Privacy Concerns of Users for Location-Based Mobile Personalization

Rakib Ahmed
The Australian National University

Shuk Ying Ho
The Australian National University

Follow this and additional works at: http://aisel.aisnet.org/confirm2011

Recommended Citation
http://aisel.aisnet.org/confirm2011/10

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2011 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Privacy Concerns of Users for Location-Based Mobile Personalization

Rakib Ahmed
The Australian National University

Shuk Ying Ho
The Australian National University

Abstract
With the proliferation of mobile technologies many firms have started using the mobile channel to advertise their products. To reduce the amount of irrelevant broadcast, location-based mobile services are employed to attract users’ attention to relevant mobile content. Compared with web-based applications, location-based mobile services can achieve a higher degree of personalization than web-based personalization due to the fact that mobile devices are carried by individuals anywhere and anytime. However, it also leads to higher concerns for privacy. This paper investigates users’ privacy concerns for location-based personalized mobile services. We look at four data management approaches and develop four hypotheses to examine how these approaches influence users’ privacy concerns when using location-based personalized services. Our findings show that providing notification regarding information collection, access to the information, choice, and security reduces users’ privacy concerns. Our findings provide empirical evidence to the practitioners and location-based personalized service developers, to consider various aspects of data management to ease users’ privacy concerns. This increases the marketability of location-based mobile services.

Keywords
Location-Based Service, Mobile Personalization, Data Management, and Privacy Concerns.

1. Introduction
Mobile commerce is gaining significance. It has become a continuously growing, large market for emerging services and applications (Allen 2003; Holzer & Ondrus 2010; Hong & Tam 2006; MMA 2008; Stafford & Gillenson 2003). Mobile merchants often use individuals’ mobile devices for interactive marketing and advertising. Among various marketing campaigns, using short message service (SMS) to promote products is the most common (Constantiou et al. 2007; Wei et al. 2010). We refer to short text messages for product promotion as mobile ads. Almost 75% of mobile users in Europe have reported receiving SMS ads (Wei et al. 2010). In 2007, mobile ads themselves generated a revenue of US $3 billion (Varnali & Toker 2010) with the projection of US $13 billion by 2014 (Wauters 2010).

Because mobile service providers avoid broadcasting spam messages that may be deemed irrelevant to some individuals, personalized SMS has become enormously popular (Chae & Kim 2003). Mobile service providers generally personalize SMS based on users’ locations. Interesting location-based services include automatic mobile news summarization (Chen 2010) and blue-casting (Duckham et al. 2007), which have been developed for forward-looking organizations to achieve competitive advantages by emphasizing targeted customers (Barnes 2003; Rao & Minakakis 2003; Chen 2010; Santos et al. 2010). In addition,
emergency and other service providers are also using numerous location-based mobile services. For instance, *Enhanced 911* wireless services in the USA augment the effectiveness and reliability of safety and security with accuracy from 50 to 300 meters (FCC 2010; Werbach 2000). *Mobile way-finding* helps urban pedestrians to quickly find their destination (Li 2006). The *Call a taxi* feature reduces the waiting time of passengers with the convenience of a touch of the “services” button (ICTR 2008).

Contrary to web applications, location-based mobile services achieve a higher degree of personalization because mobile devices are carried and used by individuals anywhere, anytime. The services can thereby offer more personalized and contextual services to its users but this comes at the cost of dynamically tracking of personal information (Crichard 2003). However, as disclosure of physical location and movement patterns are highly privacy-sensitive (Ardagna et al. 2009; Wei et al. 2010), issues regarding protection of personal information play a key role in the successful adoption of location-based personalized services. This concern has resulted in increased research in the innovation of privacy-aware location-based personalized systems (Duckham et al. 2007; Myles et al. 2003). However, because high-quality personalized service requires a lot of personal information, the association between privacy protection and quality of service is found to be inversely related (Duckham & Kulik 2006; Mokbel et al. 2006). A recent survey in the UK and the USA has shown 55% of users of personalized services feared loss of privacy and many of them thought that location-based personalization may let burglars know when they were away from home (Perez 2010).

Although prior research has made the effort to address technological issues that guide users to form positive perceptions of location-based mobile services, users’ privacy concerns about the services are always neglected. For instance, Soroa-Koury and Yang (2010) examined the effects of perceived usefulness and perceived ease-of-use on the adoption of mobile advertising without either addressing the “location-based” issue or including any relevant discussions about privacy concerns towards its adoption. Bruner-II and Kumar (2007) focused on developing a scale to measure individuals’ attitudes about location-based advertising on personal mobile devices. However, they did not consider users’ privacy issues regarding location-based personalized services. The objective of our paper therefore is to study users’ privacy concerns surrounding location-based mobile personalization. The research question of this study is: How do users’ privacy concerns affect the adoption of location-based personalized services?

To address the above research question, we looked at four data management approaches and examined whether and how these approaches ease users’ privacy concerns. We recruited 233 participants to take part in an experiment. In the experiment, they received personalized SMS and reported their privacy concerns after a four-week period.

The rest of this paper is structured as follows: Section 2 reviews literature on privacy and personalization and presents the hypotheses, which assists us in gaining an understanding of antecedents affecting users’ privacy concerns. Section 3 presents our experiment and its findings. Section 4 discusses the practical implications of the work, with some concluding remarks given in Section 5.
2. Literature Review

Research on individuals’ privacy concerns has grown significantly with the proliferation of the Internet and the wireless technologies in sales and marketing (Henderson & Snyder 1999; Paine et al. 2007). It demonstrates the mounting apprehension of individuals regarding potential threats to their information privacy (Tsai et al. forthcoming). For example, Paine et al. (2007) surveyed users of ICQ instant messenger with an automated interviewing tool and collected data from 530 respondents on their Internet privacy concerns. Their survey also included open questions for participants to describe their privacy actions. Stewart and Segars (2002) empirically looked at four aspects of privacy, including collection, errors, secondary use, and unauthorized access, and examined individuals’ concerns about organizational information privacy practices. However, as the behavior of online users is likely to vary from that of traditional offline users, Malhotra et al. (2004) considered three Internet-related factors, collection, control and awareness of privacy practices, to characterize Internet users’ information privacy concerns. McKnight et al. (2002) considered the behavior of online users to present a model with four high-level constructs, namely disposition of trust, institution-based trust, trusting beliefs, and trusting intentions. Although this research was conducted to examine users’ privacy concerns, McKnight et al. (2002) mainly focused on web-based commerce, and did not address concerns for context-based personalization such as location-based services.

In this research, we reference a privacy-trust-behavioral intention model developed by Liu et al. (2005) to examine mobile users’ concerns about location-based mobile services. Similar to the work by Liu et al. (2005), this study considers four dimensions of data management, notice, access, choice and security, and examines how data management approaches taken by companies influence individuals’ perceptions of privacy. This study examines in what manner mobile service providers should keep track of mobile users’ data so as to reduce mobile users’ privacy concerns. In the following, we will go through each dimension one by one.

First, the “notice” dimension is to provide individuals with a notice about how their personal data is being collected prior to the actual collection of that data. In fact, the data management factor, collection, has been introduced in prior research, such as (Malhotra et al. 2004)), that provides a similar definition of “notice”—it is a factor that “captures the central theme of equitable information exchange based on the agreed social contract” (p 338). If individuals are provided with data collection notifications before the data collection procedures take place, this will increase their awareness. Individuals may have doubts and concerns about why there is a need for the collection of their personal data, data collection procedures, and what mobile service providers plan to do with the data. Therefore, a notice indeed increases their privacy concerns, and individuals show a higher privacy concern to releasing their personal information. We hypothesize the following:

\[ H1: \text{If mobile users notice that their personal information is collected, then they will have a high privacy concern.} \]

Second, the “access” dimension is to provide individuals with access to the data that is collected about them. This aspect can reduce the concern of individuals regarding what personal information is collected or how the collected data is being used by the organizations. Stewart and Segars (2002) defined the terms, collection and secondary use, and suggested respectively the concerns that “too much data is collected” and “corporations use personal information for undisclosed purposes.” Phelps et al. (2000) found that 50% of the individuals
are interested in obtaining more information about the collected personal data and its potential use. For location-based services, mobile providers need to collect contextual data from individuals, and this is a growing concern for its users. Thus, it is likely that users will have a lower privacy concern if they are provided access to the information that has been collected. We anticipate the following:

**H2:** If mobile users are able to access their personal information collected in the personalization process, then they will have a low privacy concern.

Third, the “choice” dimension provides individuals with a choice of whether to allow an organization to use or share data collected about them. Malhotra et al. (2004) introduced a similar dimension, control where they raised the concerns as to whether users have control over their collected personal information and the facility to opt-in or opt-out. Mobile users may like to configure privacy parameters to set the level of personalization they want, based on their experience or level of trust about the provider. The choice of allowing an organization to use or share information has thereby a likely impact on users’ privacy concern.

**H3:** If mobile users have a choice to decide how mobile service providers use their personal information, then they will have a low privacy concern.

Fourth, the “security” dimension is to provide a reasonable assurance that the collected personal data is kept secure. Stewart and Segars (2002) presented the factor unauthorized access to accommodate the concerns of users regarding the failure of an organization to protect personal information. This particular dimension is also related to institution-based trust introduced in McKnight et al. (2002) which refers to an individual’s perception of the structural characteristics, namely safety and security, of the institutional environment. Location-based personalized service providers store the sensitive personal information of its users, such as users’ current physical locations. Therefore, we anticipate the assurance that the organization has provided security measures to protect personal information will result into lower privacy concerns. We propose the following hypothesis:

**H4:** If mobile service providers indicate that they provide security measures to protect the collected information, then mobile users will have a low privacy concern.

To test the above hypotheses, we conducted an experiment with 233 participants. The participants received location-based text messages on their mobile phones, which recommended food stores for their lunch. The recommendations were based on individuals’ personal preferences. The experiment spanned four weeks, at the end of which, the participants reported their privacy concerns.

### 3. Methodology

#### 3.1 Development of Mobile Personalization Systems

We developed a system to disseminate location-based personalized messages to individuals, and conducted the experiment from October 2009 to March 2010. The experiment context of this study was food store recommendations. Participants received a recommendation, in the form of SMS, on days when they planned to eat out. The recommendation presented the
name and description of a food store. The recommendation of the food store was personalized to match participants’ food and price range preferences.

Our personalization system had two modules: a mobile module and a web module. The mobile module analyzed participants’ profiles and generated personalized mobile content; in this case, a food store recommendation. It then sent the recommendations to participants’ mobile phones in the form of an SMS. The web module was developed to collect quantitative data. The module sent an auto-email to invite participants to complete an online questionnaire every weekend.

The process of “personalizing” recommendations was as follows: we recruited 15 students to provide lists of their favorite local food stores. We compiled these lists into 212 different food stores and supplemented the aggregate list with more food stores, which we found by searching the Internet. The final database contained 250 food stores. We used several attributes to describe each food store: name, location, cuisine (e.g., Chinese, Japanese), type of food (e.g., curry, fast food), average meal price, signature dish, and takeaway options. In the web questionnaire, participants reported their food preferences (cuisine and types of food), preferred price range, and intended days to eat out. The system detected the location of participants on the days they had planned to eat out and generated a recommendation based on location and food preferences.

We generated location-based mobile content as follows: First, we decided that the recommended food store must be within reasonable walking distance of the participant’s location. Because our participants would be students, we assumed that they would have neither the time nor the means to travel long distances for lunch. Specifically, the city in which the study was conducted is about 1,000 kilometers square and made up of eight districts. The average distance between the centers of two districts is 12.61 kilometers. The district in which the university is located is divided into 14 suburbs. The recommended food store was always in the suburb where the participant was located. We sent the recommendations to participants at 11:30am, giving them a reasonable amount of time to walk to the food store for a lunch break starting at 12 noon.

3.2 Experimental Procedure
We conducted the experiment from October 2009 to March 2010. The experimental procedures were made up of four parts. First, participants registered on a website. They filled in a short questionnaire on their demographics and food preferences (e.g., types of food, prices), and selected the days they would be likely to go out for lunch. The first part of the web process finished with a pre-task questionnaire. Second, on the mornings that participants were expecting to go out for lunch, the system sent a SMS to their mobile phones, offering food store recommendations. This process was repeated on each day the participant had indicated they would be eating out. Third, at the end of each week, the system sent an email to invite participants to complete an online post-task questionnaire in the web module and to update their eat-out days and food preferences. Lastly, at the end of the four-week study, participants completed a questionnaire on their privacy concerns.

---

1 The city was 1,000 kilometers square. The average size of each of the eight regions was 125 kilometers square. Assuming that the districts were circular, the distance between the centers of two districts was 12.61 (≈ sqrt(125 / π) × 2) kilometers.
3.3 Design and Manipulation
With limited resources, we planned to recruit about 200 participants. There were four dimensions of data management. A sample of 200 participants was not sufficient for a full-factorial design; otherwise, each treatment group might have only 12 participants (= 200 / 2^4 = 12.5). Also, as we planned not to examine the interaction effects between different data management dimensions, there was no need to adopt a full-factorial design. In the experiment, we divided the sample size into five groups.

Group 1 was the “notice” group. Participants in this group received a notice at the beginning of the experiment. The notice indicated that our system would keep track of their locations and analyze their food preferences. However, participants in this group had neither the access to nor the control over data collection. Also, we did not tell participants whether we stored their data in a secure way.

Group 2 was the “access” group. Participants in this group were given a link to access the collected data. They could only view their own data, but not others’. However, participants in this group had neither the notice nor the control over data collection. Also, we did not tell participants whether we stored their data in a secure way.

Group 3 was the “control” group. Participants in this group could opt out from the data collection process. That is, they could choose not to participate in the data collection procedures. However, participants in this group had neither the notice nor the access to data collection. Also, we did not tell participants whether we stored their data in a secure way.

Group 4 was the “security” group. Participants in this group were told that we had security measures to protect the collected data. That is, they were notified that our system was protected with anti-virus and firewall software, and only researchers involved in this project could access the data. However, participants in this group had neither the notice nor the access to data collection. Also, they could not choose to opt out from the data collection process.

Group 5 was the controlled group, which had neither the notice nor the access about data collection. They did not have any control over the data collection process. And we did not tell participants whether we stored their data in a secure way.

4. Findings
4.1 Participants
Our target participants were students in a public university in Australia. We believe that university students are authenticated participants because they are heavy mobile phone users (Kim 2002). We distributed flyers on the university campus to call for participants. The main study had 233 participants. After the participants registered, they were randomly streamed into different treatment conditions. Of 233 participants, 217 (128 males and 89 females; average age = 21 years) completed the whole study. All of them were active mobile phone users and they often went out for lunch. All participants went out for lunch at least one day per week.
4.2 Hypotheses Testing

H1 compares the difference in users’ privacy concerns towards location-based personalized services between Group 1 (the “notice” group) and Group 5 (the controlled group). The explanatory variable was the presence of notifications informing participants about the privacy data collection. The outcome variable was the average score of the three questions regarding users’ privacy concerns about location-based personalized services. We adapted an instrument of privacy concerns from Sheng et al. (2008). The four questions were “It bothers me that the service provider is able to track information about me,” “I am concerned that the service provider has too much information about me,” “It bothers me that the service provider is able to access information about me,” and “I am concerned that my information could be used in ways I could not foresee” (1 = Strongly Disagree; 9 = Strongly Agree). Results showed that there was a significant difference between users’ privacy concerns from Group 1 (mean = 5.46) and from that of Group 5 (mean = 7.70). However, we anticipated that the mean of Group 1 would be higher than Group 5, but what we found was the opposite. Hence, H1 was not supported (F(1, 80) = 21.27, p < 0.01).

H2 compares the difference in users’ privacy concerns towards location-based personalized services between Group 2 (the “access” group) and Group 5 (the controlled group). The explanatory variable was whether participants were given access to the collected data. The outcome variable was the same as in H1. Results showed that there was a significant difference between users’ privacy concerns from Group 2 (mean = 6.31) and from that of Group 5 (mean = 7.70), supporting H2 (F(1, 92) = 49.64, p < 0.01).

H3 compares the difference in users’ privacy concerns towards location-based personalized services between Group 3 (the “control” group) and Group 5 (the controlled group). The explanatory variable was whether participants could control the data collection process. The outcome variable was the same as in H1. Results showed that there was a significant difference between users’ privacy concerns from Group 3 (mean = 3.63) and from that of Group 5 (mean = 7.70), supporting H3 (F(1, 85) = 188.19, p < 0.01).
H4 compares the difference in users’ privacy concerns towards location-based personalized services between Group 4 (the “security” group) and Group 5 (the controlled group). The explanatory variable was whether participants were informed about the security measures to protect their personal data. The outcome variable was the same as in H1. Results showed that there was a significant difference between users’ privacy concerns from Group 4 (mean = 3.77) and from that of Group 5 (mean = 7.70), supporting H4 (F(1, 98) = 178.44, p < 0.01).

5. Discussion

Prior research has confirmed that personalization leads to issues regarding users’ privacy concerns (Tsai et al. forthcoming); however, it mostly focuses on web personalization. With the proliferation of mobile applications, mobile personalization, in particular location-based personalization, becomes common. Hence, this study aims to bridge the gap between the potential growth of mobile personalization and the lack of understanding of mobile users’ privacy concerns in using personalized mobile services. More importantly, we look at four dimensions of data collection and explore how these four dimensions affect users’ privacy concerns. Table 1 summarizes the findings.

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: If mobile users notice that their personal information is collected, then they will have a high privacy concern.</td>
<td>Not supported</td>
</tr>
<tr>
<td>H2: If mobile users are able to access their personal information collected in the personalization process, then they will have a low privacy concern.</td>
<td>p &lt; 0.01</td>
</tr>
<tr>
<td>H3: If mobile users have a choice to decide how mobile service providers use their personal information, then they will have a low privacy concern.</td>
<td>p &lt; 0.01</td>
</tr>
<tr>
<td>H4: If mobile service providers indicate that they provide security measures to protect the collected information, then mobile users will have a low privacy concern.</td>
<td>p &lt; 0.01</td>
</tr>
</tbody>
</table>

Table 1: Summary of Findings

This research leads to theoretical and practical contributions. First, personalization literature is mostly focused on preference matching, so we have enhanced the literature by involving a new personalization dimension, i.e., location. Much of the on-going research exploits location information for providing contextual personalized services. However, users’ privacy concerns regarding these services remain unexplored. Location is very sensitive personal information and is not desirable to disclose in many instances. It is an important contextual variable to consider because of its more dynamic nature and potential effectiveness in facilitating ease of living. This study to investigate the effect of privacy concerns also gives an insight for user-centric development of personalized services. Our research helps merchants and developers to investigate the balance between users’ rights and technology advancement, and to lead to a solution that balances rights and benefits for all the stakeholders.

Second, our findings provide significant insights for relevant business and practitioners. We have introduced four hypotheses in our study. H1 provides an important aspect of notifying users regarding the collection of information. Although the findings show H1 to be in the opposite direction to our initial prediction, it highlights a significant users’ perception regarding transparency and reliability. With a notice, users felt the mobile service providers to be more benevolent and reliable, and somehow their confidence in and trust towards the service providers improved which in turn reduced their privacy concerns. Mobile service providers can acquire valuable guidelines from H2, H3 and H4. It is evident that both access
to collected personal information and provision of users’ choice regarding the use of the information reduced their privacy concerns. As mentioned earlier, location information is very sensitive and may lead to potential threats to users. It is therefore very crucial for the service providers to ensure they keep the information safe and also protected from ending up in the wrong hands. Location-based personalized service providers can take these factors into consideration to increase the marketability of their products and services.

5. Conclusion
Emergence of location-based personalized mobile services has shown its potential to facilitate easier and faster services. At the same time it imposes the concerns for privacy to its prospective users. This paper has addressed this issue by investigating users’ privacy concerns regarding the adoption of location-based personalized services. We have used privacy perception theory to establish the theoretical framework for our research and examined how variables influence users’ privacy concerns and the adoption of location-based personalized services. It is apparent that personalized location-based mobile service providers should carefully consider users’ privacy concerns first before enhancing its location-detection or personal-data detection functions. This study also demonstrates the importance of location dimension to enrich personalization literature. Although this research sheds light on a newer aspect in location-based services, we acknowledge several limitations in this study. We have not covered users of more privacy sensitive services such as mobile banking. The sample used in this study was all university students. Although different demographic backgrounds were covered, participants from other professions, varied income groups and personalities would be more representative to generalize the findings.

References


Mobile Applications (2008), Mobile Marketing Association, USA


