consumer's judgments of the benefits of information disclosure. Procedural justice provisions, predicting "attitudes toward authorities" [42, p. 503], are mapped in our research model as *industry self-regulation* and *government regulation* which alleviate consumers' perceived privacy risks through ensuring that their personal information is treated in a respectful and fair manner. We argue that these self-regulatory and legislative efforts specifically address how to enact the procedures to address consumer concerns regarding the fairness and accountability for privacy protection actions, thereby providing consumers with a sense of procedural justice.

Research Hypotheses

Based on our discussion of the privacy calculus and justice theories, we present the research model for intention to disclose personal information in LBS (see Figure 1). At the core of the model is the privacy calculus, comprising perceived benefits and risks of information disclosure. Distributive and procedural justice provisions, through

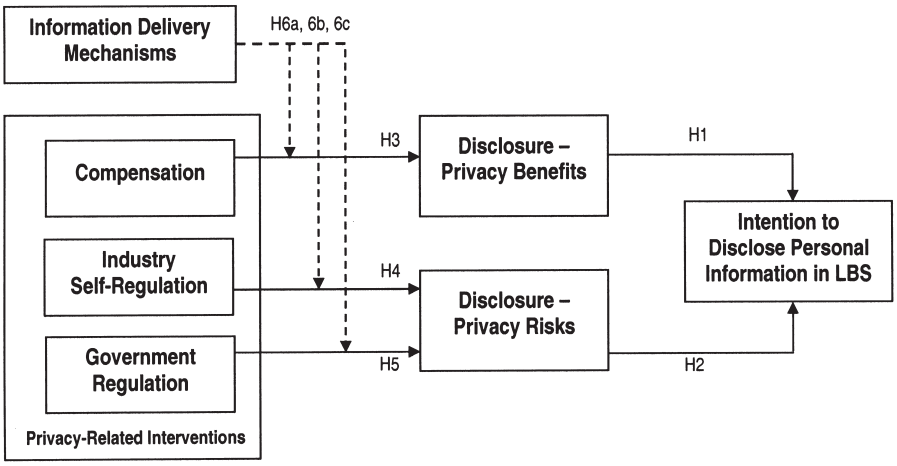


Figure 1. Research Model

the forms of compensation, industry self-regulation, and government regulation, are posited to affect perceived benefits and risks of information disclosure. We further argue that the effects of the privacy interventions on privacy calculus are moderated by information delivery mechanisms (i.e., pull and push).

In this paper, "personal information disclosure" refers to all the information disclosed for the purpose of using LBS, including both dynamic location data and static personal data such as name, shopping preferences and history, mobile phone numbers, and others. It is the combination of both groups of data that enhances the visibility of the individual behavior and thus poses a serious threat to individual privacy [7].

Perceived Benefits of Information Disclosure

In Figure 1, we see that the anticipation of benefits is expected to have a positive influence on intention to disclose personal information in LBS. Labeled as one type of context-awareness computing applications, LBS offer the value of contextualization by sending the user relevant information or services based on the user's location, identity, activity, and time [8]. Three types of value in using LBS were identified in the literature: time-dependent value (timeliness), position-dependent value (positioning), and user-dependent value [6, 39]. Following prior research, we identify two interrelated components of anticipated benefits: (1) *locatability,* which stems from the conflation of time-dependent value and position-dependent value, and (2) *personalization,* which stems from the user-dependent value.

Locatability, reflecting the technical capability to determine the current physical location of wireless devices, has been identified as the key for the visualization of an alluring location business operation [8]. A number of different positioning technologies exist and highly locatable devices can measure their positions with accuracies in the range of a few meters (see [75] for a review). In the context of this research, we use

the construct of locatability to reflect the time-dependent value and position-dependent value of using LBS and define it as the consumer's perceived value of being able to access needed information/services at the right time in the right place. Therefore, locatability enabled by positioning and timeliness is a key advantage used to entice consumers to exchange their personal information for gaining flexible access to needed information or services at anytime from anywhere [6, 39, 40].

The other key anticipated benefit of LBS is the value of personalization with the emphasis on individualized functionalities that add to the user experiences and smoothness of interactions [77]. In the literature, personalization has been generally defined as the ability to uniquely tailor products, contents, and services to an individual [46]. Adapting this definition to the LBS context, we define personalization as the extent to which the LBS can be tailored to consumers' activity contexts, preferences, and needs. Consumers may be motivated to disclose their personal information in exchange for personalized services or information access. LBS can obviously be personalized because the services are invariably tied to a mobile device (e.g., a mobile phone). To the extent that the mobile device could be uniquely identified (e.g., via the subscriber identity module [SIM] card in the case of a mobile phone) and is always handy and available, the device is ideal for delivering personalized services to roving consumers. Moreover, with information about consumers' geographical locations, service providers could channel their marketing and advertising opportunities into tailoring wireless content delivery for different consumers. Indeed, personalization, as one important dimension of perceived benefits identified by prior studies [39, 47, 63], is gained when LBS are tailored to individual customer's identities, interests, preferences, and activity contexts.

To summarize, individuals are likely to give up a degree of privacy in return for potential benefits related to locatability and personalization. Because these benefits are expected to be always positively correlated—that is, locatability and personalization (these two dimensions must always come together before users can gain any value pertaining to LBS) are inherent with information disclosure in LBS—we conceptualize perceived benefits of information disclosure as a second-order construct comprising these two first-order dimensions. To the extent that the anticipation of benefits provides direction for actual behavior through energizing and motivating individuals and enhancing the perceived value of various outcomes, a higher expectation of benefits should amplify the desire to engage in the target behavior. Thus, we hypothesize:

> *Hypothesis 1: The perceived benefits of information disclosure with regard to locatability and personalization are positively related to intention to disclose personal information in LBS.*

Perceived Risks of Information Disclosure

In a general e-commerce context, perceived risk has been regarded as a countervailing force to positive product/service evaluation and adoption decisions when situational contingencies create feelings of uncertainty, discomfort, or anxiety [30]. Perceived

risk has been identified as having various facets (i.e., performance, financial, time, safety, social, and psychological loss) and all risk facets stem from performance risk [28]. Focusing on the overwhelming privacy concerns in the e-service context, Featherman and Pavlou [31] added privacy risk as an important facet of risk, defining it as the degree to which an individual believes that a high potential for loss is associated with the release of personal information to a firm [48]. In the privacy literature, although *privacy concerns* have often been treated as a multidimensional construct [48, 65],[2] *privacy risks* have been treated as a single-dimensional construct that measures potential loss of control over personal information (e.g., [29]). Consistent with prior privacy literature, we operationalize perceived risks in information disclosure as a single-dimensional construct and define it as the expectation of losses associated with the release of personal information to the LBS service provider.

Prior privacy literature has identified sources of organizational opportunistic behavior, including unauthorized access and selling personal data to or sharing information with third parties, financial institutions, or government agencies [56]. A number of privacy studies empirically verified the negative effect of perceived privacy risk on willingness to disclose personal information in Internet transactions (e.g., [29, 48]). In the context of LBS, improper handling of personal information could result in the discovery and matching of location data and identity [19]. The information could be used to classify consumers and enhance the visibility of their behavior, and increase the scope for situations that may be personally embarrassing to them [7, 19]. Therefore, consumers may not want to disclose personal information in LBS if they sense that their personal information is not effectively protected and there exist high risks of privacy invasion. Hence, we hypothesize:

Hypothesis 2: The perceived risks of information disclosure are negatively related to intention to disclose personal information in LBS.

Effects of Privacy Intervention Strategies

The literature in information privacy describes three approaches that companies can take to alter the consumer's risk–benefit analysis and encourage information disclosure—compensation, industry self-regulation, and government regulation [16, 36, 38, 69]. *Compensation* can indeed be gainfully deployed to trade for personal information as consumers have been found willing to relinquish some privacy in exchange for compensation such as product discounts, gift certificates, rebates, and coupons [36, 38, 52]. *Industry self-regulation* is a commonly used approach that places the responsibility for protecting information privacy in the hands of those that gather, use, and sell personal information [27, 38], such as LBS providers. Together, consumers and service providers exercise collective control over the flow of personal information, often with the facilitation of trusted third parties (e.g., TRUSTe). Finally, *government regulation* is another commonly used approach that relies on the judicial and legislative branches of a government agency for protecting personal information [27, 64]. For instance, the United States has sector-specific privacy laws that apply

to specific industry sectors and specific types of records such as credit reports and video rental records, or for classes of sensitive information such as health information [27, 64]. Through a justice theoretical lens, we argue that the presence of three privacy intervention strategies ensures that distributive and procedural justice will prevail, thereby yielding positive beliefs among consumers regarding the outcome of the privacy calculus.

Ensuring Distributive Justice: Compensation

Distributive justice is introduced to "reflect a concern for one's material well-being" [3, p. 113], which is mainly concerned about the fair allocation of outcomes that would require an individual's gains to be in proportion to the inputs they have contributed in an exchange relationship. While there are various theoretical interpretations of distributive justice, they are fundamentally *comparative* in nature [3, 27]—individuals compare their outcomes to some referent standard that they believe they are entitled to in an exchange relationship. In the context of information privacy, judgments of distributive justice entail an assessment of the outcomes and inputs of the "second exchange" between consumers and firms [27]. From the consumer's perspective, this means that the outcomes for providing personal information should be commensurate with the perceived value of the information to the firm relative to the costs incurred by the firm to obtain that information [3].

In the context of LBS, we suggest that a distributively fair solution requires that the consumer's outcomes and inputs be in the same proportion as the service provider's. To the consumer, such fairness judgments entail an assessment of outcomes and inputs in the "second exchange" that may consist of the provision of personal information (which would constitute the consumer's input, and constitute the service provider's outcome) in exchange for the contextualized information/service access (which would constitute the consumer's outcome, and constitute the service provider's input) [3]. In some instances, service providers may offer financial compensation (e.g., more free calling time) for the use of LBS applications as part of their promotion strategy. These financial compensations represent an additional positive outcome for consumers that they are not entitled to without a corresponding increase in the service provider's outcomes. Accordingly, such provisions of additional positive outcomes are likely to reinforce the consumers' distributive justice perceptions by influencing their subjective judgments of the inputs and outcomes involved in the information exchange, and thus lead to higher level of benefit perceptions in information disclosure.[3]

Recent privacy studies provide empirical evidence that compensating consumers for sharing their personal information can enhance their benefit perceptions of information disclosure [36, 38, 58]. For instance, in a conjoint study of trade-offs among all the attributes associated with direct mail (volume, targeting, compensation, and permission), it was found that compensation factor (in terms of providing product discounts, gift certificates, and coupons) was the most important determinant of satisfaction [52]. Hann et al. [36] found that monetary reward significantly affected individuals' preferences for Web sites with differing privacy policies. These studies suggest that providing

financial compensation constitutes an extra consumer outcome and an additional firm input, which is likely to increase the consumer's subjective judgments of the benefits of information disclosure. Therefore, we argue that, by providing financial compensation, service providers can raise consumers' perceptions of positive outcomes of privacy calculus via the underlying mechanism of consumers' distributive justice perceptions, thereby increasing their benefit perceptions of information disclosure. Hence,

> *Hypothesis 3: Financial compensation is positively related to higher perceived benefits of information disclosure in LBS.*

Ensuring Procedural Justice: Industry Self-Regulation and Government Regulation

Research in justice theories has shown that individuals define fairness not only by considering the outcomes received from an exchange relationship, but also in terms of procedures used to arrive at the outcome and how these procedures are enacted [50]. It has been shown that the extent to which individuals are treated in a respectful and fair manner (i.e., procedural justice) significantly influences their fairness perceptions [51]. To make procedural judgments, individuals usually compare their treatments to some normative standards of respectful behavior [51]. In the context of information privacy, fair information practice (FIP) principles serve as global normative standards that reflect procedural justice, indicating consumers' privacy rights are respected and valued [27]. FIP principles are at the heart of industry guidelines and privacy laws [26], which include the stipulations that consumers be given *notice* that their personal information is being collected, *choice* with regard to use of their information, *access* to personal data records, and *security* for these data records [60]. Because complying with FIP principles is a reflection of procedural justice, it is likely to lead consumers to make positive judgments of information disclosure [27]. However, an unresolved issue in terms of FIP implementation is *onus*—whether it should be government regulation or industry self-regulation that enforces the FIP principles, and that consumers are empowered with control over the collection and use of their personal information [27].

To illuminate this controversial issue, we view industry self-regulation and government regulation as two important variables that amplify consumers' procedural justice perceptions and exert direct effects on the perceived privacy risks. Below we discuss how and why the presence of industry self-regulation and government regulation would ensure that procedural justice perceptions will prevail, thereby alleviating consumers' perceived privacy risks.

The approach for assuring privacy most heavily promoted by industry is self-regulation. Self-regulation ensures consumers that when they disclose personal information, it will be held in a protected domain wherein a firm becomes a comanager of the information and accepts responsibility for keeping the information safe and private. The result is that the firm is responsible for managing and protecting the private information by voluntarily implementing a privacy policy based on FIP [27]. Frequently,

industry self-regulatory initiatives are reinforced by third-party interventions, which involve the setting of standards by an industry group or certifying agency and the voluntary adherence to the set standards by members or associates [27]. Groups such as TRUSTe have been active as third-party entities certifying that participating firms indeed conform to the FIP principles they purport to and acting as a facilitator for resolving any conflicts that may arise [9, 27]. These self-regulatory efforts specifically address how to enact the procedures to implement FIP principles, thereby leading to perceptions of procedural justice, which will create the impression that the firm has acted fairly in the process of collecting and using consumer information. When violations occur, these industry self-regulators would provide the means of recourse for the aggrieved [9, 27],[4] thereby creating strong incentives for firms to refrain from opportunistic behavior and behave appropriately. Hence, we hypothesize that the industry self-regulation on FIP implementation will instill greater procedural justice perceptions and lower privacy risk perceptions.

Hypothesis 4: Industry self-regulation on FIP implementation is negatively related to perceived risks of information disclosure in LBS.

The government regulation approach, which embodies strong institutional structural assurances provided by government agencies [33, 78], has been argued to have a positive effect on privacy risk perceptions [25]. With legal structures in place, illegal behavior can be deterred through the threat of punishment [70]. Recognizing the deterrent value of a legal system, consumers tend to believe that firms would conform to the FIP principles as regulated by government regulation, and would therefore collect and use personal information appropriately. Government regulation is also responsible for resolving conflicts that may occur. These legislative efforts to enforce FIP principles could specifically address concerns regarding procedural fairness and accountability for privacy protection actions, thereby providing consumers with a sense of procedural justice [78]. In the presence of relevant government regulation, consumers are likely to have higher levels of procedural justice perceptions toward a firm's privacy practices, thereby perceiving a lower level of privacy risks of personal information disclosure. Hence, we hypothesize:

Hypothesis 5: Government regulation on FIP implementation is negatively related to perceived risks of information disclosure in LBS.

Effect of Information Delivery Mechanisms—Pull Versus Push

The information delivery and acquisition in the LBS context could be either *pull* or *push* [11, 72]. In pull-based LBS, users request some information or use some service based on their locations on a one-time basis [11, 72]. This type of LBS may be seen in some "on demand" services where a consumer dials or signals a service provider for specific information/service such as the nearest automated teller machine (ATM) or Starbucks store. In these services, location information is ephemeral and useful only for users to receive real-time navigational requests (e.g., informing the user of

the nearest ATM or Starbucks). The other type of information delivery mechanism is push-based LBS where a service provider sends the user relevant information/service based on his or her known proximity to a store or service center via a wireless device [11, 72]. In the push-based approach, location information is used to target a user and he or she will be sent the related advertisements when he or she gets within the vicinity of the merchants. In the context of LBS, different information delivery mechanisms (push- and pull-based LBS) could provide consumers with different levels of *control* over the amount of personal information that would be released to LBS providers [72], and thus may influence their perceptions of justice and privacy calculus judgments. In pull-based LBS, consumers exercise greater control over the interaction: the decision to initiate contact with the LBS provider is volitional, and location information is provided only to complete the transaction requested. In contrast, in push-based LBS, consumers exercise less control over their interactions with the service provider: location-based information/services are automatically sent to a consumer's cell phone (or mobile device) based on the tracking of that consumer's location and the consumer's previously stated preferences.

The information delivery mechanism (through pull or push) is expected to act as a moderator that influences both privacy benefit and risk perceptions through its effect on the inferences consumers make regarding distributive and procedural justice. As discussed earlier, in terms of distributive justice, consumers are likely to evaluate the fairness of the distribution of outcomes, which includes the tangible consequences of the information disclosure to both themselves and the beneficiaries of the information (i.e., service providers) [3]. In the push-based mechanism, consumers' real-time location information is tracked in order to provide them with customized information/services at the right time in the right place. However, in the pull-based mechanism, location information is disclosed only when consumers request the service. Therefore, compared to the pull-based mechanism, consumers in push-based LBS need to disclose a larger volume of personal information and location data to gain the benefits of locatability and personalization, which would represent the consumer's additional input, but represent a positive outcome for the firm. Consequently, it appears that a push-based information delivery mechanism works in concert to alter the input/outcome comparison in favor of the service provider, thereby lowering consumers' perceptions of distributive justice. Therefore, we argue that the provision of financial compensation that represents consumers' positive outcome should be more important for push-based LBS to ensure that consumers' distributive justice perceptions will prevail, thereby leading to their benefit perceptions of information disclosure in terms of locatability and personalization. Hence, we hypothesize:

> *Hypothesis 6a: The effect of financial compensation on increasing perceived privacy benefits is stronger for push-based LBS than for pull-based LBS.*

The information delivery mechanism may also act as a moderator that influences privacy risk perceptions through its effect on the inferences consumers make regarding procedural justice. In the case of pull-based LBS, it is likely that a user's need or desire triggers the explicit request for LBS [72]. However, in the push model, it is

likely that the service provider uses contextual knowledge of a consumer's location and preferences to anticipates the needs of the consumer and send him or her contextualized services [72]. In push-based LBS, since consumers have less control over their interactions with service providers, consumers may believe they are more likely to be interrupted by receiving unsolicited messages, which may lead to perceptions of procedural injustice in terms of what and when location-based information/service can be sent to consumers' mobile devices. As a result, the push-based mechanism may be more likely to raise consumers' concerns over a violation of the data collection and use procedures defined in FIP principles. Thus, we argue that the provision of industry self-regulation or government regulation should be more salient for push-based LBS to ensure that consumers' procedural justice perceptions will prevail, thereby lowering their risk perceptions of information disclosure. Hence,

Hypothesis 6b: The effect of industry self-regulation on reducing perceived privacy risks is stronger for push-based LBS than for pull-based LBS.

Hypothesis 6c: The effect of government regulation on reducing perceived privacy risks is stronger for push-based LBS than for pull-based LBS.

Control Variables

Prior research on information privacy and information technology adoption studies point to a number of additional factors that should be included because of their potential influence on dependent and mediating variables in the research model. Therefore, we control for the following effects:

1. *Prior Experience with Mobile Applications.* In examining direct marketing usage, individuals who have prior experience with direct or targeted marketing are more likely to understand the benefits of profiling [24]. Likewise, individuals who have prior experience with mobile applications (e.g., sports news alerts) are more likely to appreciate the benefits of information disclosure in LBS. Therefore, we treat this factor as a control variable for perceived benefits of information disclosure.
2. *Previous Privacy Experience.* Individuals who have been exposed to or been the victim of personal information abuses should have stronger concerns regarding information privacy [65]. Previous privacy experience may therefore influence concerns about privacy invasions [67] and is included as a control variable for perceived risks of information disclosure.
3. *Personal Innovativeness.* Different individuals possess different propensities for learning about or adopting innovations, and these tendencies have been found to have a positive influence on subsequent adoption behavior [2]. In particular, innovators have been found to be early adopters of wireless applications [57]. Hence, we model personal innovativeness as a control variable for behavior intention in our research model.

Research Method

We used a quasi-experimental survey method to test the proposed model. A quasi-experimental design was adopted because this approach allows us to manipulate key variables and exercise control over extraneous variables. We used a 2 (pull-/push-based LBS) × 2 (with/without compensation) × 2 (with/without industry self-regulation) × 2 (with/without government regulation) between-subject, full-factorial design. LBS in our study were introduced as the services run on mobile phones that have the ability to determine a user's current location, by leveraging cellular tower triangulation employed by the network of telecom operators.

Scale Development, Conceptual Validation, and Pilot Study

To the extent possible, we adapted constructs from measurement scales used in prior studies to fit the LBS context. *Intention to disclose information* (INT) was measured with three items asking the extent to which users would reveal their personal information to use the LBS [48]. *Perceived benefits of information disclosure* (BEN) were operationalized as a second-order construct comprising two subconstructs—*locatability* (LOC) and *personalization* (PER). The subconstruct of *locatability* was operationalized to emphasize the importance of providing information/services to mobile consumers at the right time in the right place to support their immediate needs [14]. To measure *locatability,* we used four items based on the LBS literature to reflect the properties of timeliness and positioning [14, 39]. We measured *personalization* using three items to reflect how much the LBS can be tailored to individual customers' preferences, location, and needs [76]. We defined *perceived risks of information disclosure* (RISK) as the expectation of losses associated with the release of personal information to the LBS provider. Measures of perceived risks of information disclosure were based on the measures used in Malhotra et al. [48], adapted to refer to the expectation that a high potential for loss would be associated with the disclosure of personal information to the service provider [48]. To provide deeper insights on the potential effects of three privacy intervention approaches and enhance participant involvement, we manipulated the provision of compensation, the presence of industry self-regulation, and the availability of government regulation in this study. With regard to control variables, *personal innovativeness* (INNV) was assessed with items taken from Agarwal and Prasad [2], and *previous privacy experience* (PPRE) was measured with questions adapted from Smith et al. [65]. *Prior experience in using mobile applications* (EXP) was measured with questions on the frequency in the previous year the participants used mobile applications. Appendix A presents the instrument details.

The initial questionnaire was reviewed by information systems (IS) faculty members and doctoral students for clarity. Next, a pilot study involving 24 graduate students was conducted using the modified questionnaire. The main objectives of the pilot study were to assess the clarity and conciseness of the instructions and questions and gauge the duration of the study. The respondents were also contacted for a face-to-face interview so that their opinions on the instructions and questions could be gathered. Following

analysis of the feedback, a number of revisions were made to the instrument: terms were clarified, the layout of the questions was reorganized, and instructions that the respondents found unnecessary were removed.

Research Design

Manipulations

We operationalized information delivery mechanisms (pull and push) and three privacy-related interventions (compensation, industry self-regulation, and government regulation) by using a scenario-based method. The scenario-based method has often been adopted in LBS-related studies due to the technological novelty (e.g., [41, 63]). Sheng et al. justified the appropriateness of using scenario-based methods for studying ubiquitous computing applications such as LBS: "The use of scenarios makes it possible for researchers to study the emerging . . . phenomenon without being constrained by the timing of the study or the state-of-the-art of technology" [63, p. 355]. Therefore, we manipulated three privacy-related interventions (compensation, industry self-regulation, and government regulation) in pull- and push-based LBS using different scenarios.

Pull and Push. One specific pull-based application and one push-based application—that is, location-based mobile coupon (M-coupon) services—were adapted in this study to yield two balanced scenarios. In the *pull-based* scenario, when consumers wanted to look for promotional information or coupons from merchants in the vicinity, they could dial a certain number and their location would be detected automatically via their mobile phones. The requested coupons from the nearest merchants would then be delivered to their mobile phones via text messages. The *push-based* M-coupon service would involve recruiting consumers by service registration and interest subscription: consumers first registered their mobile phone numbers and subscribed to a list of merchants that provided M-coupon services, based on their interests and preferred period of time for receiving coupons. Profiling information would then be used to target the subscribers, and their mobile phones would be sent related promotional information when they came within the vicinity of the merchants.

Compensation. Research in LBS has found that some consumers agree to receive mobile advertisements via text messages in exchange for free calling time [34]. In some instances, the more advertisements the consumer agrees to receive, the less costly the service plan becomes [34]. Consistent with such practices, for both pull-based and push-based LBS, compensation was manipulated by providing a $0.20 rebate on the consumer's monthly phone bill for every 10 coupons received via text messages (see Appendix B).

Industry Self-Regulation. For industry self-regulation, LBS providers handle personal information based on their privacy policy, with trusted third parties acting as an assur-

ance against violations. For example, TRUSTe has a set of wireless privacy principles and implementation guidelines for LBS providers to safeguard privacy of personal information [71]. 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 is internationally known and the seal is applicable for LBS providers, *industry self-regulation* was manipulated by presenting subjects with a TRUSTe seal with a URL link to the online privacy policy of the service provider (see Appendix C). A brief introduction explaining the mission of TRUSTe was also given to the participants in the industry self-regulation treatment group.

Government Regulation. 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. U.S. 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 U.S. 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.[5] In this study, we manipulated *government regulation* by informing the subjects that LBS transactions were governed by a recently activated legislative act which covers the collection and use of their personal information. Participants were presented with a news article related to recent enforcement of the privacy legislation, with a summary containing the gist of the Location Privacy Protection Act. The act used in this study was modified from a proposal by the Senate and House of Representatives of the United States.[6] The language used in the act was localized to suit Singapore's context.

Although common method bias might not be a major concern when measures of independent and dependent variables are obtained from different sources [59], we incorporated the considerations of addressing this concern in our research. In the research and instrument design (as suggested in [59]), to control acquiescence bias, we used bipolar scales and provided verbal labels for the midpoints of scales. Based on the feedback from pilot tests, we provided examples for those terms or concepts with which subjects may be unfamiliar. We presented the measurement items in a random manner to discourage respondents from figuring out the relationship between the mediator and the dependent variable that we were trying to establish. The anonymous nature[7] of the study also mitigated the likelihood that respondents provided self-serving answers or answers they believed we expected.

Procedure and Task

All the participants were told that all instructions were provided online and that they should read the instructions carefully and complete the study independently. After logging into our online system, all participants began by answering a presession questionnaire about their personal information as a form of control check. Next,

as is commonly used in marketing research that investigates consumer behavior, a cover story was provided to all the subjects. They were told that one specific LBS application—the location-based mobile coupon (M-coupon) service—would soon be introduced in the local market and their feedback would be important for the evaluation of the service.

Next, the subjects were randomly assigned one of the 16 treatment scenarios. Our Web-based system generated the scenarios randomly so that each respondent had an equal and independent chance of being put into any of the 16 scenarios. The subjects were asked to assume the role of a potential LBS user and were presented with the introduction of the pull-based or push-based M-coupon service, which took the form of the Web site of a company to enhance realism. Subjects were also provided with an interactive graphical interface of a mobile device with examples of M-coupons. The subjects were asked to read these materials and read as much of the information provided as possible. The experimental system logged the accesses made by the subjects to all the URLs to ensure that the subjects had actually read the manipulated condition. Next, the subjects were asked to complete a postsession questionnaire on locatability, personalization, perceived privacy risks, and intention to disclose personal information in LBS. Subject responses to the meaningfulness of the task (mean = 5.35, standard deviation [SD] = 1.05) were significantly higher than the neutral value of 4 ($t = 6.99$, $p < 0.001$) (see Appendix A for questions used).

Subjects

We obtained responses among mobile phone users in Singapore. We recruited the subjects by posting announcements to a number of relevant forums and discussion topics on mobile handsets and mobile applications at the major and reputable Web portals of 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. Respondents were asked to click on the URL link provided in the posted message, which linked to the online system. A lottery with nine prizes was included as an incentive to participate in the research. The invitees were assured that the results would be reported only in aggregate and that their anonymity would be ensured. Specific demographic information is given in Appendix D. Responses that either contained significant amount of missing values or failed manipulation checks were subsequently eliminated from data analysis. We used the valid data from the remaining 528 subjects for data analyses.

Data Analysis and Results

Manipulation Check

To ensure that the subjects attended to their assigned privacy intervention conditions, manipulation checks were included in the postsession questionnaire (see Appendix A). Questions were posed to assess the level of understanding of information delivery mechanisms for those subjects belonging to the pull- and push-based scenarios. By comparing subjects' responses against the neutral value of four, we confirmed that

the manipulations of pull-based (mean = 5.27, SD = 1.11) and push-based (mean = 5.51, SD = 1.02) scenarios were effective in creating the required decision-making environment for subjects. The manipulations on *compensation, self-regulation,* and *government regulation* were confirmed against true/false questions. Specifically, for the *compensation* treatment group, the subjects were asked whether the service provider provided additional discount for using the M-coupon service. For the *self-regulation* treatment group, subjects were asked whether there was a TRUSTe logo at the service provider's Web site. For the *government regulation* treatment group, subjects were asked whether there was a Privacy and Wireless Communications Protection Act to protect their privacy in LBS. Additional questions were also used to assess participants' level of understanding of the privacy statements and related laws for those subjects belonging to the industry self-regulation and government regulation treatment groups. Manipulations were also checked by examining the log of the system to verify that subjects had browsed the materials pertaining to their respective treatments. Data that failed the manipulation checks was dropped.

Mann-Whitney tests showed that gender ratio and education level of subjects did not differ significantly across the various treatments. Analysis of variance (ANOVA) tests revealed that subjects assigned to the various treatments did not differ significantly in terms of their age, mobile application usage experience, and prior privacy experience. Hence, the random assignment of subjects to the various treatments appeared to be effective.

Analysis Strategy

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold [74], was used for data analysis. PLS possesses many advantages over traditional statistical methods such as factor analysis, multivariate analysis of variance (MANOVA), and regression. First, it is not contingent upon data having multivariate normal distributions and interval scales [32]. This makes PLS suitable for handling manipulated constructs. Second, PLS has the ability to simultaneously test the measurement model and the structural model. This allows a more complete analysis of interrelationships in the model. Third, PLS is generally more appropriate for testing theories in the early stages of development [32]. Since this study is an early attempt at advancing a theoretical model on exploring the potential effects of information delivery mechanisms on an extended privacy calculus model in LBS, PLS is more suitable than other methods. To test the influence of information delivery mechanisms, we split the data sets into two subsets and thus the measurement and the structural models were tested twice: once for the pull-based LBS subset and another for the push-based LBS subset.

Evaluating the Measurement Model

We evaluated the measurement model by examining the convergent validity and discriminant validity of the research instrument. Convergent validity is the degree to which different attempts to measure the same construct agree [21]. In PLS, three tests

are used to determine the convergent validity of measured reflective constructs in a single instrument: reliability of items, composite reliability of constructs, and average variance extracted by constructs. We assessed item reliability by examining the loading of each item on the construct, and found that the reliability score for all the items exceeded the criterion of 0.707. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's [54] criterion of 0.7. The average variances extracted for the constructs were all above 50 percent, and the Cronbach's alphas were also all higher than 0.7. As can been seen from the confirmatory factor analysis (CFA) results in Table 1[8] and the reliability scores in Table 2, these results support the convergent validity of the measurement model.

Discriminant validity is the degree to which measures of different constructs are distinct [12]. To test discriminant validity [17], (1) indicators should load more strongly on their corresponding construct than on other constructs in the model, and (2) the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model. As shown in Table 1, all factor loadings are higher than cross loadings. Furthermore, as shown by comparing the diagonal to the nondiagonal elements in panels a and b of Table 2, all constructs share more variance with their indicators than with other constructs. Therefore, all items fulfilled the requirement of discriminant validity.

Testing the Structural Model

After establishing the validity of the measures, we conducted hypothesis tests by examining the sign and significance of the path coefficients. As the three privacy intervention approaches (compensation, industry self-regulation, and government regulation) were manipulated variables, they were coded as dichotomous variables with 1 being *with* condition and 0 being *without* condition in the data analysis. Because PLS does not generate any overall goodness-of-fit indices, predictive validity is assessed primarily through an examination of the explanatory power and significance of the hypothesized paths. The explanatory power of the structural model is assessed based on the amount of variance explained in the endogenous construct (i.e., intention to disclose personal information in our study).

Except the construct of perceived benefits of information disclosure (BEN), we modeled the rest of the constructs as first-order constructs that were measured using multiple indicators. Following the approach adopted by Agarwal and Karahanna [1], we measured the construct of perceived benefits of information disclosure using summated scales, which were represented by factor scores derived from the CFA. This was necessary because PLS does not directly support second-order factors. Loadings for the BEN dimensions (locatability and personalization) are shown in the structural model. Figure 2 depicts the structural models for pull-based and push-based LBS inclusive of all the significant control variables.

The structural models for the pull and push mechanisms explained 30.2 percent and 40.2 percent, respectively, of the variance in intention to disclose personal information in LBS. For the *pull* model, perceived privacy benefits (H1) and perceived privacy

Table 1. Results of Factor Analysis

	Privacy risk (RISK)		Locatability (LOC)		Personalization (PER)		Intention (INT)		Innovativeness (INNV)		Previous privacy experience (PPRE)	
	Pull	Push	Pull	Push	Pull	Push	Pull	Push	Pull	Push	Pull	Push
RISK1	**0.79**	**0.85**	0.25	0.27	0.28	0.22	–0.12	–0.14	0.04	0.17	–0.08	0.12
RISK2	**0.92**	**0.93**	0.22	0.10	0.29	0.18	–0.13	–0.22	0.05	0.11	–0.07	0.22
RISK3	**0.96**	**0.95**	0.12	0.14	0.20	0.21	–0.26	–0.17	0.07	0.10	–0.09	0.16
LOC1	0.14	0.23	**0.86**	**0.83**	0.49	0.67	0.34	0.37	–0.03	0.21	–0.15	–0.04
LOC2	0.17	0.10	**0.88**	**0.87**	0.53	0.61	0.36	0.39	–0.08	0.20	–0.16	–0.01
LOC3	0.17	0.15	**0.89**	**0.84**	0.54	0.66	0.37	0.41	–0.04	0.13	–0.14	–0.04
LOC4	0.19	0.13	**0.87**	**0.88**	0.57	0.63	0.38	0.39	–0.08	0.10	–0.13	0.01
PER1	0.19	0.22	0.48	0.67	**0.82**	**0.88**	0.24	0.38	–0.03	0.18	–0.09	–0.03
PER2	0.28	0.17	0.50	0.62	**0.87**	**0.83**	0.35	0.36	–0.01	0.16	–0.05	–0.04
PER3	0.22	0.18	0.56	0.59	**0.86**	**0.82**	0.36	0.49	0.01	0.10	0.01	–0.01
INT1	–0.24	–0.17	0.39	0.46	0.33	0.50	**0.81**	**0.96**	–0.13	0.21	–0.06	0.02
INT2	–0.13	–0.19	0.37	0.44	0.36	0.48	**0.92**	**0.98**	–0.12	0.20	–0.06	0.05
INT3	–0.15	–0.20	0.33	0.41	0.31	0.42	**0.91**	**0.96**	–0.17	0.23	–0.10	0.06
INNV1	0.03	0.13	–0.06	0.24	–0.01	0.20	0.07	0.24	**0.79**	**0.91**	0.15	0.11
INNV2	0.02	0.08	–0.07	0.01	–0.04	0.01	0.15	0.13	**0.89**	**0.85**	0.17	0.15
INNV3	0.10	0.13	–0.04	0.17	0.01	0.21	0.16	0.17	**0.91**	**0.86**	0.14	0.04
PPRE1	0.09	0.16	–0.17	–0.03	–0.04	–0.04	–0.09	–0.05	0.15	0.12	**0.97**	**0.97**
PPRE2	0.07	0.19	–0.14	–0.04	–0.06	–0.01	–0.05	–0.03	0.19	0.09	**0.86**	**0.89**

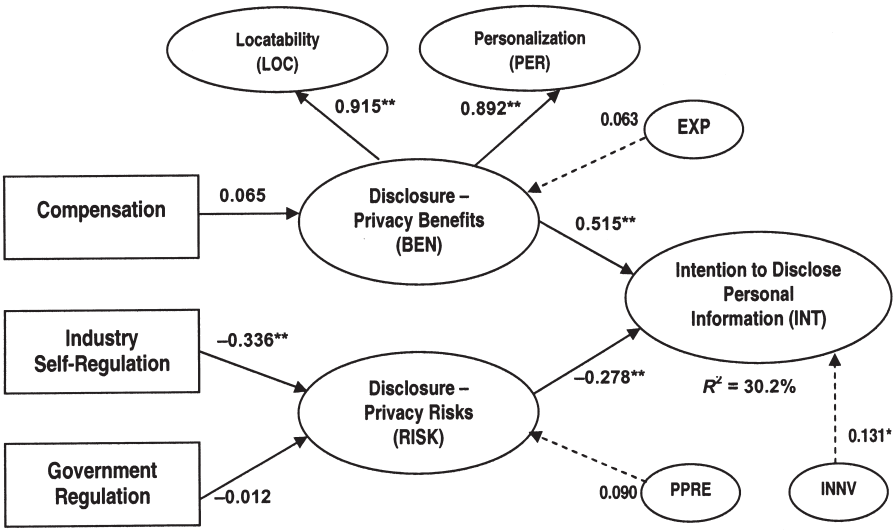
Note: Factor loadings are shown in boldface.

Table 2. Interconstruct Correlations

	Composite reliability	Cronbach's alpha	Variance extracted	LOC	PER	RISK	INT	INNV	PPRE
Panel a: pull-based model									
LOC	0.931	0.900	0.771	**0.878**					
PER	0.884	0.800	0.718	0.407	**0.847**				
RISK	0.927	0.847	0.756	–0.206	–0.284	**0.899**			
INT	0.928	0.958	0.812	0.390	0.356	–0.235	**0.901**		
INNV	0.881	0.853	0.714	0.101	0.052	0.123	0.161	**0.845**	
PPRE	0.912	0.837	0.839	0.090	0.072	0.071	0.097	0.177	**0.916**
Panel b: push-based model									
LOC	0.915	0.877	0.730	**0.855**					
PER	0.885	0.805	0.719	0.493	**0.848**				
RISK	0.936	0.897	0.831	–0.188	–0.225	**0.911**			
INT	0.971	0.955	0.918	0.302	0.316	–0.263	**0.958**		
INNV	0.907	0.847	0.764	0.181	0.116	–0.137	0.229	**0.874**	
PPRE	0.926	0.858	0.863	0.025	0.033	0.185	0.065	0.120	**0.929**

Note: The square root of the variance shared between a construct and its measures is shown in boldface.

a. Pull-Based LBS



b. Push-Based LBS

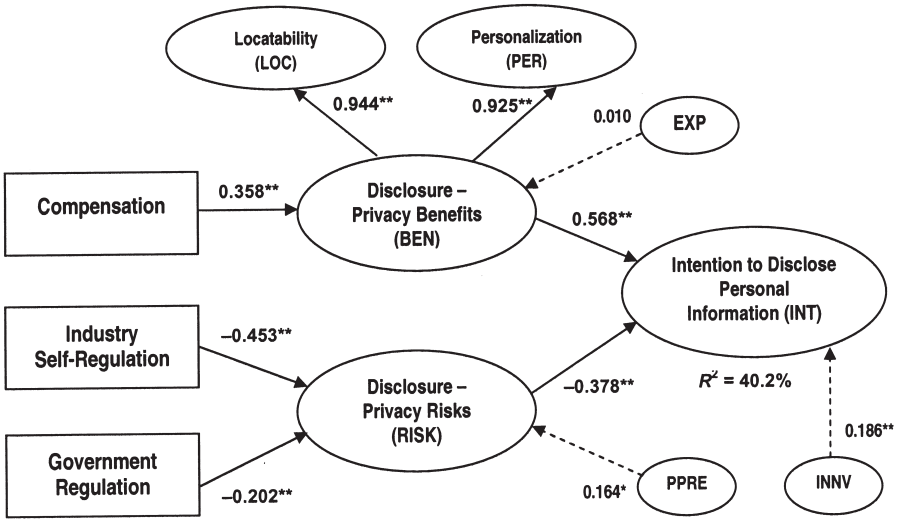


Figure 2. Structural Model
Notes: Dash lines represent the effects of control variables. INNV = Personal Innovativeness; EXP = Prior Experience in Using Mobile Applications; PPRE = Previous Privacy Experience. * Significant at the 5 percent level; ** significant at the 1 percent level.

risks (H2) were significant predictors of intention to disclose personal information in LBS, and industry self-regulation (H4) had a significant effect on perceived privacy risks. However, the positive effect of compensation (H3) on privacy benefits and the negative effect of government regulation on privacy risks (H5) were insignificant. For the *push* model, perceived privacy benefits (H1) and perceived privacy risks (H2) were

significant predictors of intention to disclose personal information, compensation (H3) had a significant effect on perceived privacy benefits, and industry self-regulation (H4) and government regulation (H5) were significant predictors of perceived privacy risks. Table 3 summaries results of hypothesis testing for Hypotheses 1 to Hypothesis 5 for both pull and push models.

Hypotheses related to the moderating effects of information delivery mechanisms (H6a, H6b, and H6c) were tested using the multigroup analysis suggested by Carte and Russell [13] and Chin [18]. First, Box's *M*-tests were performed to "reject the null hypothesis of equal covariance matrices due to differences in construct content" [13, p. 494]. Results confirmed the equality of covariance matrices for the pull and push data sets within the constructs of perceived privacy risks and perceived privacy benefits. Second, we proceeded to the multigroup analysis by testing the effects of the information delivery mechanism with the PLS-generated path coefficients and their standard errors.[9] The results of these tests are shown in Table 4. In support of Hypothesis 6a, the positive relationship between compensation and privacy benefits was stronger for push-based LBS (t (526) = –3.65, $p < 0.01$). Supporting Hypothesis 6b, the negative relationship between industry self-regulation and privacy risks (t (526) = 1.78, $p < 0.05$) was found to be stronger for the push-based LBS; supporting Hypothesis 6c, the negative relationship between government regulation and privacy risks (t (526) = 2.36, $p < 0.01$) was also found to be stronger for the push-based LBS.

Discussions and Implications

Discussion of Findings

The goal of this study was to integrate privacy calculus theory with justice theories to construct a conceptual model that features the roles of pull and push information delivery mechanisms in an individual's privacy decision-making process. Although the empirical results of this study provide overall support for the research model, they also reveal a few unexpected relationships that are not consistent with what we hypothesized. Drawing on prior research, we argued that the provision of justice through compensation, industry self-regulation, and government regulation would influence consumers' perceived privacy benefits and risks. Our results confirm that the impact of industry self-regulation on perceived privacy risks for both pull and push models is significant. However, the influence of compensation and government regulation on users' privacy perceptions varies under different information delivery mechanisms: the provision of compensation has an impact on enhancing users' privacy benefit perceptions in push-based LBS but this is not the case with pull-based LBS. Likewise, government regulation has an impact on reducing users' privacy risk perceptions in push-based LBS but its effect is not significant in pull-based LBS.

A plausible explanation for the insignificance of compensation is that the use of pull-based LBS is initiated by a well-defined need or desire, and to the extent that users seek fulfillment of their needs, the importance of compensation as an additional impetus diminishes. In such context, greater salience would be assigned to time savings,

Table 3. Results of Hypothesis Testing for Hypotheses 1 to 5

Endogenous constructs	Causes	Coefficient		Support
		Pull	Push	
Perceived privacy risks				
H5	Government regulation	–0.012	–0.202**	Partial (support for push)
H4	Industry self-regulation	–0.336**	–0.453**	Yes
Perceived privacy benefits				
H3	Compensation	0.065	0.358**	Partial (support for push)
Intention to disclose personal information				
H2	Perceived privacy risks	–0.278**	–0.378**	Yes
H1	Perceived privacy benefits	0.515**	0.568**	Yes

* Significant at the 1 percent level.

Table 4. Results on Moderating Effect of Information Delivery Mechanisms

Hypotheses	Coefficient (standard error)		t	Supported
	Pull $n = 261$	Push $n = 267$		
H6a: Compensation → Privacy Benefits (push > pull)	0.065 (0.0611)	0.358 (0.0539)	–3.65**	Yes
H6b: Industry Self-Regulation → Privacy Risks (push > pull)	–0.336 (0.0473)	–0.453 (0.0461)	1.78*	Yes
H6c: Government Regulation → Privacy Risks (push > pull)	–0.012 (0.0615)	–0.202 (0.0525)	2.36**	Yes

* Significant at the 5 percent level; ** significant at the 1 percent level.

efficiency, and convenience rather than the financial compensation provided by service providers for using LBS. As to the insignificance of government regulation in reducing privacy risk perceptions for pull-based LBS, a possible explanation is because of the higher level of control inherent in the pull-based mechanism. As discussed earlier, users exercise greater control over the interaction in pull-based LBS: the decision to initiate contact with the merchant is volitional, and location information is disclosed only to complete the transaction requested. Due to higher levels of control over releasing personal information, consumers may perceive that the implementation of FIP through government regulation is not necessary for pull-based LBS but such a legislative approach appears necessary for push-based LBS. Unlike pull-based LBS, users in push-based LBS are more likely to be interrupted by receiving unsolicited messages. Hence, users in push-based LBS would expect strong legislative privacy interventions to ensure procedural justice and implement FIP principles, for example, enforce the notice and choice principles on what information/service can be pushed to consumers' mobile devices and what cannot. As shown by our results, such a legislative approach is not necessary for pull-based LBS.

Examining control variables in the structural models also offers some insights. Personal innovativeness was found to have a significant effect on intention to disclose personal information in LBS for both pull-based and push-based mechanisms. This implies that those who are more innovative are likely to disclose personal information to try out LBS more readily than others and vice versa. Interestingly, the results show that the potential influences of previous privacy experience on users' privacy risk perceptions vary under different information delivery mechanisms: previous privacy experience has an impact on users' privacy risk perceptions in push-based LBS but this is not the case with pull-based LBS. It seems that for the push-based mechanism, individuals who have encountered privacy invasions are more aware of undesirable consequences of using LBS based on previous experience.

Limitations and Future Research

We note several limitations to our work that should be taken into account when generalizing the results. First, this study was conducted in Singapore, which has a strong reputation for rigorous enforcement of laws and regulations [37].[10] Therefore, the subjects might be biased in their behavior with respect to the regulatory approaches to privacy protection. Hence, care must be taken when generalizing these findings to consumers in other social, economic, and cultural environments, and future research could replicate this study in other countries, especially those in Europe and North America. The privacy regulatory approaches adopted in the European Union and the United States represent the two major privacy regulatory models—the comprehensive legislative approach and the industry self-regulatory approach. Second, as is the case with recent research on privacy issues in LBS (e.g., [41, 63]), a scenario-based approach is considered appropriate at the initial adoption stage of LBS. Nevertheless, we believe that such an approach represents a simplification of the real pull- and push-based LBS context, which limits the generalizability of research results. A lon-

gitudinal field experiment in which participants can gain more realistic experiences of using LBS will certainly produce more reliable and meaningful results. The challenge is to design the manipulations for both pull and push mechanisms in a balanced and realistic manner. Particularly, it would be challenging to mimic user behaviors for the pull-based LBS in an experimental setting, because in pull-based LBS (e.g., "Where is the nearest Japanese restaurant offering discounts right now?"), a consumer's decision to initiate contact with the service provider is volitional. Therefore, triggering consumers' natural motives of initiating the use of pull-based LBS in an experimental setting remains a challenge.

Finally, there are other aspects such as usability, service quality, and information quality that may affect consumers' willingness to disclose personal information, which could also be examined in future research. In the current research, we adopted a privacy calculus lens because our objective was to focus on potential users who do not yet have credible information about or affective bonds with LBS providers. For this initial adoption/usage stage, consumers may focus on evaluating the distributive outcomes of disclosing their personal information (i.e., distributive justice provisions) and the procedures enacted to safeguard against the mishandling of their information (i.e., procedural justice provisions) [66]. Future research could move beyond the initial adoption/usage stage to the domain of continuance usage where consumers need to keep their eyes open to ensure that service providers fulfill their promises associated with the benefits and privacy assurance procedures [66]. In such contexts, trust theories [4] may be particularly relevant.

Theoretical Contributions and Practical Implications

This study represents one of the first attempts at exploring the relative effectiveness of pull and push information delivery mechanisms with privacy considerations as a focal point. Through the causal modeling of antecedents affecting perceived benefits and risks of personal information disclosure, our findings provide preliminary theoretical and empirical insights into the dynamic structural relationships of these factors under two types of information delivery mechanisms. Particularly, the modeling of three privacy-related interventions with the moderating effect of pull–push mechanisms will allow the focus of attention to shift from a general discussion of potential privacy invasion to a more granular level of analysis on the privacy decision process in which competing beliefs are weighed and where the strength of one may override the influence of another.

The model of privacy calculus interprets the individual's privacy interests as an exchange where individuals disclose their personal information in return for certain benefits. Such a calculus perspective of privacy has been found in many studies to be an important framework analyzing consumer privacy concerns [29]. The current study aimed to contribute to existing research on privacy calculus in several ways. First, we integrated the justice theories into the privacy calculus model and studied the efficacy of three privacy intervention strategies (compensation, industry self-regulation, and government regulation) in influencing privacy benefits/risks. This represents one of the

few studies that theoretically differentiate three privacy intervention approaches by linking them with different types of justice provisions. It is proposed that the conventional understanding of privacy as a calculus can be explained within the justice theoretical framework: on one hand, consumers may evaluate the fairness of the distribution of outcomes, which includes the tangible consequences of the information disclosure to both themselves and firms; on the other hand, they may evaluate the fairness of the manner in which they were treated in the information exchange.

Second, the current research explored to what extent the effects of privacy intervention strategies on privacy calculus are dependent upon certain technological attributes (i.e., information delivery mechanisms). Studying the privacy implications pertaining to the information delivery mechanisms is important because there is lack of research examining how technological attributes may influence privacy theoretical development [15]. Given that the more recent reincarnations of push technologies create new privacy dilemmas (e.g., Facebook's push feature—Beacon in its social advertising initiatives) [68], it would be important for researchers to include privacy considerations in the modeling and design of information delivery mechanisms. The theoretical framework developed here can be tested in other push technology contexts to assess its applicability.

Third, following Lanier and Saini's call [43], the current research empirically tested the research model in an understudied LBS context. Privacy concerns in this new context of surveillance-based technologies become particularly salient because merchants and service providers may have access to a large volume of potentially sensitive consumer information. A final implication for future research and theoretical development is to extend and adapt the theory described here to other surveillance-based technologies that may give rise to similar or extended privacy concerns. For example, there has been much written in the popular press about technologies such as radio frequency identification devices and the ensuing consumer backlash at the capability these technologies provide for third parties to monitor and track consumer behavior. Likewise, embedded sensors are double-edged swords for potential users—simultaneously offering convenience and invading privacy. How do consumers trade off the privacy risks and benefits of these technologies? What is the nature of the privacy calculus that guides their decisions on information disclosure? These would be fruitful questions for future research.

From a practical perspective, this study has implications for various players in the LBS industry—merchants, wireless service providers, privacy advocates, and government legislators. Given that individuals' concerns for privacy are not absolute, but rather, can be traded off against benefits under different mechanisms of push and pull, there exist ample opportunities for service providers to offer LBS through different information delivery mechanisms. Our results suggest that providing compensation for push-based LBS is more important than it is for pull-based LBS. It follows that additional monetary incentives, and more services with privacy-enhancing features, need to be developed and provided to mitigate the perceived higher levels of privacy invasion associated with push-based LBS. Our findings further suggest that privacy advocates and government legislators should not adopt a unitary view of all types of

LBS. Although privacy protection is a fundamental concern that must be addressed, "one size fits all" regulations on privacy are ill equipped to accommodate the interests of broader groups of users and the full gamut of players in the LBS industry. Hence, there is need for sensitivity to the diversity of interests behind the free flow of information that promotes a dynamic marketplace and provides substantial benefits for individual consumers and society as a whole. Our evidence shows that the implementation of FIP through government regulation is not necessary for pull-based LBS users but such a legislative approach appears necessary for push-based LBS users. Therefore, future government regulation on FIP implementation could specifically target certain services.

Conclusion

The advent of mobile and positioning technologies and the recent reincarnations of push technologies provide new value to users while simultaneously creating new vulnerabilities. It is important for researchers, designers, and policymakers to understand how users strike a balance between value and risk. This research has provided preliminary evidence for some aspects of this dilemma. The current research contributed to existing privacy research by theoretically differentiating three privacy intervention approaches through a justice theoretical lens, for different technological attributes (information delivery mechanisms), in an understudied LBS context. Our initial findings that compensation, industry self-regulation, and government regulation have different efficacy for influencing the privacy calculus model depending on the type of information delivery mechanisms being examined suggests the need for future studies to understand these effects more fully. Using the groundwork laid 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 push technologies and LBS.

Notes

1. In some analyses of identifying dimensions of justice in the privacy context [27, 66], interactional justice was considered as the third component of justice besides procedural justice and distributive justice. However, other justice scholars [20, 35] have argued that "interactional justice" itself stems from explanations of the procedures used to determine outcomes, and captures the respect conveyed during the social interaction. Therefore, interactional justice reflects "the same underlying concern as that voiced for procedural justice" [3, p. 113]. Consequently, we focus on procedural justice and distributive justice in this research.

2. The concern for information privacy (CFIP) scale was developed by Smith et al. [65] and identified four data-related dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access to information) that have since served as one of the most reliable instruments measuring individuals' concerns toward organizational privacy practices. Malhotra et al. [48] operationalized a multidimensional notion of Internet users' information privacy concerns (IUIPC) that adapted the CFIP in the Internet context.

3. In this study, we position the provision of compensation as one privacy intervention strategy that will amplify privacy benefit perceptions, but we do not consider it as the *component* of privacy benefits. This is because compensation is usually provided and controlled by service

providers: some service providers provide and some do not. However, the privacy benefits in terms of locatability and personalization always come as consequences of information disclosure in LBS, and will exist with or without the provision of compensation.

4. 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 be the appropriate attorney general's office, the Federal Trade Commission, or the Consumer Protection Agency in the United States [9].

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

6. The details of the proposal by the Senate and House of Representatives of the United States are available at www.techlawjournal.com/cong107/privacy/location/s1164is.asp.

7. We only collect respondents' e-mail addresses for the prize-awarding purpose.

8. To perform CFA in PLS, the following procedure was suggested by Chin [17] and applied in Agarwal and Karahanna [1]: the loadings for the construct's own indicators were provided by PLS. To calculate cross loadings, a factor score for each construct was calculated based on the weighted sum of the construct's indicators. Then these factor scores were correlated with all other indicators to calculate cross loadings of other indicators on the construct.

9. This statistical comparison takes the standard errors for the structural paths provided by PLS-Graph in the resampling output and calculates the *t*-test for the difference in paths between pull and push groups using the following equation:

$$t = \frac{Path_{sample\_1} - Path_{sample\_2}}{\left[\sqrt{\frac{(m-1)^2}{(m+n-2)} * S.E._{sample1}^2 + \frac{(n-1)^2}{(m+n-2)} * S.E._{\text{sample2}}^2}\right] * \left[\sqrt{\frac{1}{m} + \frac{1}{n}}\right]},$$

where t = t-statistic with $(m + n - 2)$ degrees of freedom; SE_i = standard error of the coefficient in structural model of pull or push; m and n = sample size of data set for pull and push, respectively; *Path* = path coefficient in structural model of pull or push.

10. We measured perceived "rule of law," which captured the extent to which laws and regulations are enforced. Subject responses to these questions were significantly smaller than the neutral value of 4 ($t = -12.26$, $p < 0.001$), which confirmed Singapore's reputation for rigorous enforcement of laws and regulations among subjects in this study. These three questions used to measure perceived "rule of law" were taken from Gibson and Caldeira [33]: "It is not necessary to obey a law you consider unjust," "Sometimes it might be better to ignore the law and solve problems immediately rather than wait for a legal solution," and "If you don't particularly agree with a law, it is all right to break it if you are careful not to get caught."

References

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

2. 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), 204–215.

3. Ashworth, L., and Free, C. Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67,* 2 (2006), 107–123.

4. Ba, S.L.; Whinston, A.B.; and Zhang, H. Building trust in online auction markets through an economic incentive mechanism. *Decision Support Systems, 35,* 3 (2003), 273–286.

5. Bagozzi, R.P. Marketing as exchange. *Journal of Marketing, 39,* 4 (1975), 32–39.

6. Barnes, J.S. Known by the network: The emergence of location-based mobile commerce. In E.-P. Lim and K. Siau (eds.), *Advances in Mobile Commerce Technologies.* Hershey, PA: Idea Group, 2003, pp. 171–189.

7. Beinat, E. Privacy and location-based services: Stating the policies clearly. *GeoInformatics, 4* (September 2001), 14–17.

8. Bellavista, P.; Kupper, A.; and Helal, S. Location-based services: Back to the future. *IEEE Pervasive Computing, 7,* 2 (2008), 85–89.

9. Benassi, P. TRUSTe: An online privacy seal program. *Communications of the ACM, 42,* 2 (1999), 56–59.

10. Bies, R.J., and Moag, J.S. Interactional justice: Communication criteria of fairness. In R.J. Lewicki, B.H. Sheppard, and M. Bazerman (eds.), *Research on Negotiation in Organizations.* Greenwich, CT: JAI Press, 1986, pp. 43–55.

11. Bruner, C.G., II., and Kumar, A. Attitude toward location-based advertising. *Journal of Interactive Advertising, 7,* 2 (Spring 2007) (available at www.jiad.org/article89).

12. Campbell, D.T., and Fiske, D.W. Convergent and discriminant validation by the multitrait–multimethod matrix. *Psychological Bulletin, 56,* 1 (1959), 81–105.

13. Carte, A.T., and Russell, J.C. In pursuit of moderation: Nine common errors and their solutions. *MIS Quarterly, 27,* 3 (2003), 479–501.

14. Chae, M., and Kim, J. Information quality for mobile Internet services: A theoretical model with empirical validation. In V. Storey, S. Sarkar, and J. DeGross (eds.), *Proceedings of the Twenty-Second International Conference on Information Systems.* Atlanta: AIS, 2001, pp. 43–53.

15. Chan, Y.E.; Culnan, M.J.; Greenaway, K.; Laden, G.; Levin, T.; and Smith, H.J. Information privacy: Management, marketplace, and legal challenges. *Communications of the AIS, 16,* 1 (2005), 593–634.

16. Chellappa, R.K., and Shivendu, S. An economic model of privacy: A property rights approach to regulatory choices for online personalization. *Journal of Management Information Systems, 24,* 3 (Winter 2007–8), 193–225.

17. Chin, W.W. The partial least squares approach to structural equation modeling. In G.A. Marcoulides (ed.), *Modern Methods for Business Research.* Mahwah, NJ: Lawrence Erlbaum, 1998, pp. 295–336.

18. Chin, W.W. Frequently asked questions—Partial least squares & PLS-Graph. 2004 (available at http://disc-nt.cba.uh.edu/chin/plsfaq.htm#Q1).

19. Clarke, R. Person location and person tracking: Technologies, risks and policy implications. *Information Technology & People, 14,* 2 (2001), 206–231.

20. Colquitt, J.A.; Conlon, D.E.; Wesson, M.J.; Porter, C.; and Ng, K.Y. Justice at the millennium: A meta-analytic review of 25 years of organizational justice research. *Journal of Applied Psychology, 86,* 3 (2001), 425–445.

21. Cook, M., and Campbell, D.T. *Quasi-Experimentation: Design and Analysis Issues for Field Settings.* Boston: Houghton Mifflin, 1979.

22. Cropanzano, R., and Ambrose, M.L. Procedural and distributive justice are more similar than you think: A monistic perspective and a research agenda. In J. Greenberg and R. Cropanzano (eds.), *Advances in Organizational Justice.* Stanford: Stanford University Press, 2001, pp. 119–151.

23. Culnan, M.J. "How did they get my name"? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17,* 3 (1993), 341–364.

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

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

26. Culnan, M.J., and Armstrong, P.K. Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science, 10,* 1 (1999), 104–115.

27. Culnan, M.J., and Bies, J.R. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59,* 2 (2003), 323–342.

28. Cunningham, S. The major dimensions of perceived risk. In D.F. Cox (ed.), *Risk Taking and Information Handling in Consumer Behavior.* Cambridge: Harvard University Press, 1967, pp. 82–108.

29. Dinev, T., and Hart, P. An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17,* 1 (2006), 61–80.

30. Dowling, G., and Staelin, R. A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21,* 1 (1994), 119–134.

31. Featherman, M.S., and Pavlou, P.A. Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human–Computer Studies, 59,* 4 (2003), 451–474.

32. Fornell, C., and Bookstein, F.L. Two structural equation models: LISREL and PLS applied to customer exit-voice theory. *Journal of Marketing Research, 19,* 11 (1982), 440–452.

33. Gibson, J.L., and Caldeira, G.A. The legal cultures of Europe. *Law & Society Review, 30,* 1 (1996), 55–85.

34. Gidari, A. No "L-commerce" without "L-privacy": Fair location information practices for mobile commerce. Paper presented at the L-Commerce 2000—The Location Services & GPS Technology Summit, Washington, DC, June 13–14, 2000.

35. Greenberg, J. The social side of fairness: Interpersonal and informational classes of organizational justice. In R. Cropanzano (ed.), *Justice in the Workplace: Approaching Fairness in Human Resource Management.* Hillsdale, NJ: Lawrence Erlbaum, 1993, pp. 79–103.

36. Hann, I.-H.; Hui, K.-L.; Lee, S.Y.T.; and Png, I.P.L. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24,* 2 (Fall 2008), 13–42.

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

38. Hui, K.-L.; Teo, H.-H.; and Lee, T.S.Y. The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31,* 1 (2007), 19–33.

39. Junglas, I.A., and Watson, R.T. The U-constructs: Four information drives. *Communications of the AIS, 17,* 1 (2006), 569–592.

40. Junglas, I.A., and Watson, R.T. Location-based services: Evaluating user perceptions of location-tracking and location-awareness services. *Communications of the ACM, 51,* 3 (2008), 65–69.

41. Junglas, I.A.; Johnson, N.A.; and Spitzmüller, C. Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17,* 4 (2008), 387–402.

42. Konovsky, M.A. Understanding procedural justice and its impact on business organizations. *Journal of Management, 26,* 3 (2000), 489–511.

43. Lanier, D.C., and Saini, A. Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review, 12,* 2 (2008), 1–48.

44. Laufer, R.S., and Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33,* 3 (1977), 22–41.

45. Levy, S. A future with nowhere to hide? *Newsweek* (June 7, 2004) (available at www.newsweek.com/id/53986).

46. Liang, T.P.; Lai, H.J.; and Ku, Y.C. Personalized content recommendation and user satisfaction: Theoretical synthesis and empirical findings. *Journal of Management Information Systems, 23,* 3 (Winter 2006–7), 45–70.

47. Lyytinen, K., and Yoo, Y. Research commentary: The next wave of nomadic computing. *Information Systems Research, 13,* 4 (2002), 377–388.

48. Malhotra, N.K.; 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 (2004), 336–355.

49. Margulis, T.S. Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59,* 2 (2003), 243–261.

50. Martínez-Tur, V.; Peiró, M.J.; Ramos, J.; and Moliner, C. Justice perceptions as predictors of customer satisfaction: The impact of distributive, procedural, and interactional justice. *Journal of Applied Social Psychology, 36,* 1 (2006), 100–119.

51. Miller, D.T. Disrespect and the experience of injustice. *Annual Reviews in Psychology, 52,* 1 (2001), 527–553.

52. 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 (1993), 206–215.

53. Mobile location based services: Market development, revenue opportunities, LBS applications, and key industry players. Allied Business Intelligence Inc., New York, 2008 (available at www.abiresearch.com/research/1000821-Mobile_Location-Based_Services).

54. Nunnally, J.C. *Psychometric Theory.* New York: McGraw-Hill, 1978.

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

56. Otjacques, B.; Hitzelberger, P.; and Feltz, F. Interoperability of e-government information systems: Issues of identification and data sharing. *Journal of Management Information Systems, 23,* 4 (Spring 2007), 29–51.

57. Pedersen, E.P. Adoption of mobile Internet services: An exploratory study of mobile commerce early adopters. *Journal of Organizational Computing and Electronic Commerce, 15,* 2 (2005), 203–222.

58. 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), 27–41.

59. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88,* 5 (2003), 879–890.

60. Privacy online: Fair information practices in the electronic marketplace. Report to Congress, Federal Trade Commission, Washington, DC, May 2000 (available at www.ftc.gov/reports/privacy2000/privacy2000.pdf).

61. Rao, B., and Minakakis, L. Evolution of mobile location-based services. *Communications of the ACM, 46,* 12 (2003), 61–65.

62. Sarathy, R., and Robertson, C.J. Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics, 46,* 2 (2003), 111–126.

63. Sheng, H.; Nah, F.; and Siau, K. An experimental study on U-commerce adoption: The impact of personalization and privacy concerns. *Journal of the Association for Information Systems, 9,* 16 (2008), Article 15.

64. Smith, H.J. Information privacy and its management. *MIS Quarterly Executive, 3,* 4 (2004), 201–213.

65. Smith, H.J.; Milberg, J.S.; and Burke, J.S. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20,* 2 (1996), 167–196.

66. Son, J.-Y., and Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32,* 3 (2008), 503–529.

67. Stone, E.F., and Stone, D.L. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management, 8,* 3 (1990), 349–411.

68. Story, L., and Stone, B. Facebook retreats on online tracking. *New York Times* (November 30, 2007) (available at www.nytimes.com/2007/11/30/technology/30face.html?_r=1).

69. Tang, Z.; Hu, Y.J.; and Smith, M.D. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. *Journal of Management Information Systems, 24,* 4 (Spring 2008), 153–173.

70. Tittle, C.R. *Sanctions and Social Deviance: The Question of Deterrence.* New York: Praeger, 1980.

71. TRUSTe announces first wireless privacy standards to protect mobile users. TRUSTe, San Francisco, 2004 (available at https://clicktoverify.truste.com/about/press_release/02_18_04.php).

72. Unni, R., and Harmon, R. Perceived effectiveness of push vs. pull mobile location-based advertising. *Journal of Interactive Advertising, 7,* 2 (2007) (available at www.jiad.org/article91).

73. Westin, A.F. *Privacy and Freedom.* New York: Atheneum, 1967.

74. Wold, H. Soft modeling: The basic design and some extensions. In K.G. Jöreskog and H. Wold (eds.), *Systems Under Indirect Observations: Part 2.* Amsterdam: North-Holland, 1982, pp. 1–54.

75. Zeimpekis, V.; Giaglis, M.G.; and Lekakos, G. A taxonomy of indoor and outdoor positioning techniques for mobile location services. *ACM SIGecom Exchanges, 3,* 4 (2003), 19–27.

76. Zeithaml, V.A.; Parasuraman, A.; and Malhotra, A. A conceptual framework for understanding e-service quality: Implications for future research and managerial practice. Report no. 00–115, Marketing Science Institute, Cambridge, MA, 2000.

77. Zimmermann, A.; Specht, M.; and Lorenz, A. Personalization and context management. *User Modeling and User-Adapted Interaction, 15,* 3 (2005), 275–302.

78. Zucker, L.G. Production of trust: Institutional sources of economic structure, 1840–1920. In B.M. Staw and L.L. Cummings (eds.), *Research in Organizational Behavior,* vol. 8. Greenwich, CT: JAI Press, 1986, pp. 53–111.

Appendix A: Measurement Items

BASED ON YOUR UNDERSTANDING OF LOCATION-BASED SERVICES (LBS), indicate the extent to which you agree or disagree with each statement by ticking the appropriate number.

Note: By personal information, we mean all the personal information disclosed for the purpose of using LBS, including your dynamic and real-time location information, and your static personal information such as shopping preferences, cell phone number, name, gender, and others.

Intention to Disclose Information (INT)

Specify the extent to which you would reveal your personal information to use the LBS.

Willing/unwilling (INT1)
Unlikely/likely (INT2)
Not probable/probable (INT3)

Perceived Benefits of Information Disclosure—Locatability (LOC) (1 = strongly disagree; 7 = strongly agree)

With the LBS, I am able to get the up-to-date information/services whenever I need to. (LOC1)
With the LBS, I am able to access the relevant information/services at the right place. (LOC2)
With the LBS, I can get the just-in-time information/services. (LOC3)
With the LBS, I am able to access the relevant information/services wherever I want to. (LOC4)

Perceived Benefits of Information Disclosure—Personalization (PER) (1 = strongly disagree; 7 = strongly agree)

The LBS can provide me with personalized services tailored to my activity context. (PER1)
The LBS can provide me with more relevant information tailored to my preferences or personal interests. (PER2)
The LBS can provide me with the kind of information or service that I might like. (PER3)

Perceived Risks of Information Disclosure (RISK) (1 = strongly disagree; 7 = strongly agree)

Providing the service provider with my personal information would involve many unexpected problems. (RISK1)

It would be risky to disclose my personal information to the service provider. (RISK2)

There would be high potential for loss in disclosing my personal information to the service provider. (RISK3)

Personal Innovativeness (INNV) (1 = strongly disagree; 7 = strongly agree)

If I heard about a new information technology, I would look for ways to experiment with it. (INNV1)

Among my peers, I am usually the first to try out new information technologies. (INNV2)

I like to experiment with new information technologies. (INNV3)

Prior Experience in Using Mobile Applications (EXP) (1 = never; 2 = once to three times; 3 = four to six times; 4 = seven to nine times; 5 = 10 times and above)

Indicate the number of times you had used mobile applications in the past six months.

Previous Privacy Experience (PPRE) (1 = none at all; 7 = very often/much)

How often have you personally been victim of what you felt was an invasion of privacy? (PPRE1)

How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers? (PPRE2)

Manipulation Check (MC)

Manipulation Check for Information Delivery Mechanisms (MC1) (1 = strongly disagree; 7 = strongly agree)

For pull-based LBS: With the M-coupon service, I can search for the up-to-date promotional information or coupons from my favorite stores wherever I want to.

For push-based LBS: The M-coupon service allows me to instantly receive relevant promotional information or coupons when I am near to my favorite stores.

MC for Incentives (MC2)

Did the service provider provide additional discount/rebate for using the M-coupon service? (Yes/No)

MC for Self-Regulation (MC3)

Was there a TRUSTe logo at the service provider's Web site? (Yes/No) If your answer is "no," ignore questions A and B.

A. I understand the purpose of TRUSTe's privacy seal. (1 = strongly disagree; 7 = strongly agree)
B. The service provider's privacy policy demonstrates its commitments to protect consumer privacy. (1 = strongly disagree; 7 = strongly agree)

MC for Government Regulation (MC4)

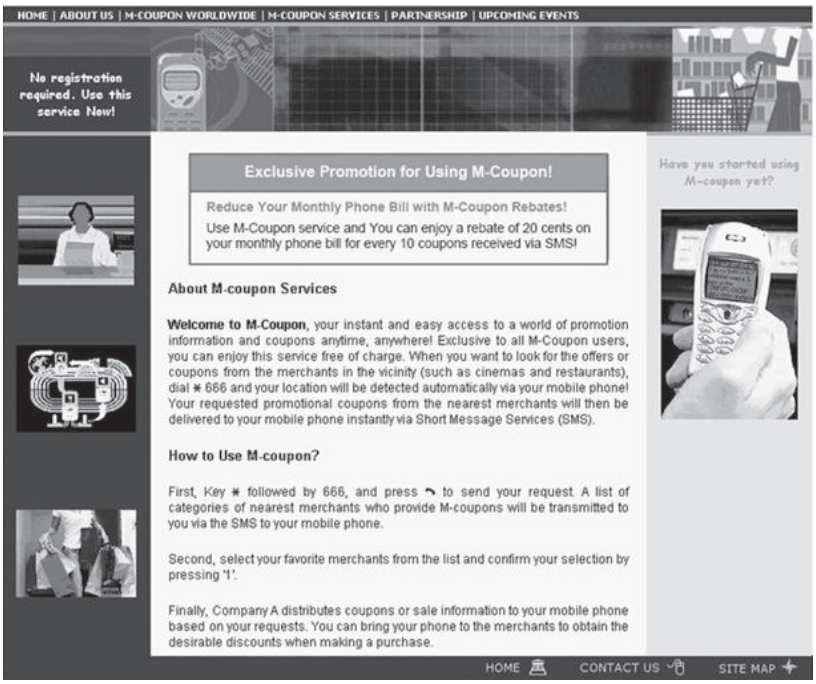
Was there a Privacy and Wireless Communications Protection Act to protect consumer's privacy in LBS? (Yes/No) If your answer is "no," ignore questions A and B.

A. I know that the Act will govern the protection of my personal information provided for using LBS. (1 = strongly disagree; 7 = strongly agree)
B. The Act will protect me from the misuse of my personal information by the service provider. (1 = strongly disagree; 7 = strongly agree)

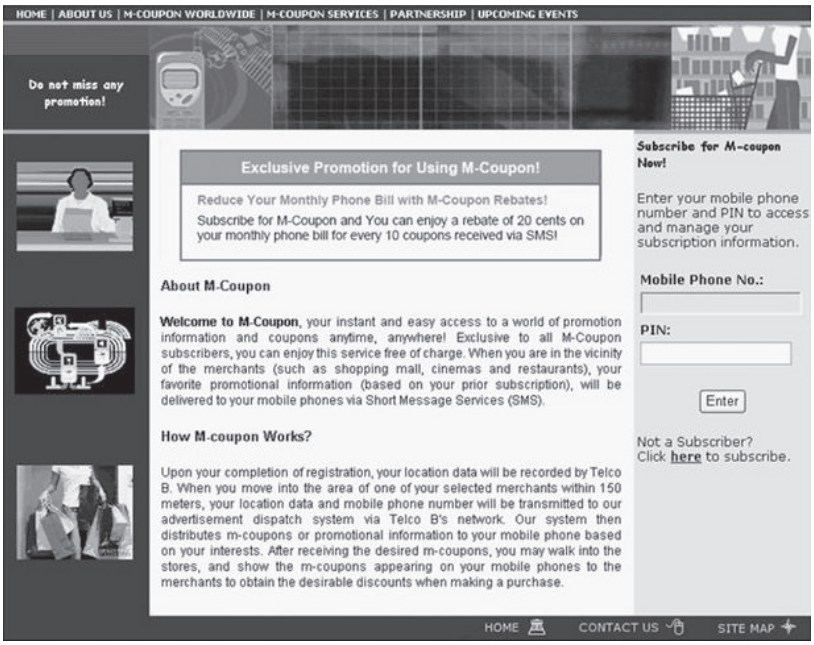
Task Check (TC) (1 = strongly disagree; 7 = strongly agree)

I feel involved when I am completing the task. (TC1)
I enjoyed completing the task. (TC2)
The role and task resemble one that I will perform in real life. (TC3)

Appendix B



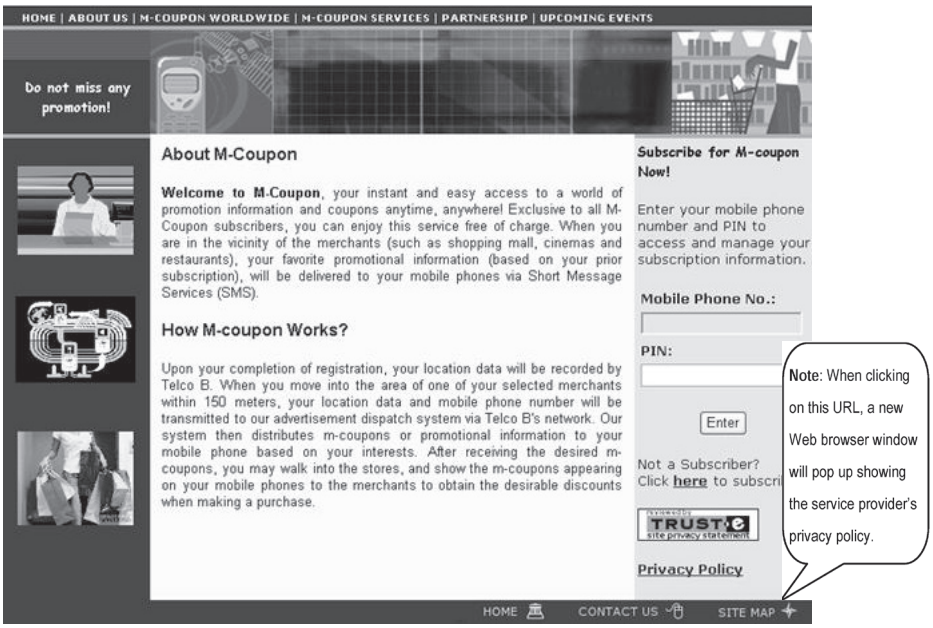
Screenshot of the Service Provider's Web Site Screen with Compensation Manipulation (Pull-Based LBS)



Screenshot of the Service Provider's Web Site Screen with Compensation Manipulation (Push-Based LBS)

Appendix C

Screenshot of the Service Provider's Web Site Screen with Self-Regulation Manipulation (Pull-Based LBS)



Screenshot of the Service Provider's Web Site Screen with Self-Regulation Manipulation (Push-Based LBS)

Appendix D

Participant Profile (n = 528)

Demographic variables/ Category	Frequency (percent)
Gender	
Male	266 (50.4)
Female	262 (49.6)
Age	
19 and below	34 (6.5)
20–24	92 (17.5)
25–29	199 (37.7)
30–34	107 (20.2)
35–39	65 (12.3)
40–49	31 (5.8)
Education	
High school or equivalent	32 (6.0)
Diploma	142 (26.9)
Bachelor's degree	238 (45.0)
Master's degree	108 (20.4)
Ph.D.	8 (1.7)
Mobile phone ownership	
Less than 12 months	43 (8.1)
12 months to 24 months	73 (13.8)
25 months to 36 months	95 (18.1)
More than 3 years	317 (60.0)
Internet usage	
Several times each week	28 (5.2)
Once per day	80 (15.2)
Several times each day	420 (79.6)
Monthly SMS usage	
Less than 10 messages	4 (0.7)
10 to 50 messages	32 (6.1)
51 to 99 messages	39 (7.4)
100 to 300 messages	244 (46.2)
More than 300 messages	209 (39.6)
Mobile application usage for the past six months*	
Never	134 (25.4)
Less than 10 times	237 (44.8)
10 to 29 times	131 (24.8)
30 to 49 times	18 (3.5)
50 times and above	8 (1.5)

* Number of times following applications were used: MMS (multimedia messaging services); downloading ring tones, logos, icons, greetings, pictures, and screensavers; participating in donations; checking information (clubbing, food, shopping, movies, horoscopes, travel, etc.); news/ information alert (business and finance, stocks, technology, sports and the entertainment scene); download/play games; participating in contests.