Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Mobile User's Privacy Decision Making: Integrating Economic Exchange and Social Justice Perspectives

Heng Xu
Penn State University, hxu@ist.psu.edu

Mary Beth Rosson
Penn State University, mrosson@ist.psu.edu

John M. Carroll
Penn State University, jmcarroll@psu.edu

Mobile User's Privacy Decision Making: Integrating Economic Exchange and Social Justice Perspectives

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

Mary Beth Rosson
College of Information Sciences and Technology
Penn State University, University Park
mrosson@ist.psu.edu

John M. Carroll
College of Information Sciences and Technology
Penn State University, University Park
jcarroll@ist.psu.edu

ABSTRACT

Recent advances in wireless computing and communication have led to the proliferation of location-based services (LBS). While LBS offer users the flexibility of accessing network services on the move, potential privacy violations have emerged as a contentious issue because details of user identities, movements and behaviors are available to LBS providers. Drawing on the economic exchange and social justice theories, this research addresses privacy issues by examining key mechanisms that can alleviate users' privacy concerns. A theoretical framework is developed to link three privacy assurance mechanisms (technology control, industry self-regulation, and government legislation) to the individual privacy decision making process. In addition, as the individual privacy decision making is usually dynamic and context-specific, the research model will be tested in three different contexts with three different types of LBS applications (safety, advertising, and social networking applications). This research contributes to a better understanding of the dynamic and dialectic nature of information privacy through a combination of theoretical and empirical research efforts. The interplay between social and technological issues associated with the privacy assurance will be the interests for application developers, service providers and policy makers.

Keywords

Information Privacy, Economic Exchange, Social Justice, Location-Based Services.

INTRODUCTION

Recent advances in mobile computing and wireless handsets make the ubiquitous information environment more of a technical reality than a distant vision. The development and enhancement of positioning technologies, such as the global positioning system 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 (Rao and Minakakis 2003). In the literature, location-sensitive applications and services that utilize geographical positioning information to provide value-added services are generally termed location-based services (LBS) (Barnes 2003).

Unsurprisingly, the increasing commercial potential and rapid growth of LBS have been accompanied by concerns over the collection and use of personal information by LBS providers. Indeed, the Big Brother imagery (Orwell 1949) looms in the popular press where LBS is discussed (Levy 2004). To respond to the call of *No LBS without L-Privacy* (Levy 2004), we aim to develop and empirically test a theoretical model that links three privacy assurance approaches (privacy-enhancing technology, industry self-regulation, and legislation) to individual privacy decision making process. In reviewing the extant literature on information privacy studies, the following controversial issues in the privacy literature become apparent:

- Although several studies have reported growing privacy concerns across US population (Ackerman et al. 1999; UCLA 2001), recent surveys, anecdotal evidence, and experiments have highlighted the apparent inconsistencies of privacy decision making and behavior (Acquisti 2004; Acquisti and Grossklags 2005; Chellappa and Sin 2005): Individuals in general value information privacy; but they are willing to trade their personal information in exchange for some economic or social rewards (Culnan 1995; Johnson and Cullen 2002). Furthermore, individuals are seldom willing to

adopt privacy assurance approaches to protect their personal information (Acquisti 2004; Acquisti and Grossklags 2005). The inconsistencies in individual privacy decision making motivate our theoretical development and empirical test of a research model that conceptualizes privacy decision making as a privacy risk-benefit analysis process.

- Although the notion of information privacy itself may sound straightforward, the individual decision process with respect to privacy is complex, multifaceted, and context-specific (Altman 1975). Information privacy management is "a process of give and take between and among technical and social entities – from individuals to groups to institutions – in ever-present and natural tension with the simultaneous need for information" (Palen and Dourish 2003, p.125). To empirically test such the contextual nature of information privacy, we consider the effects of information contexts in the research model and will test our model in three different LBS applications.

To address above challenges highlighted in the current privacy literature, we integrate research materials from the fields of computer science, marketing, social psychology and public policy to explore the process in which mobile users interact with LBS and examine how to assure users' privacy. We believe that our findings will have implications that could potentially help privacy advocates, regulatory bodies, LBS providers, system designers and merchants deliberate upon and justify their decisions on LBS.

THEORETICAL INVESTIGATION OF PRIVACY DECISION MAKING

Information Privacy: A Calculus Perspective

Within the robust body of research that attempts to understand the nature of information privacy it has been found that the *calculus* perspective of information privacy is "the most useful framework for analyzing contemporary consumer privacy concerns" (Culnan and Bies 2003). This perspective reflects an implicit understanding that privacy is not absolute (Klopfer and Rubenstein 1977); rather, the individual's privacy interests can be interpreted based on a "calculus of behavior" (Laufer and Wolfe 1977). In a commercial context, consumers can be expected to behave as if they are performing a privacy calculus (i.e., risk-benefit analysis) in assessing the outcomes they will receive as a result of providing personal information to corporations (Culnan and Armstrong 1999; Culnan and Bies 2003; Milne and Rohm 2000; Sheehan and Hoy 2000).

Consistent with the core ideas of a privacy calculus, the exchange theory (Bagozzi and Fornell 1982; Houston and Gassenheimer 1987) may further help predict how individuals make decisions regarding the revelation of personal information (Culnan and Bies 2003). This theory characterizes three classes of exchange: utilitarian, symbolic or mixed (Bagozzi 1975). A utilitarian exchange is an interaction whereby goods are given in return for money or other goods (Bagozzi 1975), and it is considered the 'first exchange' (Culnan and Bies 2003, p. 326). A 'second exchange' takes place, whereby consumers' personal information is given in return for value such as higher quality service and personalized offers or discounts, and this concept may be used to explain the privacy calculus (Culnan and Bies 2003).

Applying the second exchange framework to LBS usage behavior, we may interpret the usage of LBS as an exchange where consumers disclose their personal information in return for the benefits (e.g., timely personalized services/information based on the consumer's location) 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 information disclosure (Culnan and Bies 2003). In the study of individual decision making (i.e., risk and benefit factors), we note that there exists a wealth of e-commerce literature on the uncertainties of the online environment (Gefen et al. 2003; Jarvenpaa et al. 2000; McKnight et al. 2002; Pavlou and Gefen 2004). However, these studies tend to focus on individual risk belief in general, with privacy risk being frequently overlooked (Davison et al. 2003). In this respect, the second exchange theory intertwined with the notion of privacy calculus should provide greater explanatory power. We further integrate the privacy calculus notion with the social justice theoretical perspective to argue that the privacy calculus, at the individual level, could be differentiated according to the extent to which justice provisions are manifested in privacy actions and regulations (Caudill and Murphy 2000; Culnan 2000; Culnan and Bies 2003).

Information Privacy: A Social Justice Lens

The *justice* perspective has been proposed as a useful theoretical framework for analyzing individual privacy calculus (Culnan and Bies 2003). We argue that 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 trust that lead to a positive outcome of their privacy calculus and a greater willingness to disclose personal information (Culnan and Bies 2003).

In this research, we view privacy-enhancing technologies (PETs), industry self-regulation, and government legislation as three important variables that shape users' justice perceptions and exert direct effects on privacy risks. We argue that the presence of PETs, industry self-regulation or government legislation ensures that justice perceptions will prevail, thereby yielding positive beliefs among users regarding the outcome of their privacy calculations.

RESEARCH MODEL

Based on our discussion of the privacy calculus, economic exchange and social justice theories, we present our research model for explaining users' willingness to disclose personal information in LBS (see Figure 1). At the core of the model is the privacy calculus, comprising perceived privacy benefits and privacy risks.

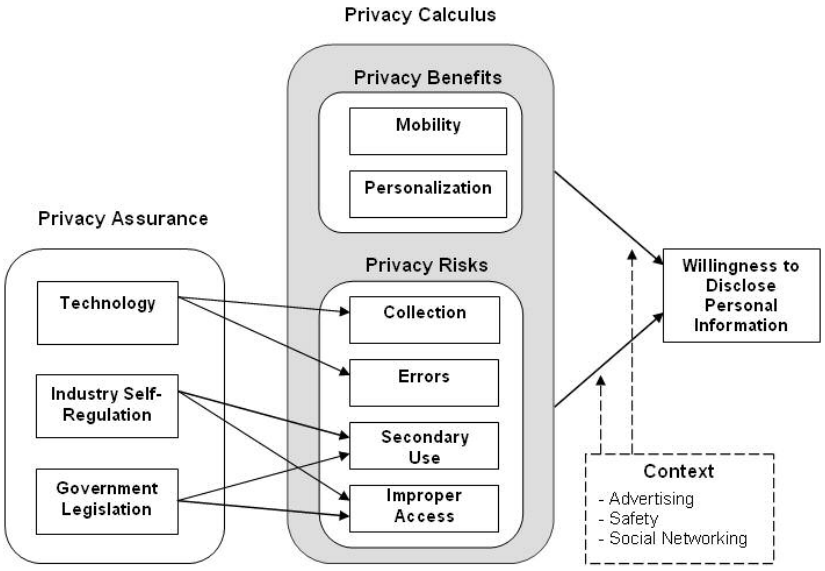

Figure 1. The Research Model

Disclosure-Privacy Benefits

In Figure 1, we see that the anticipation of privacy benefits is expected to have a positive influence on willingness to disclose personal information. Following prior research, we identify three types of anticipated benefits: time-dependent value, location-dependent value, and user-dependent value (Barnes 2003; Junglas and Waston 2003b). Time-dependent value and location-dependent value may be conflated into one dimension: mobility. A key appeal of LBS is that it provides nomadic users with flexible and timely information/services that would otherwise not be available in the conventional commercial realm (Beinat 2001a; Lyytinen and Yoo 2002; Wallace et al. 2002). Indeed, a primary motivation for using LBS is the inherent mobility enabled by positioning and timeliness. Through LBS, consumers are able to access needed information/services at any time from anywhere, and in turn, are reachable at the right time in the right place (Junglas and Waston 2003b; Lyytinen and Yoo 2002). Therefore, mobility, valued by many people (Barnes 2003; Lyytinen and Yoo 2002; Wallace et al. 2002), is a key advantage used to entice consumers to exchange their personal information for gaining flexible access to needed information or services at the right time and place.

The other key anticipated benefit of LBS is user-dependent value or personalization. Users may be motivated to disclose their personal information in exchange for personalized services. LBS can obviously be personalized as 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 smart 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. Personalization, as one important dimension of perceived benefits identified by prior studies (Junglas and Watson 2003a; Lyytinen and Yoo 2002; Wallace et al. 2002), is gained when LBS are tailored to individual customers' identities, interests, locations, and the time of the day.

Disclosure-Privacy Risks

In the LBS context, since mobile communication and positioning technologies increasingly expand the ability for firms to collect, process and exploit personal data, privacy risks are broadly regarded as the major inhibiting factor in the adoption of

LBS (Beinat 2001b; Gidari 2000; Wallace et al. 2002). Following Featherman and Pavlou (2003), we define perceived privacy risks as the expectation of losses associated with the release of personal information to the LBS service provider. Users are vulnerable to at least four kinds of risks if their personal information is not used fairly or responsibly (Culnan and Armstrong 1999; Hudson and Smith 1996). First, the very act of *data collection*, whether it is legal or illegal, is the starting point of privacy concerns (Hudson and Smith 1996; Malhotra et al. 2004). The degree to which a person is concerned about privacy risks are closely related to the amount of individual-specific data collected and possessed by others. Second, as computerized information may be readily duplicated and shared, a consumer is vulnerable to the risk that the personal information provided is being put to *secondary use* for purposes unrelated to that for which the information was originally provided (Culnan and Armstrong 1999; Smith et al. 1996). Third, since positioning and timeliness are the primary value provided by LBS, *errors* in personal identifiable and location information may lead to inaccurate provision of LBS and inconvenience for the users. Fourth, a consumer may perceive that her privacy is invaded if *improper access* is made to her personal information as a result of a security breach or in the absence of appropriate internal controls (Culnan and Armstrong 1999; Smith et al. 1996).

To summarize, individuals are likely to agree to give up a degree of privacy in return for potential benefits related to mobility and personalization. However, improper handling of personal information could result in the discovery and matching of location data and identity. Consumers may not want to use LBS if they sense that their personal information is not effectively protected and there exist high risks of privacy invasion. In general, perceived privacy benefits are positively related to willingness to disclose personal information in LBS; perceived privacy risks are negatively related to willingness to disclose personal information in LBS.

Privacy Benefit/Risk Analysis: the Role of Information Context

The individual decision process with respect to privacy benefit/risk analysis is complex, multifaceted, and context-specific. Altman (1975) conceptualized privacy decision-making as a dialectic and dynamic boundary regulation process. As a *dialectic* process, privacy is "conditioned by individuals' own experiences and social expectations, and by those of others with whom they interact" (Palen and Dourish 2003). As a *dynamic* process, privacy is "understood to be under continuous negotiation and management, with the boundary that distinguishes privacy and publicity defined according to circumstance" (Palen and Dourish 2003). Accordingly, it seems reasonable to argue that the outcome of privacy calculus (i.e., privacy benefit/risk analysis) differs among different information contexts. For example, the usage of the location-based tracking applications such as tracking their children or elder family members may lead to a positive outcome of their privacy calculus and hence higher willingness to disclose location information. While the usage of location-based advertising application (e.g., sending PizzaHut coupons based on cell-phone location tracking) may lead to a negative outcome of their privacy calculus and hence lower willingness to disclose location information.

Because of such context-specific nature of privacy calculus, parameter estimates in the model (e.g., factor mean levels, path coefficients) may not necessarily be the same among different information contexts. As such, we specifically consider how this difference in information context may affect the outcome of privacy calculus:

> **Proposition 1a:** *The positive influence of perceived privacy benefits on willingness to disclose personal information in LBS should be different in different information contexts.*
>
> **Proposition 1b:** *The negative influence of perceived privacy risks on willingness to disclose personal information in LBS should be different in different information contexts.*

Suggested by Margulis (2003a), the following three tensions that govern information privacy management in three different contexts will be studied: 1) *Government-Citizen*. The emergency and rescue service, which is able to locate an individual who is either unaware of his/her exact location or is not able to reveal it because of an emergency situation (e.g., injury, criminal attack, and so on), will be studied in this research. 2) *Merchant-Consumer*. Location-based advertising will be studied in this research. Advertisers could deliver contextually appropriate advertising messages through wireless devices on a geographically-targeted basis and could reach mobile users when they are most likely to make a purchase. 3) *Social networking* within certain small social groups (e.g., friends, family, or other members with close relationship of a particular group). Location-based buddy finder service will be studied in this research.

Privacy Assurance through Privacy-Enhancing Technologies

Empirical evidence lends support for the importance of assuring privacy through PETs (Xu et al. 2005). In the context of LBS, the rapid development of mobile communication and device technologies provides the possibility of building PETs into mobile devices, and hence, consumers can exercise personal control over their information disclosure from their own hands.

For example, a Privacy Awareness System developed by Langheinrich (2002) could implement privacy control mechanisms that support notice, choice and consent, proximity and locality. According to Anuket (2003), mobile consumers are able to limit the amount of location information collected by the service providers in a timely fashion. Consumers can turn off the subscribed LBS just by clicking some buttons on their mobile devices anytime when they want to.

It seems reasonable to expect that PETs should directly instill greater consumer justice perception by limiting the amount of information disclosed to the LBS provider in a timely fashion; thereby reduce the consumer's privacy risk perceptions (Culnan and Bies 2003). However, recent studies (Turner and Dasgupta 2003; Xu et al. 2005) critiqued that most of the current PETs only provided users with the privacy options of *notice* (i.e., notifying users whether a firm's privacy policy conflicts with users' privacy preferences) and *choice* (i.e., allowing users to make decisions on whether to provide personal information or to correct data errors). Most of PETs lack the *enforcement* mechanism to ensure firms act according to their privacy policies (Turner and Dasgupta 2003; Xu et al. 2005). Hence, when consumer privacy is invaded if *improper secondary use* or *unauthorized access* is made to their personal information, PETs could neither provide the means of recourse for the aggrieved, nor create strong incentives for firms to refrain from opportunistic behavior and behave appropriately. Therefore, we propose:

> **Proposition 2:** *The privacy assurance approach through privacy-enhancing technologies should lead to lower perceived privacy risks with regard to* ***collection*** *and* ***error****.*

Privacy Assurance through Industry Self-Regulation

Self-regulation involves the setting of standards by an industry group or certifying agency and the voluntary adherence to the set standards by members or associates (Culnan and Bies 2003). Groups such as TRUSTe and Online Privacy Alliance (OPA)[1] have been active as third-party entities ensuring justice and promoting trustworthiness to web sites through seals of approval. These self-regulatory efforts specifically address fair information practices with participating firms agreeing to provide notice, choice, access, security and enforcement, and thus encouraging consumers to believe that a particular participating firm's information practices are fair (Culnan and Armstrong 1999). Therefore, firms that conform to the industry's self-regulation practices could enhance consumers' justice perceptions, and thereby provide consumers with positive belief on the outcome of their privacy calculation.

In the context of the wireless industry, to facilitate self-regulation, the Wireless Location Industry Association (WLIA) is in the process of establishing guidelines that govern the use and compilation of personally identifiable data linked to location, and prescribing responsible practices in the emerging wireless location industry (WLIA 2001). TRUSTe announced the launch of its Wireless Privacy Principles and Implementation Guidelines on February 18, 2004, which provide vendors serving the mobile market with practical guidelines for protecting consumer privacy, and is in the process of developing a wireless version of its seal (TRUSTe 2004). Previous studies have shown that businesses that conform to the industry's self-regulation practices instill greater consumer confidence and justice perception, thereby lowering consumers' perceived privacy risks in using LBS (Culnan and Armstrong 1999).

As discussed earlier, we suggest that PETs lack the mechanisms to alleviate consumer privacy risks with regard to *improper secondary use* and *unauthorized access*. The literature on institutional structures (e.g., McKnight et al. 1998; Pavlou and Gefen 2004) may help explain the positive effects of industry self-regulation in mitigating privacy risk perception with regard to *improper secondary use* and *unauthorized access*. First, the structures built into the firm's web site, such as the privacy policy and privacy seal could assure people that everything in the setting is as it ought to be (McKnight et al. 1998), allowing consumers to form and hold beliefs about positive outcomes (Johnson and Cullen 2002). Second, when violation occurs, these structures could provide the means of recourse for the aggrieved (Johnson and Cullen 2002; McKnight et al. 1998), thereby creating strong incentives for firms to refrain from opportunistic behavior and behave appropriately. Hence, we predict:

> **Proposition 3:** *The privacy assurance approach through industry self-regulation should lead to lower perceived privacy risks with regard to* ***secondary use*** *and* ***improper access****.*

Privacy Assurance through Government Legislation

Privacy assurance through government legislation, which embodies the strong institutional structural assurances provided by government agencies (Pavlou and Gefen 2004; Zucker 1986), has been proposed to have a major positive impact on privacy

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

perceptions (Culnan 2000). Legislative efforts to implement fair information practices could specifically address concerns regarding fairness and accountability for privacy protection actions, thereby providing consumers with a sense of security (Zucker 1986). With the legal structures in place, consumers could believe that firms would conform to the fair information principles as regulated by legislation, and that disclosing personal information in such an environment would be safe. Therefore, the presence of government legislation on privacy protection contributes to justice perceptions, promoting positive beliefs among consumers.

In the wireless context, location privacy legislation has received a boost from the US E911 Phase II obligations. In the Wireless Communications and Public Safety Act (WCPSA) of 1999, US legislators suggested that wireless location Customer Propriety Network Information (CPNI) be subject to limitation in its disclosure under the Communication Act of 1996. Simultaneously, the US Congress amended Section 222 to explicitly require "express prior authorization" before the user of a commercial mobile service can be deemed to have consented to the use, disclosure or access to wireless location information[2]. A similar path was taken by the European Commission in a directive (COM 2002) on the "processing of personal data and protection of privacy in the electronic communication sector". It explicitly includes location privacy and requires that location data be used only with the consent of the subscriber and only for the duration necessary to provide the specified services, and that the user be provided simple means to temporarily deny the processing of her location data. Therefore, legislation on location data protection should directly instill greater consumer justice perception and thereby lower the level of risk related to location information disclosure.

Deterrence theory has a direct bearing on the possible effects of government legislation on mitigating privacy risk perception with regard to *improper secondary use* and *unauthorized access*. Deterrence theory is predicated on the assumption that illegal behavior can be deterred through the threat of punishment (Gibbs 1986; Tittle 1980). Hence, one objective of a legal system as the preventive function of law is to set forth guidelines for human conduct that will cause people to behave by choice as society wants them to behave (Spiro and Houghteling 1981). Recognizing the deterrent effectiveness of a legal system, consumers may perceive lower risks in personal information disclosure when using LBS. Hence, we predict:

> **Proposition 4:** *The privacy assurance approach through government legislation should lead to lower perceived privacy risks with regard to* ***secondary use*** *and* ***improper access****.*

Control Variables

Prior research on adoption, consumer behavior, information privacy, and trust studies suggests a number of additional factors should be included as control variables because of their potential influence on perceived privacy benefits, privacy risks and willingness to disclose personal information. They are: *general privacy attitudes* (Culnan 1993), *personality traits* (Smith et al. 1996), *disposition to trust* (McKnight and Chervany 2002; McKnight et al. 2002), *prior experience with mobile applications* (Culnan 1995), *previous privacy experience*(Hudson and Smith 1996; Stone and Stone 1990), and *personal innovativeness* (Agarwal and Prasad 1998).

RESEARCH METHOD

Design

We will conduct an experiment to test the proposed research model as this approach supports the testing of causal relationships between manipulated and theoretical constructs with minimal interference from extraneous variables. We will use a 3 (within factor: privacy assurance mechanisms – PETs/self-regulation/legislation) × 3 (between factor: context – safety/advertising/social networking) factorial experiment design. Based on the pre-investigations conducted in the pilot study, PETs, self-regulation and legislation will be manipulated to create the environment in which potential LBS users would have to make their privacy decisions.

PETs will be manipulated by introducing a mobile device with an interactive graphical user interface for turning on/off the subscribed LBS anytime when the user wants to. *Self-regulation* will be manipulated by providing a TRUSTe seal and a URL linked to a simulated LBS provider's privacy policy on its Web site. A brief introduction explaining TRUSTe's mission will be provided in the privacy policy. *Legislation* will be manipulated by informing the subjects that LBS transactions are governed by related location privacy protection laws. The subjects belonging to the legislation treatment group will also be presented with a piece of local news reporting that LBS transactions are governed by recently activated location privacy protection law. *Information contexts* will be manipulated by simulating the LBS usage in terms of safety, advertising and

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

social networking applications in the experiment. We will carry out pilot tests to ensure that the manipulations will be anchored at the appropriate level to be able to detect differences, to modify and finalize the instrument, and to refine the experimental procedures and instructions.

Subject

We will recruit over 300 experiment participants from undergraduate students at a large, northeastern university. Our recruiting messages will explain who we are and what we were trying to do (i.e., the purpose of this study), and invite subjects' participation. Respondents will be asked to click on the URL link provided in the posted message, which will link to the online experiment. The invitees will be assured that the results will be reported only in aggregate and that their anonymity will be ensured.

Each subject will be randomly assigned to one of the three LBS usage scenarios (safety, advertising and social networking). Our web-based experiment system will generate the scenarios randomly so that each respondent has an equal and independent chance of being put into any of the three scenarios. The subject will then be given a scenario that asks him/her to assume the role of a potential LBS user and will be presented with one of three different LBS applications. At the final stage of the experiment, subjects will be asked to complete a questionnaire regarding their perceptions of privacy benefits and risks, and their willingness to disclose personal information in LBS in each specific scenario.

FUTURE WORK AND CONCLUSION

Currently, we are in the process of data collection. At AMCIS, we should be able to present our results and findings. Upon collecting the data, we will first perform manipulation check to ensure that participants attended to their assigned experimental conditions. Next we will analyze them using multigroup structural equation modeling (SEM) techniques. The statistical techniques selected for multigroup SEM will be Partial least squares (PLS). We will use PLS to perform confirmatory factor analysis to assess validity of all multi-item research constructs. The validity of the constructs will be assessed in terms of unidimensionality, convergent validity, internal consistency, and discriminant validity. After establishing the validity of the measures, we will extract the statistically significant relationships and test the research propositions.

This research will have important implications for both researchers and practitioners. First, this project will enrich the information privacy literature by integrating economic exchange and justice theories which will unpack the nature of information privacy in the LBS context. Second, our findings will shed some light on the controversial issues surrounding the role of technology versus industry self-regulation versus government legislation in ensuring information privacy. Particularly, the modeling of three privacy assurance approaches will allow the focus of attention to shift from a general discussion of the potential privacy invasion inherent in LBS to a more granular level of analysis on how to effectively alleviate users' privacy risk perceptions. Third, although we focused on the LBS context, the theoretical framework, the evaluation methodologies and experiment systems developed in this research will be made available for future undertakings. Finally, several practical recommendations to the various players in the LBS landscape—service providers, privacy advocates, industry self-regulators, and government legislators—will be fueled by the results of this study.

ACKNOWLEDGMENT

This research has been supported by a research grant from the National Science Foundation (NSF-CNS 0716646). The authors like to thank Hock Hai Teo, Bernard Tan and Ritu Agarwal for their valuable help on an earlier version of this research.

REFERENCE:

Ackerman, M., Cranor, L., and Reagle, J. "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," Proceeding of The 1st ACM Conference on Electronic Commerce ACM Press, Denver, Colorado, 1999, pp. 1-8.

Acquisti, A. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," Proceedings of the 5th ACM Electronic Commerce Conference, ACM Press, New York, NY, 2004, pp. 21-29.

Acquisti, A., and Grossklags, J. "Privacy and Rationality in Decision Making," *IEEE Security and Privacy* (January/February) 2005, pp 26-33.

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

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

Anuket, B. "User Controlled Privacy Protection in Location-Based Services," University of Maine, Orono, ME, 2003.

Bagozzi, R.P. "Marketing as Exchange," *Journal of Marketing* (39), October 1975, pp 32-39.
Bagozzi, R.P., and Fornell, C. "Theoretical Concepts, Measurement, and Meaning," C. Fornell (ed.), Praeger Publishers, Westport, CT, 1982.
Barnes, J.S. "Known by the Network: The Emergence of Location-Based Mobile Commerce," in: *Advances in Mobile Commerce Technologies,* E.-P. Lim and K. Siau (eds.), Idea Group Publishing, Hershey, PA, 2003, pp. 171-189.
Beinat, E. "Location-based Services - Market and Business Drivers," *GeoInformatics*), April 2001a, pp 6-9.
Beinat, E. "Privacy and Location-based: Stating the Policies Clearly,," *GeoInformatics*), September 2001b, pp 14-17.
Caudill, M.E., and Murphy, E.P. "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing* (19:1) 2000, pp 7-19.
Chellappa, R.K., and Sin, R. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6:2-3), forthcoming 2005.
COM. 2002. Processing of personal data and protection of privacy in the electronic communication sector (Data Privacy Directive) European Union. Retrieved Jan 1, 2007, http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf.
Culnan, M.J. "'How Did They Get My Name'? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3) 1993, pp 341-364.
Culnan, M.J. "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing* (9), Spring 1995, pp 10-19.
Culnan, M.J. "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing* (19:1) 2000, pp 20-26.
Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), Jan-Feb 1999, pp 104-115.
Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2) 2003, pp 323-342.
Davison, M.R., Clarke, R., J., S.H., Langford, D., and Kuo, F.-Y. "Information Privacy in a Globally Networked Society: Implications for IS Research," *Communications of the Association for Information Systems* (12) 2003, pp 341-365.
Featherman, M., and Pavlou, P. "Predicting e-services adoption: a perceived risk facets perspective," *Int. J. Human-Computer Studies* (59) 2003, pp 451-474.
Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in online shopping: an integrated model," *MIS Quarterly* (27:1), March 2003, pp 51-90.
Gibbs, J.P. "Deterrence Theory and Research," in: *Law as a Behavioral Instrument,* G. Melton (ed.), University of Nebraska Press, Lincoln, 1986.
Gidari, A. "No 'L-Commerce' Without 'L-Privacy' : Fair Location Information Practices for Mobile Commerce," in: *L-Commerce 2000-the Location Services & GPS Technology Summit*, Washington, D.C., 2000.
Houston, S.F., and Gassenheimer, B.J. "Marketing and Exchange," *Journal of Marketing* (51) 1987, pp 3-18.
Hudson, S.E., and Smith, I. "Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems," Proceedings of Computer Supported Cooperative Work'96 Conference, ACM Press, New York, 1996, pp. 248-257.
Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. "Consumer Trust in an Internet Store," *Information Technology and Management* (1:12) 2000, pp 45-71.
Johnson, L.J., and Cullen, B.J. "Trust in Cross-Cultural relationships," in: *The Blackwell Handbook of Cross-Cultural Management,* M.J. Gannon and K.L. Newman (eds.), Blackwell, Oxford, UK, Malden, Mass, 2002, pp. 335-360.
Junglas, I.A., and Waston, R.T. "U-Commerce: A Conceptual Extension of E-Commerce and M-Commerce," Proceedings of 24th Annual International Conferences on Information Systems (ICIS 2003), Seattle, United States, 2003b, pp. 667-677.
Junglas, I.A., and Watson, R.T. "U-Commerce: An Experimental Investigation of Ubiquity and Uniqueness," Proceedings of 24th Annual International Conferences on Information Systems (ICIS 2003), Seattle, United States, 2003a, pp. 414-426.
Klopfer, P.H., and Rubenstein, D.L. "The concept privacy and its biological basis," *Journal of Social Issues* (33) 1977, pp 52-65.
Langheinrich, M. "A Privacy Awareness System for Ubiquitous Computing Environments," The Fourth International Conference on Ubiquitous Computing, Springer-Verlag LNCS 2498, 2002, pp. 237-245.
Laufer, R.S., and Wolfe, M. "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues* (33) 1977, pp 22-41.
Levy, S. 2004. A Future With Nowhere to Hide? Newsweek. Retrieved Jan 1, 2007, http://www.msnbc.msn.com/id/5086975/site/newsweek/.

Lyytinen, K., and Yoo, Y. "Research Commentary: The Next Wave of Nomadic Computing," *Information Systems Research* (13:4), December 2002, pp 377-388.

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

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

McKnight, D.H., and Chervany, N.L. "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce* (6:2) 2002, pp 35-59.

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

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

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

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

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

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

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

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

Smith, H.J., Milberg, J.S., and Burke, J.S. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June 1996, pp 167-196.

Spiro, W.G., and Houghteling, L.J. *The Dynamics of Law*, (2nd ed.) Harcourt Brace Jovanovich, New York, 1981.

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, pp 349-411.

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

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

UCLA. 2001. The UCLA Internet report 2001: Surveying the digital future. UCLA Center for Communication Policy. Retrieved Jan 1, 2007, http://ccp.ucla.edu/pdf/UCLA-Internet-Report-2001.

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

WLIA. 2001. Draft WLIA Privacy Policy Standards (first version). Wireless Location Industry Association. Retrieved April 1, 2005, http://www.wliaonline.com/indstandard/privacy.html

Xu, H., Teo, H.H., and Tan, B.C.Y. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," Proceedings of 26th Annual International Conference on Information Systems (ICIS 2005), Las Vegas, NV, 2005, pp. 897-910.

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