Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2014 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2014

INFORMATION PRIVACY CONCERNS AMONG NOVICE AND EXPERT USERS OF SOLOMO

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

Maffee Peng-Hui Wan
National University of Singapore, diswp@nus.edu.sg

Recommended Citation

Chua, Wen Yong; Chang, Klarissa T T.; and Wan, Maffee Peng-Hui, "INFORMATION PRIVACY CONCERNS AMONG NOVICE AND EXPERT USERS OF SOLOMO" (2014). *PACIS 2014 Proceedings*. 138.
http://aisel.aisnet.org/pacis2014/138

INFORMATION PRIVACY CONCERNS AMONG NOVICE AND EXPERT USERS OF SOLOMO

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

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

Maffee Peng-Hui Wan, National University of Singapore, Singapore, diswp@nus.edu.sg

Abstract

SoLoMo (Social-Local-Mobile) services are becoming dominant to the huge population of semi-literate users living in emerging economies due to low costs and ubiquity. However, usage of SoLoMo services is still susceptible by information privacy concerns. Studies typically addressed the ways to mitigate information privacy concerns for the literate users and not the semi-literate users. To fill the gap of semi-literate users and have a better understanding of the information privacy concerns among different communities, this study draws upon theories of privacy calculus, familiarity, intrinsic and extrinsic motivation and protection motivation to identify the precursors of information privacy concerns related to SoLoMo services and users' expertise. The proposed research model is empirically tested in a laboratory experiment. The findings show that the two channels (covert and overt) of delivering SoLoMo services affect the degree of information privacy concerns between the literate and semi-literate users. Implications for improving usage intentions and mitigating information privacy concerns for SoLoMo services for different types of mobile applications are discussed.

Keywords: SoLoMo, Information Privacy Concerns, Usage Intentions, Covert and Overt Channels.

1 INTRODUCTION

The proliferations of GPS (Global Positioning System) enabled mobile devices have created opportunities for social media developers to leverage on location data to introduce location-sensitive features. Marcelo from Business Insider has termed this concept as SoLoMo where developers have deviated from the “check in” concept (Marcelo 2013). Usage of SoLoMo services is frequently jeopardized by individuals’ information privacy concerns (Wiese et. al. 2011). In the context of SoLoMo services, individuals are anxious about the breach of their location information (Xu et. al. 2009). Such anxieties often give rise to concerns about information privacy, which refers to “the ability of the individual to personally control information about one’s self” (Stone et. al. 1983). Information privacy concern is known as the ability to restrict how personal information is obtained and used (Westin 1967). While SoLoMo services leverages on the spatial and temporal information of users to customize mobile experience, individuals may view this as an invasion of privacy (Culnan 1999). Therefore, we need to understand the precursors of information privacy concerns so as to propose ways that can be migrated to improve usage intentions.

SoLoMo services delivers information through two channels, covert and overt. In the covert channel, personalized information is being delivered by monitoring the individuals’ activities at different locations over time implicitly (Xu et. al. 2011). This approach may raise stronger information privacy concerns (Carnor 2004). One plausible explanation is that the individual does not feel to be in control over the disclosure of their personal information (Culnan and Armstrong 1999; Phelps et. al. 2000; Culnan and Bies 2003; Xu 2007). On the other hand, the overt channel delivers personalized content where and when the user explicitly initiates the request (Xu et. al. 2011). One problem with this approach is that the user may enter false or wrong information (Lavie et. al. 2010). To protect information privacy, individuals have to feel to be in control of their information (Xu 2007). Therefore, it is important to examine the factors that affect individuals’ information privacy concerns. Furthermore, not all users are willing to provide explicit information about their preferences, and their willingness to do so depends on the type of applications (Schiaffino and Amandi 2004).

The personalization-privacy paradox suggests that the effects of personalized information delivered by SoLoMo services on information privacy concerns can be influenced by the type of mobile applications (Figge 2004). Previous research (e.g. Van der Heijden 2004; Sun and Zhang 2006a) has acknowledged that task performed on mobile applications can be classified into two types - utilitarian and hedonic, which provide different values to the users. The task on utilitarian application provides extrinsic value (e.g., an app to perform a task) but a task on hedonic application provides intrinsic value (e.g. an app to that provides fun and joy) (Xu et al. 2012).

Existing literatures on the personalization-privacy paradox typically addresses the needs of the users who are familiar with mobile applications. However, the widespread usage of mobile devices among billons of subscribers living in the rural areas of emerging economies (Medhi et al. 2011) means that half of the populations are novice users who use only simple functions on their mobile phones for synchronous voice communications (Chipchase 2005). Shneiderman (1992) indicated that novice and expert users are common classes of users along the user experience scale. Novice users are defined as “users who know the task but have little or no knowledge of the system”. Expert users are “users who have deep knowledge of tasks and related goals and the actions required to accomplish the goals” (Shneiderman 1992). There is a lack of studies in existing literatures that explain how mobile personalization should be delivered to users with different expertise levels so as to minimize privacy concerns and increase the use of personalized content in mobile applications.

Motivated by the unique characteristics of novice and expert users, as well as the types of applications that affect information privacy concerns and usage intentions, our study aims to answer the following questions:

1. What are the impacts of SoLoMo service delivery channels on information privacy concerns?

2. How is the relationship between SoLoMo service delivery channels and information privacy concerns contingent on the types of users (novice vs experts) and the types of tasks performed on applications (utilitarian vs hedonic)?
3. 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 SoLoMo service delivery channels and information privacy concern is contingent on novice / expert users. Second, we provide insights on how the technological attributes impacts the information privacy concerns of novice / expert 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 mobile application context. First, as individuals trade-off their privacy for the benefit, we let system designers know which approach to use for delivering SoLoMo services to novice / expert users. Second, we alert users to the methods used to collect information about them so they may take precautions when using mobile applications. Third, this study helps policy makers to devise policies to better protect different group of users based on their unique characteristic and concern for information privacy.

2 THEORY AND HYPOTHESES DEVELOPMENT

2.1 SoLoMo Service Delivery Channels

Culnan and Bies (2003) introduced the privacy calculus framework based on exchange theory (Houston and Gassenheimer 1987). Privacy calculus is commonly found in empirical research of information privacy literatures (e.g. Culnan 1993; Culnan and Armstrong 1999; Xu et al. 2009; Xu et al. 2011). Privacy calculus suggests that a person acts on a calculus of behavior (e.g. privacy calculus) where personal information disclosure will happen only when the value gained from disclosure outweighs the cost of disclosure (Dinev et al. 2008). That is, the person will perform a risk-benefit analysis under the privacy calculus and decide whether or not to disclose personal information (Xu et al. 2009).

Applying the privacy calculus framework to the context of the delivery channels used by SoLoMo services, an individual has to decide if he/she should or should not disclose his/her location information to the service provider. The decision lies in whether the personalized content is of higher value to the user versus the amount of risk exposure from privacy invasion of revealing one's location information. If the user considers the value of the personalized content to be of higher value than the cost of disclosure, the user will take the risk of information privacy breach and proceed to disclose his/her personal information (Chellappa and Sin 2005). Previous research (e.g. Culnan 1993) suggested that the covert channel subject individuals to higher information privacy risk than the overt channel as the covert channel allows applications to implicitly monitor the user. Hence, we hypothesize:

- H1: Compared to overt personalization, covert personalization will be associated with a greater level of information privacy concerns.

2.2 Expertise Level

Novice and expert users differ on two dimensions. Goal is one dimension that differentiates a novice user from an expert user (Moran 1981). The goal of a novice user is to be wealthy so that the basic needs like food can be fulfilled (Diener and Biswas-Diener 2002). The expert users, on the other hand, are more concerned about receiving respect, love, and self-actualization (Diener and Biswas-Diener 2002). The individuals' goal affects an individuals' privacy concern. Hann et al (2007) found out that certain users value convenience over money or Web site privacy policies and certain users were willing to sell their information for money.

Another dimension that differentiates between novice and expert is prior experience (Moran 1981). A novice user has lesser experience with mobile application as compared to an expert user (Medhi et al. 2011). Individuals who are more experienced have a lower degree of information privacy concerns (Phelps et al. 2000). Phelps et al (2000) reported that consumers who had purchased products from a catalogue within the past six months showed less concern about information privacy than those who had not. Table 1 summarizes the dimensions of the expert and novice users.

Dimension	Expert User	Novice User
Goals	The expert users are more concerned about receiving respect, love, and self-actualization (Diener and Biswas-Diener 2002).	The goal of a novice user is to be wealthy so that the basic needs like food can be fulfilled (Diener and Biswas-Diener 2002)
Prior Experience	Has greater prior experience	Has lesser prior experience

Table 1. Distinctions between Expert and Novice Users

The familiarity perspective is a useful theoretical lens for understanding the moderating effects of users' expertise on the relationships between the SoLoMo service delivery channels and information privacy concerns. Familiarity is the individuals' understanding of another, often based on previous interactions, experience, and learning of "the what, who, how, and when of what is happening" (Gefen et al. 2003). Hence, individuals' familiarity of the delivery channels used by SoLoMo services comes with the direct experience of receiving personalized content from the provider (Komiak and Benbasat 2006). Familiarity reduces the uncertainty of expectation through increased understanding of what has happened in the past (Luhmann 2000). An individual's privacy concern is influenced by past privacy experiences (Stone and Stone 1990; Xu et al. 2009; Xu et al. 2011; Xu et al. 2012).

Using the lens of familiarity, an expert user is one who has more experience in consuming personalized content through mobile applications than novice users. If an expert 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 (Smith et al. 1996; Xu et al. 2009). On the other hand, if the expert user has not been victimized by privacy breaches through mobile application, the user will have a weaker concern about information privacy than novice users. Culnan (1993) suggests individuals are less likely to consider it as privacy-invasive when information is collected on an existing relationship.

The expert users are more familiar with delivery channels used by SoLoMo services, privacy, and privacy breaches than the novice users. As the expert users are more aware about privacy and privacy breaches, they are likely to be more concern about privacy. This is because the expert users know that they are taking a risk of privacy invasion when consuming personalized information from SoLoMo services as they are releasing their personal location information. Hence, to receive respect, love, and self-actualization, these expert users will not take the risk of privacy invasion. The novice users, on the other hand, are more concern about being able to achieve their basic needs though the value that the application can provide. Therefore they are willing to release their personal information in exchange for wealth to achieve their basic needs. Hence, we hypothesize:

- H2: Compared to expert users, novice users will be associated with a greater level of information privacy concerns.

2.3 Task Performed in Different Types of Application

Research has suggested that consumer value is driven by intrinsic and extrinsic motivators (Holbrook 1999). Individuals are intrinsically motivated to perform task on hedonic applications, as the pleasure derived from using the application is the ultimate goal (Van der Heijden 2004; Xu et al. 2012). One intrinsic motivator is pleasure (Tam et al. 2002). Pleasure refers to the state of enjoyment that can be derived from products or services (Mehrabian and Russell 1974). In exchange for personal information, application providers can offer features that bring pleasure to an individual.

Individuals are extrinsically motivated to use utilitarian application as they derive instrumental value from using the application (Van der Heijden 2004; Xu et al. 2012). Time saving is one extrinsic motivator (Tam et al. 2002). Time savings can come in the form of less time, less effort, or better convenience when purchasing products or services (Bhatnagar et al. 2000; Chandon et al. 2000). Application providers can offer features that help user save time to exchange for personal information. Money saving is another extrinsic motivator (Tam et al. 2002). For example, consumers have been found to offer personal information to mailing lists in exchange for compensation (e.g., coupons, rebates, and special offers) (Milne and Gorden 1993).

The two types of application offer different values to the user. The degree of information privacy concern when using SoLoMo services in the application relies on how much the user values the benefit receives from using the application.

A utilitarian application is used to perform a task and provide the users with extrinsic value, whereas the purpose of performing a task on hedonic application is to have fun and provide the users with intrinsic value (Van der Heijden 2004; Xu et al. 2012). The extrinsic value an individual receives often results in practical benefits as compared to the intrinsic value. This will cause individuals to be more willing to trade off their privacy for the potential extrinsic benefits. Hence, we hypothesize:

- H3: Compared to utilitarian application, performing task on hedonic application will be associated with a greater level of information privacy concerns.

2.4 Usage Intention

Rogers (1975) introduced the protection motivation theory (PMT) to explain how individuals behave when faced with a potential threat. PMT has been widely used in information security literatures to explain and predict individuals' protective behaviors (e.g. Johnston and Warkentin 2010; Pahnila and Mahmood 2007). PMT suggest that individuals evaluate a threat based on the factors: (1) perceived severity of the threat, (2) perceived vulnerability to the threat, and (3) perceived likelihood of occurrence. The higher the factors are to an individual, the more an individual is motivated to take protective measures (Johnston and Warkentin 2010).

Previous research has agreed that individuals are unwilling to use new mobile applications when the individual is highly concern about information privacy (Xu et al. 2012). We apply the PMT to explain how individuals' information privacy concerns affect the consumption of personalized content. Individuals are taking a risk of possible privacy-invasion when they disclose personal information (Xu et al. 2009). In this situation, individuals can, for example, read the privacy policy to identify whether the content provider has taken protective measures of individuals' personal information before deciding if they should release their personal information. On the other hand, individuals can completely avoid consuming the personalized content. Individuals will adopt the method that they have the self-efficacy to perform the tasks (Rogers 1975). That is, an individual will only perform a task that the individual thinks he has the ability to do it. An individual will read the privacy policy only if the individual feel that he can read to determine which content provider is taking precautionary measures.

The PMT posits that an individual will avoid a situation where the individual feels that the threat is likely to happen. An individual will not adopt personalized content if the individual view the situation as a threat that the individual cannot control. On the other hand, an individual will adopt personalized content if the individual does not view the situation as a threat that the individual cannot control. Hence, we hypothesize:

- H4: Information privacy concerns will be negatively associated with intention to use.

3 METHODOLOGY

3.1 Research Design

We conducted a laboratory experiment with 160 participants to test our hypotheses. We have a 2 (covert / overt) by 2 (expert / novice users) by 2 (hedonic / utilitarian tasks) factorial design where we presented a mobile agricultural application, mPest, running on the Android platform to each group of user.

3.2 Prototypes of Mobile Application

We developed a mobile agricultural application, mPest, on the Android platform as it is open source. mPest has three components. First, the mobile client will take in input from the participants and send it back to the server. Then, the web application residing at the server process the request and stores the data in the database. We want the participants to experience a working application with network connectivity to create an environment that is similar to the actual usage.

3.3 Participants

A total of 200 novice and 200 expert users participated in our study. The novice users were farmers that belong to the Middle of the Pyramid in their home country and earn less than $20 per day. They own feature phones. The expert users were undergraduate students in a large university. We first determined whether the users had characteristics of novice or expert users through a simple survey. Participants who did not fall into the novice and expert groups were removed from the statistical analyses. For example, some farmers had goals and prior experience with mobile phones that were similar to expert users. Some students had goals and prior experience with mobile phone that were similar to novice users. These users who were not representative of novice and expert user characteristics were not included in further analyses. The final sample size included 80 novice and 80 expert users. Demographic information of the subjects is presented in Table 2.

Gender		Expert	Novice	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	26	26
	High school	10	53	63
	Bachelor	67	1	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
Goals	Wealth	6	77	83
	Self-Actualization	74	3	77

Table 2. Demographic Information of Subjects

Previous studies have shown that younger people are more pragmatic where they are willing to sacrifice privacy for benefits. People over the age of 45 tend to be either not at all concerned about privacy or highly concerned about privacy (Sheehan 2002). In our research, we are interested in studying the moderating effect of the delivery channels used by SoLoMo services on users' information privacy concerns. Hence, our subjects who are below the age of 45 are appropriate subjects for the study.

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, goals in their life, 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 and password. In the utilitarian task with delivery of information through the overt channel, the participant sought advice on removing a pest that they have found in their farm. They took a photo of the crop's condition and input a text message regarding the condition using the phone. Each participant had to provide his location and time explicitly by keying the information into the phone. The personalized advice took into account the environmental conditions such as weather using the location information provided by the participants. In the utilitarian task with delivery of information through the covert channel, each participant's location and time was automatically detected using the phone GPS.

In the hedonic task, the participants were told that they were out on a relaxed shopping trip. They saw a product they liked and they wanted to find out more about the product. They had to take a photo of the product and key into the phone about information related to what the product. In the hedonic task with delivery of information through the covert channel, the participants' location and time were automatically detected using the phone GPS. In the hedonic task with delivery of information through the overt channel, the participants were asked to explicitly provide their location and time. 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 2009; Venkatesh et al. 2003.

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 (2000); Dinev and Hart (2004); Xu et al (2009).

3.6 Experimental Manipulation

The utilitarian application and hedonic application were designed to provide personalized advice to the user. The personalized advice took into account the usage history, location and time. The utilitarian application is operationalized by using an agricultural application. This application allows the users to seek for pest advice when they saw a pest at their farm. As for the hedonic application, it is operationalized by using a commerce application. This application allows the user to find out more about the product when they are out shopping.

Delivery of information through the covert channel is operationalized by detecting the user's location and time and the application provides personalized advice based on the location and time while delivery of information through the overt channel is operationalized by having the user type in their location and time and the application provides personalized advice based on the location and time.

The manipulations of the novice and experts users were accessed through the pre-experiment survey where they were asked questions regarding their experience with mobile phones and their goals in life.

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 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 (Culnan 1995). 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 personalization. Therefore, we treat this factor as a control variable for usage intention of personalized application.
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 (Smith et al. 1996). Previous privacy experience may therefore influence concerns about privacy invasions (Stone and Stone 1990) and is included as a control variable for information privacy concerns.

4 DATA ANALYSES

4.1 Manipulation Checks

The manipulations of information delivery through the covert and overt channels were accessed through 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 acquire their location and time were different (F=4.182, t = 1.010, p<0.05). They also understood the difference between hedonic and utilitarian task (F=16.031, t= -1.921, 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 3. 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.

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 4). Cronbach's alpha coefficients are also used to assess the internal consistency or reliability of the constructs (see Table 4). Since Cronbach's alpha coefficients for the constructs far exceeded Nunnally's (1978) threshold of 0.70, the measurements for privacy concerns and usage intentions were highly reliable.

	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

Table 3. Results of Factor Analysis

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

Table 4. Variance Explained

4.3 Hypothesis Testing

We used two-way ANOVA to analyze the hypothesized interaction between delivery of information through the covert/overt channels 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 information delivery channels 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: delivery of information through the covert/overt channels and user group. The mean values and standard deviations are shown in Table 5, while the results of the two-way ANOVA test are presented in Table 4. The results in Table 6 suggest that there is a significant interaction effect between delivery of information though the covert/overt channels and user group on privacy concerns (F=11.77, p<0.05). We also used two-way ANOVA test with two between-subject factors as independent variables: hedonic task / utilitarian task and user group. The mean values and standard deviations are shown in Table 7, while the results of the repeated measure ANOVA test is presented in Table 8. The results in Table 8 suggest that there is significant interaction effect between task type and user group on privacy concerns (F=10.91, p<0.05).

Personalization	User Group	Privacy concerns	
		Mean	Standard deviation
Covert	Novice	4.60	1.46
	Expert	5.80	1.24
Overt	Novice	2.23	1.51
	Expert	4.83	0.84

Table 5. Means and Standard Deviations for Privacy Concerns

	F	P-value	Observed Power
Personalization	66.37	0	1
User Group	86.69	0	1
Group Personalization	11.77	0.01	0.926

Table 6. Results for Two-Way ANOVA on Privacy Concerns

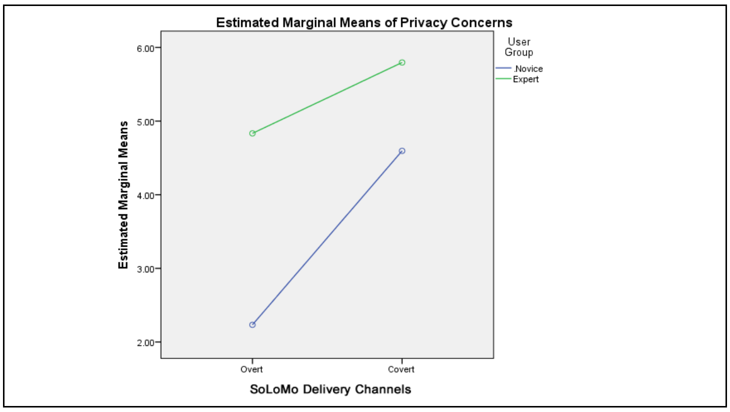

Figure 2. Estimated Marginal Means of Privacy Concerns

Figure 2 shows the interaction effect of information delivery through the covert/overt channels and user group on privacy concerns. As presented in Figure 2, delivery of information through the covert channel triggers higher privacy concerns in both novice users and expert users. Hence, H1 is supported. Figure 2 also shows that the expert users have a greater privacy concerns than the novice users. Hence, H2 is supported.

		Privacy concerns	
Task type	User Group	Mean	Standard deviation
Hedonic	Novice	3.58	1.66
	Expert	6.23	0.83
Utilitarian	Novice	3.26	2.11
	Expert	4.40	0.57

Table 7. Means and Standard Deviations for Privacy Concerns

	F	P-value	Observed Power
Task type	22.25	0	0.997
User Group	70.04	0	1
Group Task	10.91	0.001	0.907

Table 8. Results for two-way ANOVA on Privacy Concerns

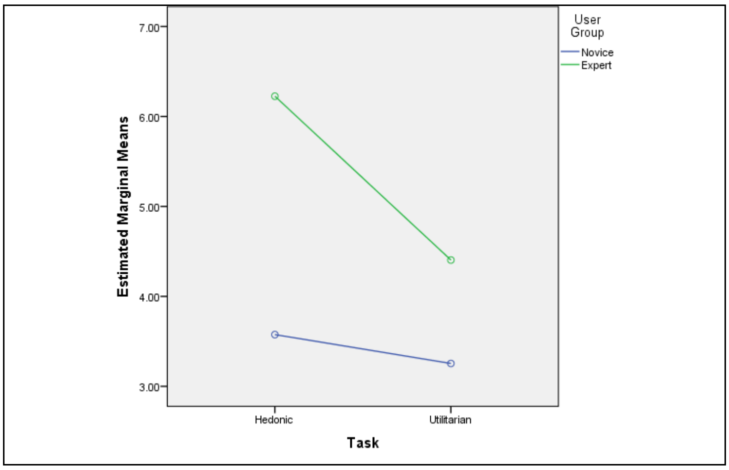

Figure 3. Estimated Marginal Means of Privacy Concerns

Figure 3 shows that there is significance interaction that the type of task has on privacy concerns. Performing task on the hedonic application triggers a higher concern for privacy than performing task on the utilitarian application among the expert and the novice users. Hence, H3 is supported.

4.3.2 Privacy Concerns and Usage

We analyzed the relationships between privacy concerns and usage. As mentioned earlier, this is needed to satisfy the independence assumption. Privacy concerns negatively influence usage (B=-0.25, p<0.05), as presented in Table 9. Hence, H4 is supported.

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

Table 9. Results of Regression

5 DISCUSSION

5.1 Key Findings

This study examines the trade-off and suggests privacy concern may be mitigated by delivering personalized content through the channel that triggers lesser privacy concerns. We also suggested that privacy concerns vary with the types of application. We conducted an experiment with the expert and novice users to examine our hypothesis.

Consistent with prior research (e.g. Phelps et al. 2000; Chellapa and Sin 2005), our study also shows that usage intention is influenced by the trade-off between privacy and the expected value derived. As the value provided by a utilitarian application task differs from a hedonic application task, the amount of privacy concerns triggered differs. This is also in line with prior research (e.g. Belk 1974; Belk 1975; Grewal et al. 1996) that privacy concern and usage intention are situation dependent.

Our study also shows that the channel used to deliver personalized information has impact on privacy concerns for both novice and expert users. The covert channel triggers higher privacy concerns than the overt channel on both groups of user. This is also consistent with prior research (e.g. Culnan 1993; Carnor 2004) that technologies which allow surveillance to be carried out triggers a higher concern for information privacy.

The novice users who have a different set of goals in life and lesser experience with mobile application as compared to the expert users shows a lower privacy concerns than the expert users. This is an interesting finding as previous information privacy literatures have not examined information privacy at a group level.

Our study made a number of additional interesting findings. First, we discovered that the difference between the information privacy concerns triggered by delivery of information through covert and overt channels differs much in the novice group but not the expert group. One plausible explanation may be the novice users are less worried when they can perform voluntary disclosure. The expert users are probably aware that means of data collection does not reduce their risk of being subjected to information privacy breaches. That is, the application provider controls their personal information so long they disclose their personal information to the application provider.

Another finding we discovered is the expert users are more worried in performing tasks on the hedonic application than the novice users are. However, the difference in information privacy concerns between the novice and the expert users is smaller in utilitarian application. One plausible explanation that we have is seeking advice related to work may be viewed as a group. That is, a group of farmers are facing the pest problem so they seek help. However, the hedonic task may be viewed as a more personal one by the expert users so this trigged higher information privacy concerns.

5.2 Theoretical Implications

This study focuses on delivery of personalized information which is one of the key advantages of mobile applications. It also examines the personalization-privacy paradox to enhance our understanding of factors influencing usage intentions.

This study provides empirical evidence on the importance of the preferred delivery channel and the technological attributes in assessing users’ 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.

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.

Prior research on technology innovation has pointed out the importance of fit between information technologies and the tasks to be supported, as a precursor to technology use and its subsequent benefits (Dennis et al. 2001; Goodhue and Thompson 1995). The task-technology-fit (TTF) model, which was proposed by Goodhue and Thompson (1995), suggests that a fit between the features and functions provided by the technology and the tasks to be supported will result in an increase in its usage intentions and better performance. Our research examines the interaction effects between the preferred channel and the types of application 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 demonstrates the use of laboratory experiment to study how information privacy concerns affects the use of personalized mobile applications by the novice and expert users in the Asian countries. This follows the call by Bélanger and Crossler (2011) 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 developers are attempting to develop mobile applications that stand out from the rest to attract usage. Hence, the results of this study can serve as a guide to developers on the ways in which personalized content should be delivered to users so as to reduce users' privacy concerns which in turn increases usage intentions. Application providers should also work on improving privacy protection, such as adopting privacy-enhancing technologies, self-regulations, and legislation to increase users' confidence (Xu and Teo 2004).

Users of mobile applications should also be aware of the techniques that can be used to collect information about them and resist temptations provided by any application. Malicious applications may, for example, provide a location-based game to engage the users but exploit the covert channel to implicitly monitor the user. Regulators can also make use of our results to devise better policies to protect the users. For example, the novice users are less concerned about information privacy, probably because they are not familiar about the potential of privacy breaches. Hence, regulators could introduce an education program to educate the novice users on how to better protect themselves.

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 and commerce 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. Forth, the expert users were undergraduates who are told to take on a farmers' role who may not have the experience of a farmer. Future studies maybe conducted with participants with farming experience.

6 CONCLUSION

The proliferation of mobile applications provides new values to users while simultaneously creating 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 personalization-privacy paradox and different technological attributes. Our findings suggest that the channel used to deliver personalized information and the types of application have an impact on information privacy. The novice users show a lower concern for information privacy than the expert users are. 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 novice and expert users use mobile application.

ACKNOWLEDGEMENTS

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its International Research Centres in Singapore Funding Initiative and administered by the Interactive Digital Media Programme Office.

References

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

Bélanger, F., & Crossler, R. E. 2011. “Privacy in the digital age: a review of information privacy research in information systems,” MIS Quarterly (35:4), pp. 1017-1042.

Belk, R. W. 1974. “An exploratory assessment of situational effects in buyer behavior,” Journal of Marketing Research, pp. 156-163.

Belk, R. W. 1975. “Situational variables and consumer behavior,” Journal of Consumer research, pp. 157-164.

Bhatnagar, A., Misra, S., & Rao, H. R. 2000. “On risk, convenience, and Internet shopping behavior,” Communications of the ACM, (43:11), pp. 98-105.

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

Chandon, P., Wansink, B., & Laurent, G. 2000. “A benefit congruency framework of sales promotion effectiveness,” The Journal of marketing, pp. 65-81.

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

Chipchase, J. 2005. “Understanding non-literacy as a barrier to mobile phone communication,” Retrieved September, 16, 2008.

Culnan, M. J. 1993. “How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information us,” MIS Quarterly (17:3), pp. 341-363.

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

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

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

Dennis, A. R., Wixom, B. H., & Vandenberg, R. J. 2001. “Understanding fit and appropriation effects in group support systems via meta-analysis,” MIS Quarterly, pp. 167-193.

Diener, E., & Biswas-Diener, R. 2002. “Will money increase subjective well-being?,” Social indicators research (57:2), pp. 119-169.

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

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

Figge, S. 2004. “Situation-dependent services—a challenge for mobile network operators,” Journal of Business Research (57:12), pp. 1416-1422.

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

Grewal, D., Marmorstein, H., & Sharma, A. 1996. “Communicating price information through semantic cues: the moderating effects of situation and discount size,” Journal of Consumer Research, pp. 148-155.

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

Holbrook, M. B. 1999. “Consumer value: a framework for analysis and research,” Psychology Press.

Houston, F. S., & Gassenheimer, J. B. 1987. “Marketing and exchange,” The Journal of Marketing, pp. 3-18.

Johnston, A. C., & Warkentin, M. 2010. “Fear appeals and information security behaviors: an empirical study,” MIS quarterly, (34:3), pp. 549.

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

Lavie, T., Sela, M., Oppenheim, I., Inbar, O., & Meyer, J. 2010. “User attitudes towards news content personalization,” International journal of human-computer studies (68:8), pp. 483-495.

Luarn, P., & Lin, H. H. 2005. “Toward an understanding of the behavioral intention to use mobile banking,” Computers in Human Behavior (21:6), pp. 873-891.

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

Marcelo, B. (2013, 09 26). Beyond Check Ins: How Social Media Apps Are Driving A Boom In Location-Based Data. Business Insider.

Medhi, I., Patnaik, S., Brunskill, E., Gautama, S. N., Thies, W., & Toyama, K. 2011. “Designing mobile interfaces for novice and low-literacy users,” ACM Transactions on Computer-Human Interaction (18:1), 2.

Mehrabian, A., & Russell, J. A. 1974. “An approach to environmental psychology,” Cambridge, MA: MIT press.

Milne, G. R., & Gordon, M. E. 1993. “Direct mail privacy-efficiency trade-offs within an implied social contract framework,” Journal of Public Policy & Marketing, pp. 206-215.

Moran, T. P. 1981. “Guest editor's introduction: An applied psychology of the user,” ACM Computing Surveys (13:1), pp. 1-11.

Nunnally, J. 1978. ”Psychometric theory,” McGraw-Hill, New York, NY.

Pahnila, S., Siponen, M., & Mahmood, A. 2007. “Employees' behavior towards IS security policy compliance,” System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference, pp. 156b-156b. IEEE.

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

Rogers, R. W. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology (91:1), pp. 93-114.

Schiaffino, S., & Amandi, A. 2004. “User–interface agent interaction: personalization issues,” International Journal of Human-Computer Studies (60:1), pp. 129-148.

Shneiderman. B.1992. “Designing the User Interface: Strategies for Effective Human-Computer Interaction,” 2nd edition. Addison-Wesley Publishing Company, Reading, MA.

Smith, H. J., Milberg, S. J., & Burke, S. J. 1996. “Information privacy: measuring individuals' concerns about organizational practices,” MIS quarterly, pp. 167-196.

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

Stone, E. F., & Stone, D. L. 1990. “Privacy in organizations: Theoretical issues, research findings, and protection mechanisms,” Research in personnel and human resources management, (8:3), pp. 349-411.

Sun, H., & Zhang, P. 2006. “The role of moderating factors in user technology acceptance,” International Journal of Human-Computer Studies (64:2), pp. 53-78.

Tam, E. C., Hui, K. L., & Tan, B. C. Y. 2002. “What do they want? Motivating consumers to disclose personal information to internet businesses, ”Proceedings of the Twenty-Third Annual International Conference on Information Systems, Barcelona, Spain. pp. 11-21.

Tan, M., & Teo, T. S. 2000. “Factors influencing the adoption of Internet banking,” Journal of the AIS, 1(1es), 5.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. 2003. “User acceptance of information technology: Toward a unified view,” MIS quarterly, pp. 425-478.

Van der Heijden, H. 2004. “User acceptance of hedonic information systems,” MIS quarterly, pp. 695-704.

Westin, A. F. 1968. “Privacy and freedom,” Washington and Lee Law Review, (25:1), 166.

Xu, H., & Teo, H. H. 2004. “Alleviating consumer's privacy concern in location-based services: A psychological control perspective,” Proceedings of the Twenty-Fifth International Conference on Information Systems, pp. 793-806.

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

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. 2009. “The role of push-pull technology in privacy calculus: the case of location-based services,” Journal of Management Information Systems, (26:3), pp. 135-174.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. 2011. “The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing,” Decision support systems (51:1), pp. 42-52.

Xu, L., Lin, J., & Chan, H. C. 2012. “The Moderating Effects of Utilitarian and Hedonic Values on Information Technology,” Continuance. ACM Transactions on Computer-Human Interaction (19:2), 12.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. 2012. “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), pp. 1342-1363.