2014 47th Hawaii International Conference on System Science

Location Based Services and Information Privacy Concerns among Literate and Semi-Literate Users

Adrian Z.Y. Tan
National University of Singapore
adrianzy@comp.nus.edu.sg

Wen Yong Chua
National University of Singapore
wenyong@comp.nus.edu.sg

Klarissa T.T. Chang
National University of Singapore
changtt@comp.nus.edu.sg

Abstract

Location-based services mobile applications are becoming increasingly prevalent to the large population of semi-literate users living in emerging economies due to the low costs and ubiquity. However, usage of location-based services is still threatened by information privacy concerns. Studies typically only addressed how to mitigate information privacy concerns for the literate users and not the semi-literate users. To fill that gap and better understand information privacy concerns among different communities, this study draws upon theories of perceptual control and familiarity to identify the antecedents of information privacy concerns related to location-based service and user literacy. The proposed research model is empirically tested in a laboratory experiment. The findings show that the two location-based service channels (push and pull) affect the degree of information privacy concerns between the literate and semi-literate users. Implications for enhancing usage intentions and mitigating information privacy concerns for different types of mobile applications are discussed.

1. Introduction

Location-based services (LBS) mobile applications have created many opportunities for diverse communities to receive customize content via their mobile devices. Usage of LBS is often impended by individuals' information privacy concerns [42]. In the LBS context, individuals worry about the breach of their location information [45]. Such feelings give rise to concerns about information privacy, which refers to "the ability of the individual to personally control information about one's self" [34]. Information privacy concerns refer to the ability to control how personal information is acquired and used [41]. While LBS takze advantage of spatial, temporal and personal information of users to customize mobile experience, users may view this as an invasion of privacy [11]. Hence, we need to understand the key sources of information privacy concerns to prescribe how they can be mitigated to improve usage intentions.

"LBS are services in which the location of a person or an object is used to shape or focus the application or service" [15]. The push channel is one channel to deliver LBS [3, 29, 39, 45]. In the push channel, the delivery of LBS is done by implicitly monitoring the users' activities at different locations over time [3, 29, 39, 45]. This approach may raise stronger information privacy concerns [44] as individuals do not feel to be in control over the discourse of their personal information [11, 12, 28, 43]. On the other hand, the pull channel delivers LBS where and when the user explicitly initiates the request [3, 29, 39, 45]. Individuals have to feel to be in control of their information in order to protect information privacy [43] so it is important to examine what affects individuals' to feel in control of their information.

Existing information privacy literatures typically target at the literate users to explain how control affects individuals' information privacy concerns. However, the widespread usage of mobile devices among billons of subscribers living in the rural areas of emerging economies [24] means that half of the population is semi-literate and uses only simple functions on their mobile phones for synchronous voice communications [7]. Literacy is notoriously difficult to define as it varies from context to context [23]. Literacy can be generally defined as "the ability to read, write, communicate and comprehend". Thomas and Maria-Helena [38] defined literate as one who "can read and write easily" and semi-literate as one who is "able to read and write with difficulty". Education level is one of the dimensions that separate a literate and semi-literate [37]. Sheehan [32] found that individuals with higher educational level are more concern about information privacy than those with lower educational level. With information communication technologies, literacy is defined as "the knowledge and ability to use information and communication technologies" [23].

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.394

Another dimension that differentiates the literate and semi-literate user is the knowledge and ability to use information communication technologies. The literate users are people who can use information communication technologies efficiently. The semi-literate users are people who have very minimal information and communications technology skills [23] Our work is novel as existing studies has not examined how literacy level will cause individuals to feel in control of their information when using LBS.

Motivated by the differences between the literate and semi-literate users, as well as the LBS delivery mechanism that affect information privacy concerns and usage intentions, our study aims to answer the following questions:

1. What are the impacts of literacy on information privacy concerns?
2. Are information privacy concerns related to usage intentions?

This study provides theoretical contributions into the information privacy literatures in several ways. First, we provide insights on how LBS and information privacy concern is contingent on literate / semi-literate users. Second, we provide insights on how one technological attributes impacts privacy concerns of literate / semi-literate users. Third, we expand the knowledge about information privacy from individuals into user groups.

This study provides practical contributions to the stakeholders involved in the LBS context. First, LBS designers can benefit by learning which delivery mechanisms to implement for the literate / semi-literate users. Second, we let users gain an understanding about the mechanism behind LBS so they can better protect themselves. Third, policymakers can formulate specific policies to protect different group of users based on their needs and concern for information privacy.

2. Theory

2.1. Perceptual Control Theory

Powers [26] introduced the Perceptual Control Theory (PCT) which is a self-regulatory framework based on control system engineering which provides an integrative theoretical account of human behavior. The PCT posits that there are four key principles of human functioning and behavior; control, hierarchical organization, conflict and reorganization. According to the PCT, individuals' behavior is caused by their control of perception [5]. For example, individuals have a standard for how close we like to stand to others. If an individual encountered an experience that does not meet the standard, or went beyond the standard, the individual will try to change and meet the standard.

To further understand control, we need to understand where the goals (also called internal standards) come from. The PCT posits that goals are set within individuals. Individuals may set sub-goals to achieve one main goal. For instance, an individual may want his personal computer to be virus free. This goal does not trigger any kind of behavior, but it set sub-goals like not opening email attachments. This may cause conflict between goals. In this example, the individual may have to open an email attachment that his boss has emailed him.

To resolve the conflict, the PCT posits that reorganization which is a trial-and-error learning process that randomly alters the way individuals perceive the environment and set their goals until they managed to achieve them. In the example above, the individual may install anti-virus software which scan email attachments, or use the office computer to open the attachment.

We apply the PCT to help us explain the relationship between LBS usage intention and information privacy concerns. Privacy theorists have defined information privacy in terms of control [e.g. 34, 41]. Having a loss of control over information is similar to the notion of privacy invasion [34]. Previous studies on LBS [e.g. 42, 44, 45] suggested that LBS create values for individuals but simultaneously cause individuals to feel a loss of control over their location information. This creates a conflict of goals. An individual has to decide whether to use LBS for the benefits and risk a possible privacy invasion, or to maintain information privacy.

In the reorganization phase, individuals can completely avoid the use of LBS, or to learn more about LBS and its providers. For example, individuals can read up on the privacy policy before using the LBS. The individual will stop the reorganization process when what the individual experience what the individual perceives. Previous studies on LBS [e.g. 45] have also suggested that individuals feel a greater loss of control when LBS are delivered via the push channel.

2.2. Familiarity

The familiarity perspective is a useful theoretical lens for understanding the moderating effects of user expertise on the relationships between personalization and information privacy concerns. Familiarity is the individual's understanding of another, often based on previous interactions, experience, and learning of "the what, who, how, and when of what is happening" [16]. Hence, individuals' familiarity of LBS comes with the direct experience of receiving LBS from the provider [21]. Familiarity reduces the uncertainty of expectation through increased understanding of what has happened in the past [22]. An individual's privacy concern is influenced by past privacy experience [35, 44, 45, 46].

Using the lens of familiarity, a literate user is one who has more experience in using LBS than semi-literate users. If a literate user has been exposed to or was the victim of personal information abuses through mobile application, the user will have a stronger concern about information privacy [32, 44]. On the other hand, if the expert user has not been victimized by privacy breaches through LBS, the user will have a weaker concern about information privacy than novice users. Culnan [10] suggests individuals are less likely to consider it as privacy-invasive when information is collected on an existing relationship.

2.3. Hypotheses

The literate users can read and write more fluently as compared to the semi-literate users. The literate users have better in using information communication technologies. Hence, they are able to obtain information easily and become more aware about the risk involved when using LBS. With the greater awareness regarding the risk involved, the literate users will have a greater concern over information privacy. Hence, we hypothesize:

- H1: Literate users will have a higher degree of concern for information privacy than the semi-literate users.

The use of LBS causes individuals to feel a loss of control over their location information [44, 45]. Individuals have to decide whether they want the benefits that LBS provide or control their location information. The PCT posits that individuals will reorganize their goals whenever there are conflicting goals. This process will stop only when individuals experience what they expect. Individuals who want to control their location information are less likely to use LBS as this creates conflicting goals. Hence, we hypothesize

- H2: The concern for information privacy will not lead to usage than without.

3. Methodology

3.1. Research Design

We conducted a laboratory experiment with 200 subjects to test our hypotheses. We have a 2 (push / pull LBS) by 2 (literate / semi-literate users) factorial design. We developed a mobile agricultural application, mPest, running on the Android platform for the experiment.

3.2. Prototypes of Mobile Application

The mobile agricultural application, mPest, was developed using the native Android platform. In this experiment, we hope to stimulate an environment that is similar to the actual usage. Hence, network connectivity and the GPS embedded in the mobile device must be enabled for mPest to work. mPest works on a client-server architecture where the mobile application will take in input from the user and send it back to the server. Then, the web application residing at the server processes the request and stores the data into the database.

3.3. Participants

A total of 200 literate and 200 semi-literate users participated in our study. The literate users were undergraduate students in a large university. The semi-literate users were farmers in their home country and have an education level of up to high school. They own feature phones.

Table 1. Demographic Information of Subjects

Gender		Literate	Semi-literate	Total
	Female	46	42	88
	Male	34	38	72
Age	20 – 24	63	30	93
	25 – 29	17	22	39
	30 – 34	0	19	19
	35 – 39	0	8	8
	40 – 44	0	1	1
Education	Elementary	0	27	27
	High school	10	53	63
	Bachelor	67	0	68
	Graduate	3	0	3
Prior Experience with mobile phones	Less than 1 year	0	28	28
	1 – 2 years	0	39	39
	3 – 4 years	30	13	43
	5 – 6 years	25	0	25
	7 – 8 years	15	0	15
	9 – 10 years	10	0	10

We first determined whether the users had characteristics of literate or semi-literate users through a survey. Most importantly, they must be concern about information privacy. Participants who did not fall into the literate and semi-literate groups were removed from the statistical analyses. For example, some farmers had education level and prior experience with mobile technology that were similar to the literate users. Some students indicated that they are not concerned about information privacy and had prior experience with mobile technology that was similar to semi-literate users. These users who were not representative of literate and semi-literate user characteristics were not included in further analyses. The final sample size included 80 literate and 80 semi-literate users. Demographic information of the subjects is presented in Table 1.

3.4. Procedures and tasks

At the start of each session, the participants had to complete a survey. The survey questions included questions about their demographics, concern about information privacy, experience with mobile phones and mobile applications. The participants then performed role-playing tasks on the mobile phone in each experimental condition. The participants were told to take on a farmer's role and provided with the background scenario of the farming context. They registered for an account using their phone number, password, and crop that they grow in the farm. In the pull LBS condition, the participant initiated a request for the latest alert sent by the application to farmers near their current location. Personalized advice on how to manage their crop given the environmental condition was also disseminated. In the push LBS condition, each participant will automatically receive a notification whenever an alert has been sent near their current location. Personalized advice on how to manage their crop given the environmental condition was also disseminated. Thereafter, each user completed a survey about their experience.

3.5. Measurements

Usage intentions were measured by asking whether the individuals were going to use the application in future, for example, "I am going to use this application in future." We also considered whether the user found the application easy to use, for example, "This application is easy to use". We adapted the questions from Angst and Agarwal [1] and Venkatesh et al. [40].

Information privacy concerns were measured by whether a user was worried that the application could track and access their personal information continuously, for example, "I am concerned that the application tracks my location." We also asked whether a user was worried that the application disclosed their personal information to a third party, for example, "I worry over who has access to my usage history when using mobile application." We adapted the questions from Tan and Teo [36], Dinev and Hart [24] and Xu et al [45].

3.6. Experimental Manipulation

Push LBS is operationalized by detecting the user's location and time implicitly and the application delivers a notification of any alert sent based on the location and time. Personalized advice on how to manage their crop given the environmental condition was also disseminated. As for pull LBS, it is operationalized by having the request the application provides notify them of the latest alert sent based on the location and time. Personalized advice on how to manage their crop given the environmental condition was also disseminated.

The manipulations of the literate and semi-literate users were accessed through the pre-experiment survey where they were asked questions regarding their experience with mobile phones and their education level.

3.7. 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 the demographic of our subjects i.e. age, gender, and income [9]. Demographic differences have been found to influence the degree of general privacy concerns.

For example, it was found that those consumers who were less likely to be concerned about privacy were more likely to be male who are young [9]. Hann et al [18] found certain users value convenience over money or Web site privacy policies and certain users were willing to sell their information for money.

4. Data Analyses

4.1. Manipulation Checks

The manipulation of push LBS and pull LBS were accessed following the presentation of each screen. We conducted an independent T-test to test the effectiveness of the manipulations. The results show that all treatments were manipulated effectively. The subjects understood that the methods used to deliver the notification to them were different (F=4.182, t = 1.010, p<0.05).

4.2. Factor Analysis

We conducted principle component factor analysis to assess the reliability and validity of the constructs –

privacy Concerns and usage. The results are presented in Table 2. All items loaded on the constructs they were intended to measure, with non-significant loadings on the other construct. The eigenvalue for privacy concerns is 3.91 and percentage of the variance is 58.15 explained by this factor.

Table 2. Results of Factor Analysis

	Component	
	Privacy Concerns	Usage Intentions
PC1	0.931	0.290
PC2	0.923	0.282
PC3	0.946	0.239
PC4	0.916	0.331
PC5	0.922	0.263
PC6	0.904	0.301
U1	-0.313	0.879
U2	-0.368	0.888
U3	-0.346	0.904
U4	-0.265	0.900
U5	-0.362	0.896
U6	-0.114	0.824

The eigenvalue for usage intentions is 2.34, and percent of the variance is 33.20 explained by this factor. A total of 91.96 percent of the variance can be explained by these two factors (see Table 3). Cronbach's alpha coefficients re also used to assess the internal consistency or reliability of the constructs (see Table 3). Since Cronbach's alpha coefficients for the constructs far exceeded Nunnally's [24] threshold of 0.70, the measurements for privacy concerns and usage intentions were highly reliable.

Table 3. Variance Explained

Factor	Cronbach's Alpha	Eigenvalue	Variance Explained	Cumulative Variance
Privacy concerns	0.986	5.69	47.39%	47.39%
Usage intention	0.968	5.16	42.98%	90.38%

4.3. Hypothesis Testing

We used two-way ANOVA to analyze the hypothesized interaction between personalization and user group, and their impact on privacy concerns and usage. The two-way ANOVA focuses on testing the significance of differences of means in different conditions in a between-subject design, and has been used widely in experimental studies to uncover the main and interaction effects of categorical independent variables (called "factors") on interval dependent variables. Therefore, the two-way measure ANOVA is an appropriate statistical method to examine the main and interaction effects of personalization and user groups on users' privacy concerns and usage of mobile applications.

We used regression to examine the relationships between privacy concerns and usage of mobile application.

4.3.1. Information Privacy Concerns

Data associated with information privacy concerns was analyzed using two-way ANOVA test with two between-subject factors as independent variables: personalization and user group. The mean values and standard deviations are shown in Table 4, while the results of the two-way ANOVA test are presented in Table 5.

Table 4. Means and Standard Deviations for Privacy Concerns

User Group	LBS	Privacy concerns	
		Mean	Standard deviation
Semi-literate	Push	4.67	0.31
	Pull	3.23	0.29
Literate	Push	4.60	0.36
	Pull	3.10	0.38

Table 5. Results for Two-Way ANOVA on Privacy Concerns

	F	P-value	Observed Power
User Group	3.22	0.01	1
LBS	610.76	0.00	1
Group LBS	0.161	0.10	0.068

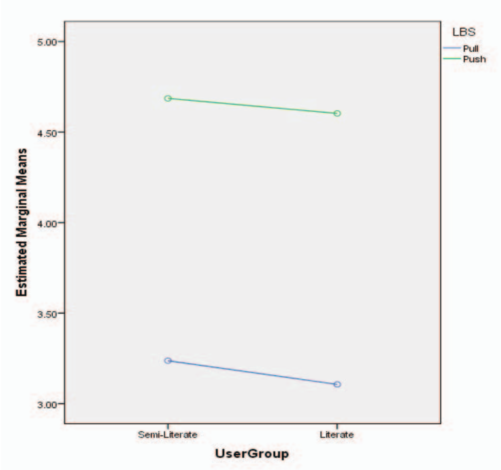

Figure 1. Estimated Marginal Means of Privacy Concerns

Figure 1 shows the interaction effect of LBS and user group on privacy concerns. As presented in Figure 1, push LBS triggers higher privacy concerns in both literate users and semi-literate users. The results in Table 5 suggest that there is no significant interaction effect between LBS and user group on privacy concerns. Hence, H1 is not supported.

4.3.2. Information Privacy Concerns and Usage

We analyzed the relationships between information privacy concerns and usage. As mentioned earlier, this is needed to satisfy the independence assumption. Information privacy concerns negatively influence usage (B=-0.25, p<0.05), as presented in Table 6. Hence, H2 is supported.

Table 6. Results of Regression

Model	Unstandardized coefficients		Standardized coefficients	T	Sig
	B	Std. Error	Beta		
(Constant)	7.16	0.17		42.83	0
Privacy concerns	-0.25	0.04	-0.263	-6.53	0

5. Discussion

5.1. Key Findings

This study conducted a laboratory experiment to examine whether the mechanism to deliver LBS has an impact on information privacy concerns between the two groups of users – literate and semi-literate. Our findings suggest that the channel used to deliver LBS has impact on information privacy concerns for both literate and semi-literate users. The push channel triggers higher information privacy concerns than the pull channel on both groups of user. This is in line with prior research [e.g. 8, 10] that technologies, which allow surveillance to be, carried out triggers a higher concern for information privacy.

The semi-literate users who have a lower education level and lesser experience with LBS mobile applications as compared to the literate users show no significant difference in the degree of information privacy concern from the literate users when using LBS. This is an interesting finding as previous studies [e.g. 32] suggest that education level influence information privacy concerns. Culnan [10] also suggested that it is less privacy invasive when information is collected on an existing relationship. One plausible explanation is that individuals worry no less about information privacy regardless of education level. They are merely coping with the situation. Previous information privacy literatures have not examined information privacy at a group level. In fact, the existing information privacy literatures only carry out their study with the literate users.

5.2. Theoretical Implications

This study focuses on how types of technological attributes affect users' information privacy concerns. We used the PCT to examine the factors that will affect the use of LBS. This study provides empirical evidence on the importance of the literacy level and the technological attributes in assessing individuals' information privacy concern and usage intentions. When studying users' attitudes, beliefs, and perceptions toward new technologies or information systems, it is important for information systems researchers to take into account the purpose of use and who the users are.

From the perspective of theoretical development and advancement, we suggest that mobile application adoption models should take into account of the purpose of use as it moderates users' privacy concerns which negatively influence usage intention.

The task-technology-fit (TTF) model, which was proposed by Goodhue and Thompson [17], suggests that a fit between the features and functions provided by the technology and the tasks to be supported will result in increased use intentions and better performance. Our research examines the interaction effects between the LBS delivery channel and individuals' literacy level on information privacy concerns which negatively influence usage intentions and suggest that usage intentions are higher when personalized content is delivered through the overt channel. Therefore, a fit between these dimensions is very important in mobile application adoption.

This study also integrates the familiarity theory to help us understand why information privacy concerns differ in the two groups of user. We also demonstrate the use of laboratory experiment to study how information privacy concerns affects the use of LBS by the literate and semi-literate users in Asian countries. This follows the call by Bélanger and Crossler [2] to expand the knowledge about information privacy into groups and carry out laboratory experiments with subjects that are outside America.

5.3. Practical Implications

Many are attempting to develop LBS that stand out from the rest to attract usage. Hence, the results of this study can serve as a guide to developers on how LBS should be delivered to reduce privacy concerns which in turn increases usage intentions. Since individuals are more concern about information privacy in the push channel, application providers should offer more incentives for individuals to use push LBS. Application providers should also work on improving privacy protection, such as adopting privacy-enhancing technologies, self-regulations, and legislation to increase users' confidence.

Users and potential users of LBS should also be aware of the techniques used to collect information about them in order to provide LBS. They should resist temptations offered by any untrusted application. Malicious applications may, for example, provide a location-based game to engage the users but exploit the push channel to implicitly monitor the user's location over time. Regulators can also make use of our results to devise better policies to protect the two groups of user. For example, the semi-literate users are less concerned about information privacy, probably because they are not familiar about the risk involved in using LBS. Hence, regulators could introduce an education program to educate the novice users on how to better protect themselves. Since the LBS providers are the ultimate guardian of the users' location information, regulators should also regulate how LBS providers should protect the location information collected.

5.4. Limitations and Future Work

This study is not without limitations. First, the study is done in a laboratory setting. The actual usage behavior cannot be monitored. Future studies may deploy the application into the field and monitor the actual usage. Second, the mobile applications we developed for our experiment was in the agriculture context. Future studies may repeat this study by using applications in another context. Third, the participants are from Asian countries that have a different set of cultures compared to the western countries. Hence, the results may not be generalizable to western countries. Future studies may repeat the study in western countries.

6. Conclusion

The advancement in technology may value-add to users but also subjecting them to new vulnerabilities. It is important for researchers, designers, and policymakers to understand how individuals strike a balance between value and risk. This study has provided empirical evidence for this dilemma. This current study contributed to existing information privacy research by expanding the knowledge into group level by using the lens of familiarity and different technological attributes. Our findings suggest that the LBS delivery mechanisms impact information privacy concerns. The semi-literate users showed no less concern for information privacy than the literate users. 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 help the literate and semi-literate users use LBS mobile application.

7. References

[1] Angst, C. M., and R Agarwal., "Adoption of electronic health records in the presence of privacy concerns The elaboration likelihood model and individual persuasion", MIS Quarterly 33(2), 2009, pp. 339-370.

[2] Bélanger, F, and R. E. Crossler., "Privacy in the digital age: a review of information privacy research in information systems", MIS Quarterly 35(4), 2011, pp. 1017-1042.

[3] Bruner, G. C., and A. Kumark, "Attitude toward location-based advertising", Journal of Interactive Advertising, 7(2), 2007, pp. 3-15.

[4] Campbell, A. J., "Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy", Journal of Interactive Marketing 11(3), 1997, pp. 44-57.

[5] Carver, C. S., and Scheier, M. F., "Control theory: A useful conceptual framework for personality–social, clinical, and health psychology," Psychological bulletin, 92(1), 1982, pp. 111.

[6] Chellappa, R. K., and R G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma", Information Technology and Management, 6(2-3), 2005, pp. 181-202.

[7] Chipchase, J., "Understanding non-literacy as a barrier to mobile phone communication", Retrieved September 16 2008 at http://research.nokia.com/bluesky/non-literacy-001-2005/index.html, 2005.

[8] Cranor, L. F., "I Didn't Buy it for Myself", Designing personalized user experiences in eCommerce, pp. 57-73.

[9] Culnan, M. J., "Consumer awareness of name removal procedures: implications for direct marketing," Journal of Direct Marketing 9 (2), 1995, pp. 10-19.

[10] 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. 341-363.

[11] Culnan, M. J., and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", Organization Science, 10(1), 1999, pp. 104-115.

[12] Culnan, M. J., and R. J. Bies, "Consumer privacy: Balancing economic and justice considerations", Journal of social issues, 59(2), 2003, pp. 323-342.

[13] Dinev, T, and P. Hart., "Internet privacy concerns and their antecedents-measurement validity and a regression model", Behaviour & Information Technology, 23(6), 2004, pp. 413-422.

[14] Dinev, T, P. Hart, and M. R. Mullen, "Internet privacy concerns and beliefs about government surveillance–An empirical investigation", The Journal of Strategic Information Systems, 17(3), 2008, pp. 214-233.

[15] Duri S., A. Cole, J. M, and J. Christensen, "An approach to providing a seamless end-user experience for location-aware applications", Proceedings of the 1st International Workshop on Mobile Commerce, ACM, 2001, pp. 20-25.

[16] Gefen, D., Karahanna, E., and Straub, D. W., “Trust and TAM in online shopping: an integrated model,” MIS quarterly, 2003, pp. 51-90.

[17] Goodhue, D. L., and Thompson, R. L., “Task-technology fit and individual performance,” MIS Quarterly, 19(2), 1995, pp. 213-236.

[18] Hann, Il-H., K-L. Hui, S-Y. T.Lee, and I. P.L. Png, "Overcoming online information privacy concerns: An information-processing theory approach", Journal of Management Information Systems, 24(2), 2007, pp. 13-42.

[19] Houston, F. S., and J. B. Gassenheimer., "Marketing and exchange", The Journal of Marketing, 1987, pp. 3-18.

[20] Johnston, A. C., and M. Warkentin, "Fear appeals and information security behaviors: an empirical study", MIS Quarterly 34(3), 2010.

[21] Komiak, S. Y., and Benbasat, I.,”The effects of personalization and familiarity on trust and adoption of recommendation agents,” MIS Quarterly, 2006, pp. 941-960.

[22] Luhmann, N., “Familiarity, confidence, trust: Problems and alternatives,” Trust: Making and breaking cooperative relations, 6, 2000, pp. 94-107.

[23] Masizana-Katongo, AN. & Morakanyane, R., “Representing Information for Semi-Literate Users: Digital Inclusion Using Mobile Phone Technology,” Gaborone: Department of Computer Science, University of Botswana, n.d.

[24] Medhi, I, S. Patnaik, E. Brunskill, S. N. Gautama, W. Thies, and K. Toyama, "Designing mobile interfaces for novice and low-literacy users", ACM Transactions on Computer-Human Interaction (TOCHI), 18(1), 2011.

[25] Nunnally, J., Psychometric theory, McGraw-Hill, New York, 1978.

[26] Powers, W. T., “Behavior: The control of perception,” New York, NY: Hawthorne, 1973.

[27] Prahalad, C. K., and S. L. Hart, "The Fortune at the Bottom of the Pyramid", Strategy and Business, 2002, pp. 54-54.

[28] Phelps, J, G. Nowak, and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information", Journal of Public Policy & Marketing, 2000, pp. 27-41.

[29] Rao, B, and L. Minakakis, "Evolution of mobile location-based services", Communications of the ACM, 46(12), 2003, pp. 61-65.

[30] Roberts, P,. “Defining literacy: Paradise, nightmare or red herring?,” British Journal of Educational Studies, 43(4), 1995, pp. 412-432.

[31] Schiaffino, S, and A. Amandi, "User–interface agent interaction: personalization issues", International Journal of Human-Computer Studies, 60(1), 2004, pp. 129-148.

[32] Sheehan, K. B., “Toward a typology of Internet users and online privacy concerns”, The Information Society, 18(1), 2002, pp. 21-32.

[33] Smith, H. J, S. J. Milberg, and Sandra J. Burke, "Information privacy: measuring individuals' concerns about organizational practices", MIS Quarterly, 1996, pp. 167-196.

[34] Stone, E. F., H. G. Gueutal, D. G. Gardner, and S. McClure, "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations", Journal of Applied Psychology, 68(3), 1983, pp. 459-468.

[35] 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.

[36] Tan, M, and T. S.H. Teo, "Factors influencing the adoption of Internet banking", Journal of the AIS, 2000.

[37] Thatcher, A., Shaik, F., & Zimmerman, C., “Attitudes of semi-literate and literate bank account holders to the use of automatic teller machines (ATMs),” International Journal of Industrial Ergonomics 35(2), 2005, pp. 115-130.

[38] Thomas, D, J. Strauss, and Maria-Helena H., "How does mother's education affect child height?", Journal of human resources, 1991, pp. 183-211.

[39] Unni, R, and R. Harmon, "Perceived effectiveness of push vs. pull mobile location-based advertising", Journal of Interactive advertising, 7(2), 2007, pp. 28-40.

[40] Venkatesh, V, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view", MIS Quarterly, 2003, pp. 425-478.

[41] Westin, A. F., "Privacy and freedom", Washington and Lee Law Review, 25(1), 1967.

[42] Wiese, J, P. G. Kelley, L. F. Cranor, L. Dabbish, J. I. Hong, and J Zimmerman, "Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share", Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp), 2011.

[43] Xu, H, "The effects of self-construal and perceived control on privacy concerns", Proceedings of the 28th Annual International Conference on Information Systems (ICIS 2007), 2007.

[44] Xu, H., Teo, H. H., Tan, B. C., and Agarwal, R., "Research Note—Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services," Information Systems Research, 23(4), 2012, pp. 1342-1363.

[45] Xu H, HH Teo, BCY Tan, and R. Agarwal, "The role of push-pull technology in privacy calculus: the case of location-based services", Journal of Management Information Systems, 26(3), 2009, pp.135-174.

[46] Xu, H, X. R. Luo, J. M. Carroll, and M. B. Rosson, "The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing", Decision Support Systems, 51(1), 2011, pp. 42-52.

Acknowledgement

This research is supported by the Singapore National Research Foundation under its International Research Centre @ Singapore Funding Initiative and administered by the IDM Programme Office. I would like to thank Prof. Bernard C. Y. Tan, Prof Roger Zimmerman and Prof Ravi Poovaiah for their timely advice and guidance. I would also like to thank the team members and research assistants, including Avijit Sengupta, Jia Rubio, Michelle Gwee, Yimeng Deng and Yi Wu.