A Multi-Pronged Empirical Approach to Mobile Privacy Investigation

First Author
Clara Mancini
Department of Computing
The Open University
Milton Keynes, MK7 6AA, UK
C.Mancini@open.ac.uk

Second Author
Yvonne Rogers
Department of Computing
The Open University
Y.Rogers@open.ac.uk

Third Author
Lucasz Jedrzejczyk
Department of Computing
The Open University
L.Jedrzejczyk@open.ac.uk

Fourth Author
Keerthi Thomas
Department of Computing
The Open University
K.Thomas@open.ac.uk

Fifth Author
Blaine Price
Department of Computing
The Open University
B.A.Price@open.ac.uk

Sixth Author
Adam Joinson
School of Management
University of Bath
Bath, BA2 7AY, UK
A.Joinson@bath.ac.uk

Seventh Author
Arosha Bandara
Department of Computing
The Open University
A.K.Bandara@open.ac.uk

Eighth Author
Bashar Nuseibeh
Department of Computing
The Open University
B.Nuseibeh@open.ac.uk

CHI 2009, April 5 – April 10, 2009, Boston, USA
ACM 978-1-60558-012-8/08/04.

Abstract
We describe the design of three empirical studies planned as part of an investigation into privacy when mobile. The studies exemplify complementary investigation strands, whose aim is to uncover the multi-faceted nature of privacy for mobile computing applications.

Keywords
Mobile privacy requirements, empirical investigation

ACM Classification Keywords
D.2.1: Requirements: elicitation methods; J.4 Social and Behavioural Sciences: sociology; K.4.1: Public Policy Issues: privacy

Introduction
The PRiMMA (Privacy Rights Management for Mobile Application) project [1] is investigating privacy requirements for mobile computing technologies with the aim of producing a privacy-management reusable framework with demonstrator applications. In this paper, we describe three empirical studies to be carried out within the project, which exemplify complementary approaches to the investigation of privacy requirements for mobile computing.

An enormous amount has been written about privacy in HCI, but privacy issues are so complex and sensitive

that, not only are they still not fully understood, they are also very difficult to study. While research methods such as questionnaires or interviews, commonly used in requirements elicitation, can gather large amounts of information quickly and cheaply, they provide 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, for instance, would be like asking self-proclaimed healthy eaters if they prefer to snack on a piece of fruit or on a candy bar: everyone says they prefer fruit, but when it comes to actually choosing one or the other, many go for the candy bar [2]. Furthermore, any methods employed to investigate privacy should take into account the fact that communication has many channels: verbal and facial expressions, voice tone, body language, behaviours, etc., all contribute to the meaning of someone's response to a situation, whether the responder is aware that they are communicating through them or not. Often it is the information that we give away spontaneously and unwittingly that is the most revealing.

In other words, investigating privacy requirements necessitates a diversified approach, one that allows researchers to closely observe users' spontaneous communication processes while they are in action. Here we describe three different types of user study, through which we propose to observe: 1) how people deal with privacy issues as part of their daily practices when using networking services on their mobile phones; 2) how people react when using mobile devices that offer no privacy protection and how they compensate for such sudden loss; 3) what emotional responses people have in relation to privacy issues when presented with mobile computing future scenarios.

Mobile Facebook Practices

According to some [3], Facebook has become the leading social networking site, offering a wealth of functionalities and allowing the sharing of both information and artefacts. Consistently with its wide-spread use, Facebook is also possibly the most studied networking application in relation to privacy. Some have focussed on location disclosure (e.g., [4]), while others have looked at motivations and uses (e.g., [5]). However, to understand how people really feel about privacy, it is critical to understand how people's networking practices integrate with their daily life practices and routines (see [6] and [7]). In this first study, we will observe how Facebook activities integrate with people's other daily practices, in order to identify behavioural patterns relevant to privacy concerns, when people deal with an existing technology that is already familiar to them. In particular we will focus, on the one hand, on status updates and photo uploading and tagging in Facebook (a little studied and potentially very interesting area), on the other hand, we will look at how these Facebook activities relate to other activities carried out by the participants and to their engagement with the surrounding environment.

We plan to run this experiment with around 20 participants, over a period of three weeks. Participants will be experienced and enthusiastic users of Facebook on mobile phone and desktop computer. They will all be using the same type of phone (e.g., Nokia N95), in order to avoid inconsistencies due to the different functionalities and user interface features of different phones. A control group will be participating using desktop computers instead of mobile phones. We will record participants' Facebook activity, accessing their Facebook accounts via an application that we are

currently implementing, which will also record contextual information such as location, time, etc. During the first week, we will take part in the experiment to directly observe any networking activity. During the second and third week, one researcher will also shadow some of the participants for short periods of time to observe any behavioural patterns.

It is our deliberation to approach this kind of exploratory study as open-mindedly as possible in order not to prejudice the interpretation of the findings with references to existing frameworks. Nevertheless, we do have questions about what we might find. For instance, is it reasonable to expect that any differences in the way people use Facebook at their desktop and on their mobile reflect the way in which the privacy cost-benefit relationship changes in the two different scenarios? At their desktop people may feel safer and less exposed than in public places (where they are likely to use their mobile) and their use of Facebook may reflect their feeling of relative safety. However, as the potential interactions with the physical world increase they may feel that the privacy costs (e.g., being over-looked, over-heard, intercepted, etc.) are worth paying in order to take advantage of the added benefits (e.g., using the service to meet-up with friends, stalk people, etc.). Furthermore, is it reasonable to expect that the level of awareness about the potential costs of using Facebook on a mobile device may decrease as people are 'distracted' by those added benefits? In a public place people may become oblivious to the fact that certain information about them could become accessible to undesired witnesses, because they are enjoying the exchanges that the mobile experience can offer. This is the sort of questions this experiment can begin to answer and whose answers will play a key role in determining what kind of privacy management requirements our framework needs to satisfy.

Predator vs Prey Probes

Our second study is a kind of 'breaching experiment'. We are not aware of any studies of this nature with regard to privacy in mobile computing, but they are common in ethnomethodological research [8]. The idea is to 'force' people to make their feelings and reactions obvious by putting them in an uncomfortable situation to observe how they behave in order to make themselves comfortable again. The study entails getting a group of people to use a mobile system that does not offer any privacy protection against the disclosure of their location. Hopefully this will trigger a pray-predator dynamic, which underlies people's concerns about privacy, allowing us to observe it closely. Our aim is to find out how people really feel about the disclosure of personal information and, if and when they are concerned, how far they are prepared to go in order to avoid being tracked-down. Likewise, 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 two weeks. The participants' mobile phones will carry an application, whose implementation we are currently completing and which can track the location of other mobile phones and plot it on a Google map. As with the first study, we will record participants' mobile phone activity, calls and contextual information such as location, time, motion, etc; one researcher will also take part in the

experiment during the first week and will then shadow some of the participants during the second week.

For this study we cautiously advance a hypothesis on what sort of patterns might emerge that describe the reasons why people may want to access other's location information or protect their own location information. For one thing, A might want to use B's location information to maintain a certain control over them and make sure that certain social rules are respected ("Are you there? Why are you there at this time?"); however, B may wish to escape A's control and give themselves the space to break those rules without incurring the social consequences. For another thing, 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 a drink?"); however, B may be having a meeting with other common peers but may not wish A to be part of it. Finally, A might want to know where B is as they want to take advantage of B's location for personal gain ("While you are there, could you buy some bread for me, please? I forgot to get it when I went to the store."); 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 when it comes to acquiring or divulging personal information.

Mobcomp Visions

In the third study we will film two futuristic scenarios, getting a group of potential users to watch and discuss the films. A similar study has been carried out with regard to the implementation of ubiquitous healthcare systems [9]. In that study, the futuristic system represented could do anything that appeared to be desirable. Similarly, we will represent the futuristic mobile application that we wish to be able to prototype by the end of the project (or that our research will have made possible to implement in the near future). However, we will produce two films, each ten minutes long: the first film will represent a utopian scenario, demonstrating the features of our imaginary application and how perfectly they integrate with people's daily life; on the other hand, the second film will represent a dystopian scenario, demonstrating how our imaginary application could cause adverse effects in people's lives. The purpose of the study is to face people with scenarios that explore the benefits and risks of having advanced mobile technology in a way that is emotionally engaging (and film is a very powerful media when it comes to triggering emotions: see [10]). The idea is to trigger an emotionally involving discussion, by teasing out people's (possibly subconscious) feelings about the subject.

Two groups of 10 participants will take part in the experiment, respectively viewing the film about the utopian scenario and the dystopian scenario, and then engaging in a semi-structured discussion guided by one of the researchers. The participants will have some awareness of mobile computing devices, to be able to relate to the subject of the discussion. We will video-record both the viewing of the film and the discussion, in order to capture body language, facial and verbal expressions, etc., of viewers during both the projection of the films and the discussion.

Again, without wanting to prejudice the analysis of the experimental data, we conjecture that in the face of a

perfect scenario, people will start thinking of the negative aspects of such a reality; on the other hand, in the face of a perfect scenario gone wrong, people might start thinking of the positive aspects, as a way of counterbalancing the negative scenario represented by the films. Then again, we might find that in the face of perfect scenarios people think of yet more possible positive effects of advanced mobile computing, while in the face of rotten scenarios they might conceive of even more catastrophic effects. Again, the main interest here is in finding out people's visceral reactions when presented with different prospects and identifying thinking patterns in groups of people exposed to different emotional experiences.

Conclusions

The studies described above are complementary to one another and aim to uncover different aspects of the relation between mobility and privacy. Such a relation is multi-faceted and only a multi-pronged approach can provide us with the insights we need to understand it. So, the first study focuses on what happens to our privacy concerns when mobile devices follow us into the physical world and how the interactions mediated by such devices integrate with our physical life. The second study aims to identify our privacy boundaries by breaching them and looking at what predators and preys do to take advantage of others' or escape their own exposure. Finally, the third study looks into our emotional reactions when we are projected into a world in which ubiquitous computing is part of the fabric of our daily life and mediates many of our interactions with the world. These studies will provide us with a rich corpus of experimental data consisting of textual, photographic, audio and video records. We will analyse the records relative to different communication channels in counterpoint, juxtaposing participants' different forms of expression and action.

Acknowledgements

This is a joint research project between The Open University and Imperial College London and is funded by the UK Engineering and Physical Sciences Research Council – EPSRC (EP/F024037/1).

References

[1] http://primma.open.ac.uk

[2] http://www.usatoday.com/tech/science/2008-09-21-big-brother-restaurant_N.htm?csp=34

[3] http://en.wikipedia.org/wiki/Facebook

[4] Voong, M. and Beale, R. (2008). Representing Location in Location-Based Social Awareness Systems. *Proceedings of HCI'08*.

[5] Joinson, A. N. (2008). 'Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook. *Proceedings of CHI'08*, pp.1027-1036.

[6] Tolmie, P., Pycock, J., Diggins, T., MacLean, A., Karsenty, A. (2002). Unremarkable Computing. *Proceedings of CHI'02*, pp. 399-406.

[7] Ebbjörnsson, M. and Weilenmann, A. (2005). Mobile Phone Talk in Context. *CONTEXT'05*, pp.140-154.

[8] Garfinkel, A. (1984 - reprint). *Studies in Ethnomethodology*. Polity Press.

[9] Little, L., Briggs, P. (2008). Ubiquitous Healthcare: Do We Want It? *Proceedings of HCI'08.*

[10] http://www.youtube.com/watch?v=oXuLhcMdfLk