Studying Location Privacy in Mobile Applications: 'Predator vs. Prey' probes

K. Thomas, C. Mancini, L. Jedrzejczyk, A. K. Bandara, A. Joinson,
B. A. Price, Y. Rogers, B. Nuseibeh
The Open University,
Milton Keynes, MK 76AA, UK
{k.thomas, c.mancini, l.jedrzejczyk, a.k.bandara, a.n.joinson, b.a.price, y.rogers, b.nuseibeh}@open.ac.uk

1. OVERVIEW

Although mobile privacy concerns are central to mobile applications, they remain poorly understood. We aim to study such concerns through a variety of user studies. Here in particular we discuss the use of a *breaching experiment*, which envisages putting participants in uncomfortable situations and forcing them to make their inner feelings and reactions observable. In relation to this experiment, we also discuss the use of a novel method - which we have already successfully used in a previous study - to enable the observation of a mobile user's spontaneous behavior without physically intruding their privacy.

2. METHOD

Privacy issues are sensitive and difficult to study, and therefore poorly understood. Survey methods such as questionnaires or standard interviews commonly used in requirements elicitation quickly gather large amounts of data but provide only limited insight into what users really feel and need when it comes to privacy. Asking users what level of privacy they want on their mobile phones may not reveal their actual preferences, because they may not know how they will actually feel and what they really need until they find themselves in a real situation. In addition, people communicate their response to a situation through different channels, such as verbal and facial expressions, voice tone, body language, behaviors, etc., all of which need to be taken into account. We propose that investigating mobile privacy requires an approach which allows for the cross-interpretation of data from diverse complementary studies [1]. We discuss the first of our studies elsewhere [6]; here we discuss our second study.

2.1 Predator vs. Prey Probes

Our second study aims to investigate some aspects of mobile privacy (namely those connected to location information) through a "breaching experiment" [2]. While these are common in ethnomethodological research [3], we are not aware of any that have been carried out to study privacy in mobile computing. The aim of the experiment is to 'force' people to make their feelings and reactions more obvious by putting them in an uncomfortable situation and observe how they adjust their behavior in order to make themselves comfortable again. The study involves a group of people using a mobile system that does not offer any privacy protection against the disclosure of their location to one another. We expect that this will trigger predator-prey dynamics underlying people's concerns about privacy and will allow us to observe the interaction among them. Our aim is to find out how people really feel about the disclosure of their location and, if and when they are concerned, how far they are prepared to go in order to avoid being tracked. Likewise, we expect that looking at what people do (what actions they take or what assumptions they make) with the information they get about others' location will also help us to understand why and how people feel the need to protect themselves. A group of 20 experienced mobile phone users will take part in the study over a period of three weeks. The participants' mobile phones will carry an application which can track the location of the other participants in the study and plot it on a map. In the first phase of the study, the participants will have no privacy controls to protect their location and will be free to use others' location information as they like. In the second phase of the study, participants will be given tasks such as investigating the location of co-participants and, based on that information, make inferences on what they are up to. In the third phase of the study, participants will have privacy controls and will receive alerts every time one of their co-participants is within a given geographical range or is checking their location. We expect the study to reveal patterns than might explain why people may want to access others' location information or protect their own location information. For example, in one scenario, A might want to use B's location information to maintain certain control over them and make sure that certain social rules are respected ("Are you there? Why are you there at this time?"); at the same time, B may wish to escape A's control and give themselves the space to break those rules without incurring the social consequences. In another scenario, A may want to know where their peers are and whether they are together, as A feels the need to be included in the group and is afraid that the group might exclude them ("Are you at the pub with C and D? May I join you, I feel like having a drink?"); but B may be having a meeting with other common peers and may not wish A to be part of it. Finally, A might want to know where B is to take advantage of B's location for personal gain ("While you are there, could you buy some x for me, please? I forgot to get it"); however, B may not wish to be at others' disposal. Breaking location privacy boundaries and forcing people to take action to re-establish them will enable us to observe and understand this kind of emerging patterns, which is critical if we are to understand people's drives and motivations in acquiring or divulging personal information.

2.2 Enhanced Experience Sampling

Experience sampling has been used in user studies to capture data about people's feelings and behaviors in daily life situations in a non-intrusive way and over an extended period of time [4]. Usually, this is done by giving or delivering a set of questions to the participants in the study, either on paper or electronically, automatically or manually, at regular intervals, or upon the

occurrence of specific events. This method is used when it is impractical to use direct observation methods, as is the case when studying mobile privacy: any direct observation method would result in a modification of what would otherwise be spontaneous behavior. For reasons on which we elaborate elsewhere [6], in mobile privacy studies an experience sampling questionnaire can only ask for a minimum feedback that can be provided in the shortest possible time. On the other hand, in order to be useful, the feedback needs to provide detailed information about specific situations and the contexts in which they occur. This detailed information can be better communicated by participants during one-to-one interviews, but these usually take place with some delay with respect to the participants' experiences, so it is likely that some of the important contextual information ends up getting lost as participants usually remember only some of the details relating to their experiences. In order to gather rich and meaningful data from real-life experiences, we have devised a method that combines experience sampling and semi-structured interviewing techniques specifically adapted for the study [6].

2.2.1 From experience sampling to memory triggering

Our experience sampling questions are delivered via mobile phone, which makes it easy for the participant to contribute their feedback. The participant can quickly answer the questions by choosing from a set of predefined multiple-choice answers. Their answers are then discussed in one or more follow-up interviews. Because they may have to provide feedback on several events in a day and because the interview may take place a number of days after the occurrence of an event, participants are requested to provide a *memory phrase*, which can be anything they associate with the particular event they provide feedback on. Because participants themselves choose the memory phrase they wish to associate to an event, the phrase constitutes a powerful trigger, which is capable of bringing the participant back to the event's context.

2.2.2 Deferred contextual interviews

Once participants have reconnected to those events, they are able to provide detailed information about their experience of them during interviews. The interviewer reminds the participant of the memory phrase they associated with a particular event and, as the participant goes back to it in their mind, the interviewer can use the experience sampling questions and answers as pointers to different aspects of the participant's experience. As our previous study shows [6], this method enables participants to retrieve far more information than the experience sampling questions could possibly allow them to record during the study. Given the effectiveness of the memory phrase in bringing the participant back to a particular experience and the context in which it took place, the interviewer can carry out what effectively constitutes a *deferred* contextual interview, which can elicit detailed and specific information about the context in which certain events took place.

2.3 Implementation

The implementation of our method first required the identification of a suitable mobile device. The evaluation of the mobile devices available on the market was based on four criteria: i) accuracy of location information, to allow for accurate tracking ii) size of graphical display, to enable the display of maps iii) usability of the device, to offer a user-friendly interaction iv) popularity among the public, to facilitate the recruitment of participants. iPhone met most of these criteria.

The software system for the study consists of a client system on an iPhone which allows users to track their co-participants in the study. For this, the client makes use of the Google API to display the location of the subject on the map. For the third phase of the study, the client system supports additional features to provide real-time feedback on who is tracking whom and to provide fine-grained privacy-management controls.

An integral part of the system is a centrally hosted Server which polls for specific events. When an event is detected, the server generates and sends, via 3rd party SMS gateway, an SMS to the user with an embedded URL. By opening the SMS and clicking on the URL, participants connect to the User Feedback System (UFS). The UFS is a web application optimized for display on a mobile device, in this case an iPhone. Once connected to the UFS using the mobile browser, participants are prompted to answer the experience sampling questions and provide a memory-phrase.

3. SUMMARY

Privacy in mobile applications is difficult to study. However, our approach, which entails the use of 'breach experiments', enhanced experience sampling, and deferred contextual interviews is a promising way forward. We have already used the proposed method in a recently concluded study called 'Mobile Facebook Practices' with encouraging results [6]. We are currently recruiting participants for the 'Predator vs. Prey' study.

4. REFERENCES

[1] Smith, H., G. Fitzpatrick, and Y. Rogers. Eliciting reactive and reflective feedback for a social communication tool: a multi-session approach. Proc. Designing interactive systems: processes, practices, methods, and techniques 2004. p. 39-48.

[2] Mancini, C., et al., 2009. A Multi-Pronged Empirical Approach to Mobile Privacy Investigation. Workshop on Mobile User Experience Research: Challenges, Methods & Tools, CHI '09, 5-10 April, Boston, USA.

[3] Rogers, Y., et al., Why It's Worth the Hassle: The Value of In-Situ Studies When Designing Ubicomp, in UbiComp 2007: Ubiquitous Computing. 2007, Springer Berlin Heidelberg. p. 336-353.

[4] Consolvo, S. and M. Walker, Using the experience sampling method to evaluate ubicomp applications. Pervasive Computing, IEEE, 2003. **2**(2): p. 24-31.

[5] Holtzblatt, K., Top Field Interviewing Mistakes: Recognizing and Preventing Them, CHI 2009.

[6] Mancini, C., et al., From Spaces to Places: Emerging Contexts in Mobile Privacy. 2009, The Open University: Milton Keynes, UK. Report #: TR2009-08, http://computing-reports.open.ac.uk/2009/TR2009-08.pdf.

[7] Proust, M., A La Recherche du Temps Perdu. 1912-28, Paris: Grasset & N.R.F.