Supporting Location Privacy Management through Feedback and Control

Thesis

Supporting Location Privacy Management through Feedback and Control

Łukasz Jędrzejczyk, BSc, MSc

A thesis submitted to The Open University
for the degree of
Doctor of Philosophy in Computing

Department of Computing
Faculty of Mathematics, Computing and Technology
The Open University
Milton Keynes, UK

August 2011

Keywords: awareness systems, feedback, mobile computing, location based services, privacy management, location, privacy, social translucence, mobile interaction design.

This thesis is dedicated to

my wife Monika

my sons Tymek and Filip

and my family.

Abstract

Participation in modern, socially-focused digital systems involves a large degree of privacy management, i.e. controlling who may access what information under what circumstances. Effective privacy management (control) requires that mobile systems' users be able to make *informed* privacy decisions as their experience and knowledge of a system progresses. By *informed*, we mean users be aware of the actual information flow. Moreover, privacy preferences vary across the context and it is hard to define privacy policy that reflects the dynamic nature of our lives.

This research explores the problem of supporting awareness of information flow and designing usable interfaces for maintaining privacy policies ad-hoc. We borrow from the world of Computer Supported Collaborative Work (CSCW) and propose to incorporate social translucence, a design approach that "*supports coherent behaviour by making participants and their activities visible to one another*". We use the characteristics of social translucence, namely *visibility*, *awareness* and *accountability* in order to introduce social norms in spatially dispersed systems. Our research is driven by two questions: (1) how can artifacts from real world social interaction, such as responsibility, be embedded into mobile interaction; and (2) can systems be designed in which both privacy violations and the burden of privacy management is minimized.

The contributions of our work are: (1) an implementation of Buddy Tracker, privacy-aware location-sharing application based on the social translucence; (2) the design and evaluation of the concept of real-time feedback as a means of incorporating social translucence in location-sharing scenarios; and finally (3) a novel interface for ad-hoc privacy management called Privacy-Shake.

We explore the role of real-time feedback for privacy management in the context of Buddy Tracker. Informed by focus group discussions, interviews, surveys and two field trials of Buddy Tracker we found that when using a system that provided real-time feedback, people were more accountable for their actions and reduced the number of unreasonable location requests. From our observations we develop concrete design guidelines for incorporating real-time feedback into information sharing applications in a manner that ensures social acceptance of the technology.

Acknowledgements

This is for my supervisors: Arosha Bandara, Bashar Nuseibeh and Blaine Price who *spotted the potential* and gave me the opportunity to explore the world of science. The work presented here would not have been possible without the guidance and support they provided me over the past 3 years I spent at The Open University. I will always be grateful to them for their help and invaluable contribution to the work presented in this thesis.

This is to my family, especially my beloved wife Monika for her love, the patience and continuous support over the past 3 years. I would like to thank my son Tymek for keeping mummy busy while daddy was at *uni*.

This is to the PRiMMA team members: Yvonne Rogers, Clara Mancini, Keerthi Thomas for their intellectual support and comments, which helped shape the work presented here. I would also like to thank to PRiMMA members from Imperial College London. I also want to thank to Domenico Corapi for his help in building the learning engine presented in Chapter 6.

Finally, I would like to acknowledge other students and members of The Computing Department, in particular members of the PG Forum for sharing their experiences with the community. I am indebted to Marian Petre and Robin Laney for hosting the forum and giving us (students) opportunity to meet and discuss our research in the larger group.

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

> "*The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used (...), and what are the consequences of any given action.*"
>
> Mark Weiser

According to Altman (Altman 1975), privacy can be regarded as an ongoing process of regulating boundaries. At the heart of Altman's theory is an environment that provides tools and mechanisms for regulating privacy. The environment can be regarded as physical structures (walls, position of physical items) (Archea 1977; Kupritz 2000), systems (Kupritz 2000), meaningful places, social actions, or events (Heft 2001) that determine our behaviour. One of the key properties of Altman's privacy regulation theory is bi-directionality, whereby privacy regulation is a social process involving *input* from (i.e. noise, previous experience) and *output* to the environment (e.g., communication).

Longitudinal accumulation of experience with an environment builds social awareness, a shared knowledge that helps us structure our interactions with one another. According to Dourish and Bellotti awareness is *an understanding of the activities of others, which provides a context for your own activity* (Dourish and Bellotti 1992). Evidence from the literature shows that awareness is an important element of the privacy management process, because it conditions our social interaction (Erickson and Kellogg 2000), affects our privacy decisions and impacts our comfort in sharing information (J. Y. Tsai et al. 2009). In this respect, the task of a privacy-aware system designer is to create environments (e.g. ubicomp systems) that can incorporate artifacts from the physical world into digital systems in a way that supports continual privacy management (Palen and Dourish 2003).

Continual privacy management in both online and offline activities requires people's ability to share their information with others (*output*) but also sense *input* from others (e.g., when others make comments about them, respond to them during a conversation or view who looked their location information).

In the physical world, when someone walks in the street they can be seen by others but can also see others around them. However, apart from academic examples (Toch et al. 2010), socially-focused applications make it easy to share information but not easy to sense input from others (e.g. Google Latitude[1]), in that the user can be seen without knowing that others are looking at them. This contradicts Altman's bi-directional property of privacy, which says that privacy regulation requires both *output* (sharing) and *input* (sensing, feedback).

Previous studies have shown that end-users have difficulties in expressing and setting their privacy preferences, and their privacy policies change only marginally unless they are given tools that help them understand the implications of their privacy-related choices (Cranor and Garfinkel 2005; Sadeh et al. 2009). This has been reasserted by Nguyen and Mynatt who argued that in the socio-technical ubicomp systems (systems that encompass social, technical and physical environments) *privacy is addressed best by giving users methods, mechanisms and interfaces to understand and then shape the system in all three environments* (Nguyen and Mynatt 2002).

The key problem we address in this thesis is that current privacy-awareness solutions for socio-technical systems provide insufficient support for traditional human to human behaviour, which results in lack of enforcement of social norms. In consequence end-users cannot draw upon their face to face world experience to structure interactions with others in digital systems. Although ubicomp encompasses social, technical and physical environments, there is no coherence between the human behaviour in the face to face world and actions in the digital systems. As stated above, privacy regulation requires *input* and *output* from the environment, thus more

[1] www.google.com/latitude/

work is needed that will enable people to manage privacy in digital systems in a way that is more consistent with their behaviour in the non-digital world.

Although significant attempts have been made to support *awareness* in ubicomp systems (Hong 2005; Langheinrich 2005), usable *awareness interfaces* design remains a big challenge. We define awareness interfaces as those which deliver timely information in a meaningful manner in order to help users understand the extent to which the (invisible) system manipulates information.

We see the lack of previous work in awareness interfaces as a strong motivation to design privacy awareness tools that help users make informed privacy decisions as their experience and knowledge of a system (environment) progresses. We borrowed from Altman's privacy regulation theory as well as Erickson and Kellogg's concept of social translucence in supporting awareness through shared understanding that enforces accountability by making things visible to one another. We propose to build privacy-sensitive systems supporting the continual and selective disclosure of personal information by supporting awareness. Awareness is achieved by real-time feedback as the method of informing users about how their information is being used. In our work we define feedback to be the notification of information disclosure, where the notification specifies *what information about the person is disclosed when and to whom*. This definition is drawn from the work of Bellotti and Sellen (Bellotti and Sellen 1993).

This thesis addresses two problems that we have identified. To address the lack of privacy awareness tools, we describe a context-aware real-time feedback system that incorporates bi-directionality and social translucence in the ubicomp scenario. We evaluate our privacy-awareness system in the context of Buddy Tracker, a mobile, location-sharing application.

The second problem that this thesis addresses is that of managing privacy, which is a cumbersome task that many people are unwilling to do due to the time effort. Moreover, all known privacy management solutions are based on graphical user interfaces, and treat privacy management as a main task, while privacy is a very contextual concept. Visual interfaces absorb

the user's attention and require the user to grapple with the application while their main goal is to interact with the physical (Robinson, Eslambolchilar, and Jones 2009).

To further address the privacy interface problem, we describe "Privacy-Shake" (Jedrzejczyk et al. 2010a), a novel interface for managing coarse grained privacy settings. We present a prototype that enables users of Buddy Tracker to enable or disable sharing and change the level of granularity of disclosed information by moving their phone in specific ways (shaking and sweeping gestures).

1.1. Research Problems

We derive the following questions from the above motivation that addresses the problem of designing feedback and control that enables users of socio-technical systems to manage their privacy in a more natural manner:

- Can elements from real world social interaction (e.g. responsibility, accountability) be embedded into ubicomp systems through awareness?
- Can systems be designed in which both privacy violations and the burden of privacy management is minimized?

Ubicomp encompasses three environments: technical, physical and social; and can be regarded as an ecology of devices (technical) situated in the physical space (physical), in which people are connected (social). There are several smaller problems associated with each environment. Therefore from the questions above we derived a number of sub-problems focused on technical, physical and social aspects of feedback and control in ubicomp:

i. Insufficient support for traditional (non-digital) human behaviour and lack of support for social norms does not enable end-users to draw upon their real world (non-digitally mediated) experience to structure interactions with others when using digital systems. Therefore novel interactions are needed that will support participation in socio-technical systems and allow social norms to be upheld. A question of how to build a new

informational society, in which behaviours in the face-to-face word and digital system are consistent, is still unexplored.

ii. Although several attempts have been made to support awareness in the digital systems, usable awareness interfaces design remains a big challenge. Previous work does not address an important issue for awareness interfaces: how to deliver timely information in a meaningful manner in order to help users understand the extent to which the (invisible) system manipulates information. For example, how to bring the privacy awareness technology into the physical world in a way it is socially acceptable?

iii. Inadequate and non-effective feedback. With a few exceptions, most awareness interfaces focus only on historical aspects of feedback, and there is no evidence in the literature that end-users actually use the historical feedback feature. Consequently, there is little evidence that historical feedback has an impact on users' behaviour, apart from improving the comfort of sharing location information. Therefore the impact of real-time feedback technology on users' behaviour needs to be explored.

iv. Emphasis on visual representations for feedback. Although novel ubicomp devices provide several methods supporting human-computer interaction, current privacy awareness solutions are mainly focused on visual feedback, which is not appropriate in the dynamic environments of Ubiquitous Computing. Therefore, alternative feedback representations require more attention.

v. Since privacy is a contextual and malleable concept, novel ways for expressing privacy preferences are required that will support ongoing privacy management in the context.

1.2. Objectives and Contributions

Prior to presenting the main contributions of this dissertation, we first sketch the key objectives using the MOST strategy (Mission, Objective, Strategy, and Tactics) (Campbell and Alexander 1997):

Mission: To enable end users to draw upon their real-world experience and social norms to structure interactions with others in ubicomp systems.

Objective: To adapt bi-directional function of privacy and characteristics of social translucence, namely *visibility*, *awareness* and *accountability*, into ubicomp systems.

Strategy: To build novel tools for feedback and control that will enable the user to understand the dynamics of information flow and will support a continuous privacy management process.

Tactics:

i. To propose a privacy-aware system architecture based on the concept of social translucence and evaluate the privacy-protection potential of the proposed architecture;
ii. To support multiple sensory dimensions of feedback representation;
iii. To design novel interaction methods for expressing privacy preferences in different contexts.

I claim the following novel contributions of this thesis:

1. Buddy Tracker, a privacy-aware location-sharing application based on Altman's privacy regulation theory (in particular the bi-directional property of privacy) and social translucence supporting *visibility*, *awareness* and *accountability* aiming at incorporating social rules in spatially dispersed systems by bridging technical, social and physical environments.
2. A design and evaluation of a real-time feedback concept as a means of incorporating social translucence in a location-sharing scenario. This thesis presents a classification of feedback and provides guidance on how it can be implemented in mobile applications. This thesis provides empirical evidence that real-time feedback is an effective tool for supporting users' privacy.
3. Examination of the role of context-awareness at improving real-time feedback. A context-aware extension has been built into the real-time feedback system to improve

the user experience and social acceptance of the technology. Context-aware real-time feedback is a bridge between three different environments covered by ubicomp systems.

4. A novel interface for ad-hoc privacy management, namely Privacy-Shake. We propose a concept of the haptic interface for managing coarse grained privacy. A prototype has been built and evaluated with respect to usability, support for privacy management tasks and social acceptance.

This thesis also provides several additional contributions:

5. Clear proposition of what mobile context is and how it can be used to design for better user experience.
6. A working prototype of context-aware, socially translucent system that meets Bellotti and Sellen's criteria.
7. Support for researchers conducting field studies on privacy in location sharing technologies. Software used in this research (server application, Buddy Tracker application and the Real-Time Feedback Manager) is freely available from www.buddytracker.open.ac.uk.

1.3. Research Approach

The research presented in this thesis has taken an extended user-centred design approach proposed in (Harper et al. 2008) and follows an iterative cycle that consists of five phases: (1) understand, (2) study, (3) design, (4) build and (5) evaluate (due to the time limitations we could not re-iterate the design process of Privacy-Shake, in this thesis we present results of one iteration). The decision to take this approach was largely motivated by the nature of our research problem, which includes human factors and user interface design.

1.3.1. Designing Real-Time Feedback

During three years of our research on the feedback mechanisms for privacy management we have gone through three design iterations. Here we present goals and research methods used during each design phase. All three cycles detailing phases and methods used are presented in

the Figure 1-1. Different studies conducted during our research are described in detail in the further part of this thesis.

The first phase (understand) was largely supported by data collected during the literature analysis (especially during the first iteration), project meetings and discussion with domain experts and potential users. Since in the first iteration we identified human values we decided to design for (i.e. supporting privacy-awareness and social-norms enforcement in the digital systems), during next iterations we were focused more on the user-experience and social-acceptance.

In the second phase (study) we made use of focus groups and interviews in order to collect richer and more precise data about how those values should be incorporated into the design and how people achieve those values in the real-world. We looked at how a privacy-awareness system should be designed and what factors have an impact on users' experience and social acceptance of the technology in the real-world.

The third phase (design) involved analytical and creative work aimed at identifying design implications and issues related to our technology that have been highlighted in the previous phases. We have identified key design goals underpinning our design choices, such as appropriate timing, unobtrusiveness or support for context-awareness.

In the next phase we made a step towards working interfaces that could be evaluated. We have built a functional application that helped us evaluate our technology and its impact on users' experience, their behaviour and their comfort of using the technology. We started from paper designs and low-fidelity wireframes, then we developed a series of high-fidelity prototypes and finally working and complete application was built.

Next, we looked at how our technology affected the people and studied people's reaction to the technology. We incorporated both in the lab and field trial methods during evaluation phases.

We used memory triggering mechanisms, experience sampling method and instrumented interfaces in order to gather richer understanding of the user and his context.

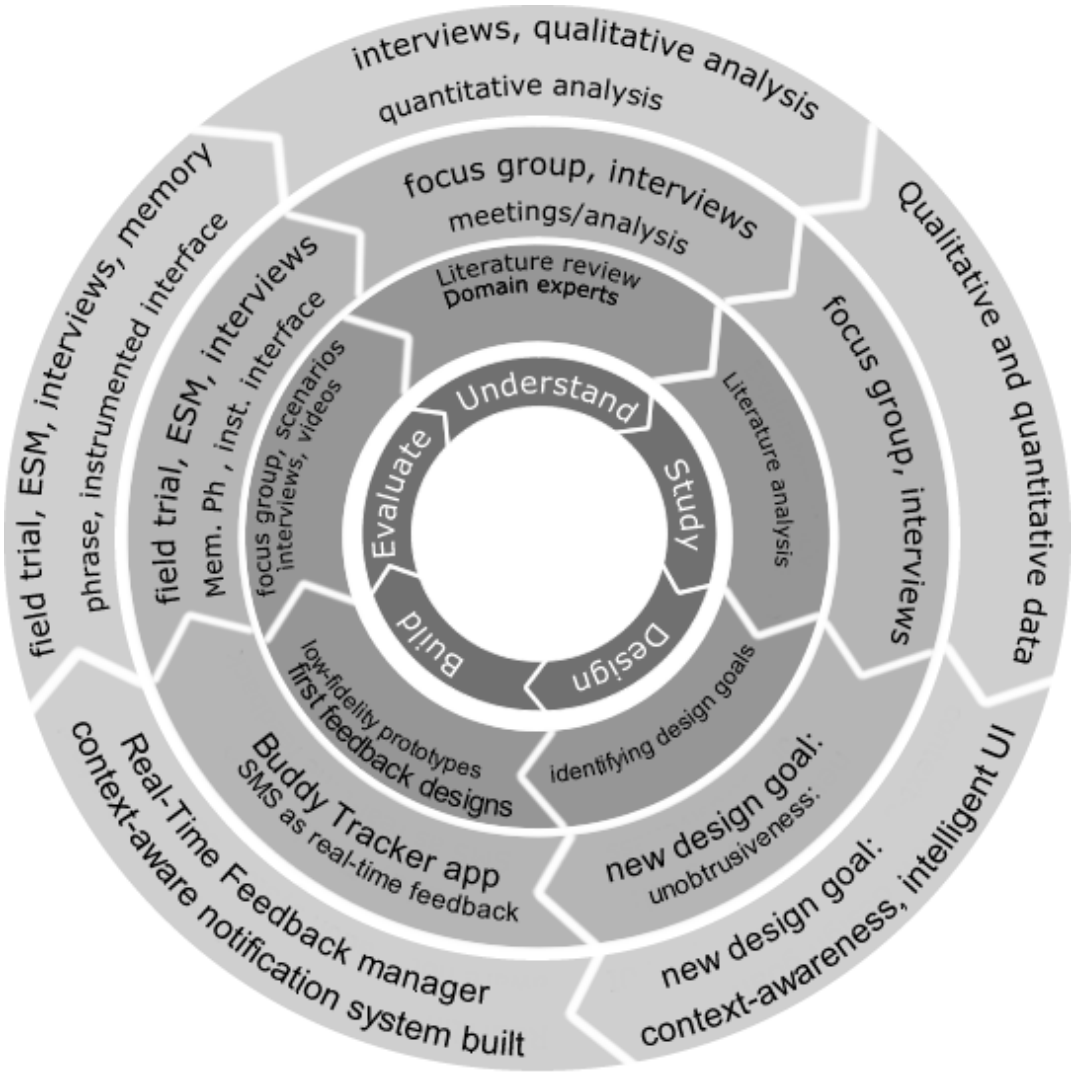


Figure 1-1. User-centred design methodology applied to our research on the real-time feedback. This diagram presents different phases of the user-centred design process and different methods and research activities undertaken during each phase. Different iterations are presented as new layers, starting from inner layer (early design phase) to the outer level (the final phase).

In terms of data analysis, our studies have taken both qualitative and quantitative approaches. During initial phases of our research we concentrated on understanding and studying users'

values and expectations therefore we have focused on qualitative research, while in the next phases we collected both quantitative data (through questionnaires, experience sampling method (ESM), and logging users' activities) and qualitative data (mainly through interviews).

1.3.2. Designing Privacy Shake

We applied a user-centred design methodology to the design process of Privacy-Shake, a novel control tool for managing privacy preferences. In our design process we went through one full iteration, and collected data required for redesign of the existing prototype. A design process is illustrated in the Figure 1-2 below.

Figure 1-2. User-centred design methodology applied to our research on the Privacy-Shake, a haptic control tool for privacy management. This diagram presents different phases of the user-centred design process and different methods and research activities undertaken during each phase. We completed only one full iteration.

Motivated by our exploratory study (see (Jedrzejczyk et al. 2009)), literature (Lederer et al. 2004) and preliminary results from the focus group discussion and interviews (see Chapter 4) we found the need for simple interface for managing basic privacy preferences in the context. Our design was largely motivated by observations of the non-computer mediated human-human interaction. We used common gestures (in Western countries) to influence the design of gestures language for privacy management, which was then implemented in the Android application.

In the evaluation phase we used both quantitative and qualitative data to evaluate the effectiveness and performance of the interface. Interviews and Likert-scale forms were used to understand users' expectations and social acceptance of the technology.

1.4. Author Statement

Some of the material presented in this thesis has been previously published in the following papers:

1. L. Jedrzejczyk, B.A. Price, A.K. Bandara, and B. Nuseibeh, *I Know What You Did Last Summer: risks of location data leakage in mobile and social computing*, Technical Report no 2009/11, Milton Keynes, UK: The Open University, 2009. Presented at Workshop on Security and Human Behaviour (SHB '10), 2010, Cambridge, UK
2. L. Jedrzejczyk, B.A. Price, A.K. Bandara, and B. Nuseibeh, *On the impact of real-time feedback on users' behaviour in mobile location-sharing applications*, Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10), ACM, 2010, pp. 1-12.
3. L. Jedrzejczyk, B.A. Price, A. Bandara, and B. Nuseibeh, *Privacy-shake: a haptic interface for managing privacy settings in mobile location sharing applications*, Proceedings of the 12th international conference on Human computer interaction with mobile devices and services (Mobile HCI '10), ACM, 2010, pp. 411-412.
4. L. Jedrzejczyk, C. Mancini, D. Corapi, B.A. Price, A.K. Bandara, and B. Nuseibeh, *Learning from Context: A Field Study of a Privacy Awareness System for Mobile Devices*, Technical Report no 2011/07, Milton Keynes, UK: The Open University, 2011.

This thesis also reproduces small parts the following material, which has been published as a result of author's collaboration with other researchers, but is not a sole work of the author:

5. Mancini, C., Y. Rogers, A. K Bandara, T. Coe, L. Jedrzejczyk, A. N Joinson, B. A Price, K. Thomas, and B. Nuseibeh. *Contravision: exploring users' reactions to futuristic technology*. Proceedings of the 28th international conference on Human factors in computing systems (CHI '10), 153-162. Atlanta, GA, USA: ACM, 2010.
6. Mancini, C., Y. Rogers, K. Thomas, A. N Joinson, B. A Price, A. K Bandara, L. Jedrzejczyk, and B. Nuseibeh. *In the Best Families: Tracking and Relationships*, Proceedings of the 30th international conference on Human factors in computing systems (CHI '11). Vancouver, BC, Canada: ACM, 2011.

All of the work presented in this thesis describes my original contributions, except otherwise stated and referenced. This work was undertaken as part of the PRiMMA project (Privacy Rights Management for Mobile Applications) funded by EPSRC (Grant # EP/F024037/1).

The protocol for the empirical research carried out in this dissertation and within the PRiMMA project involving human participants was approved by our institution's Human Research Ethics Committee with approval number 559.

1.5. Thesis Structure

This chapter has explained the research problem driving this research and formed the research question from the motivation, outlined key contributions of this thesis and discussed research approach.

Chapter 2 surveys related literature and defines the scope for privacy problems addressed in this thesis. We start by presenting privacy evolution from the technological perspective, then we discuss common privacy issues in ubicomp. We conclude with the presentation of existing privacy enhancing technologies. Shortcomings of these technologies are discussed.

Chapter 3 describes a privacy awareness system grounded on Altman's privacy regulation theory, Erickson's and Kellog's social translucence and Bellotti and Sellen's feedback and control. We present the architecture of our system and feedback characteristic. We also present multi-sensory interfaces for feedback and visual interfaces for control. Next, we motivate and describe current implementation of the system (Buddy Tracker - mobile location sharing application).

Chapter 4 presents results of our investigation into the efficacy of real-time feedback as a mechanism for incorporating features of social translucence in Buddy Tracker.

Chapter 5 describes a field-based study aimed at exploring the social implications of the technology presented in the Chapter 3. This chapter focuses on ways in which real-time feedback affects people's behaviour in order to identify the main criteria for acceptance of this technology.

Chapter 6 presents a modified version of the Buddy Tracker, which has been influenced by the findings from previous studies. We present and evaluate new version equipped with context-awareness feature, machine learning mechanism and several sensory dimensions for the real-time feedback. In this chapter we report on our experience from the development process and also discuss findings of the field study with 15 participants.

Chapter 7 presents and motivates our work on Privacy-Shake, a haptic interface for managing coarse privacy settings. It also reports on a lab-based evaluation of the interface with 16 participants.

Chapter 8 concludes with the contributions of the work presented in this thesis and presents future research agenda for the work on the real-time feedback and Privacy-Shake.

Chapter 2. Research Context and Related Work

> "*Books are the carriers of civilization. Without books, history is silent, literature dumb, science crippled, thought and speculation at a standstill.*"
>
> Barbara W Tuchman

In this chapter we define the scope for privacy issues addressed in this thesis and discuss the impact of early technological inventions on privacy research. This chapter also reviews the previous work on the topic of privacy in the field of Human Computer Interaction and Ubiquitous Computing. We conclude with the presentation of limitations of previous attempts at addressing privacy problems in HCI and highlight the gap in existing literature.

2.1. Defining Privacy Scope for This Thesis

According to Rotenberg and Laurant (Rotenberg and Laurant 2004) privacy can be divided in four groups: (1) *bodily privacy* (concerned with protection of people's physical spheres against any intrusive actions e.g. genetic tests), (2) *territorial privacy* (concerned with intrusions into work and public spaces, e.g. searches, video surveillance and ID checks), (3) *information privacy* (concerned with the collection and handling of personal data e.g. private photographs, credit card information or medical records), and (4) *privacy of communications* (concerned with the security and privacy of mail, telephones, e-mail, IM and other methods of communication).

Novel technologies have opened new ways for communication in which sharing personal information becomes a part of communication practice. In this thesis we are mainly concerned about information privacy and the risks of intentionally or unintentionally sharing data without realizing the future privacy implications.

The purpose of this section is to show how information privacy evolved in time, and how privacy theories met demands of the information society.

2.1.1. From "*the right to be let alone*" to Privacy Management

Over the years, technological inventions stimulated law makers and researchers to redefine privacy to meet the needs of society. One of the most profound examples of the technological impact on privacy was the proliferation of photography initiated by Kodak in 1888[2]. This created a new problem: anyone could take a picture of another person, which could be then used in printed magazines without their consent.

What sounds obvious nowadays, in the 19th century was a huge step towards the establishment of the tabloid press. This highlights the negative impact of technology on what Rotenberg and Laurant called *information privacy* (Rotenberg and Laurant 2004), and what current legislation calls *data protection*.

Unsolicited use of pictures prompted two lawyers, Samuel Warren and Louis Brandeis, to publish a law review article "The Right to Privacy" (Warren and Brandeis 1890). In the article, they highlighted the privacy problem that stems from the technological inventions and business methods ("*instantaneous photographs and newspaper enterprise"*), which negatively affected "*sacred precincts of private and domestic life*".

Warren and Brandeis popularized a new definition of privacy, in which privacy is characterized as the "*right to be let alone*". They argued that people should have full protection "*in person and in property*" and it is necessary from time to time to redefine such protection so it can meet new demands of society that are result of political, social and economical changes.

In 1967, Alan Westin described privacy as a dynamic process with a non-monotonic function (Westin 1967). He argues that during *this process* we control access to ourselves by others *so it* (privacy) *is sufficient for serving momentary needs and role requirements* (Margulis 2003). Westin's theory speaks of privacy as "*the claim of individuals, groups or organisations to determine for themselves when, how, and to what extent information about them is*

[2] "History of Kodak". http://www.kodak.com/global/en/corp/historyOfKodak/historyIntro.jhtml [Accessed June 9, 2011].

communicated to others. Viewed in terms of the relaltion of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve". According to his theory we meet our privacy needs by adjusting four different privacy states: (1) solitude, (2) intimacy, (3) anonymity and (4) reserve. Solitude refers to not being observed by others. Intimacy describes the need for individual or small group seclusion. Anonymity is being free from identification and any kind of public surveillance. Reserve refers to the desire for limited disclosure of private information to others.

When we look at Westin's privacy theory from the perspective of current technology we see that he introduced an *adjustment* element. In his definition privacy is no longer a static concept, but a process, in which we, as data owners, are taking part by *determining* who has access to what information about us. Westin's theory serves as an introduction to *privacy management*. Privacy management implies the employment of four privacy factors (Adams 2000), namely *what* (information), *who* (data requester), *how* (under what circumstances) and *when* that have been recognized in the literature as key determinants used in privacy decisions making (Adams 2000; Consolvo et al. 2005; Lederer, Dey, and Mankoff 2002; Moor 1997).

The literature shows the importance of other factors that have an impact on our privacy decisions such as time and sensitivity of information, which are part of the richer context (Adams 2000; Sadeh et al. 2009). Privacy factors, also called variables, can be divided into personal and situational factors (Pedersen 1999). Situational include social and physical variables. Social elements might entail the presence of others and personal characteristics of peers taking part in the social interaction. Physical factors might include location, barriers or distances.

Another influential privacy theory that tried to understand how people manage their privacy is Altman's *privacy regulation theory* (Altman 1975). According to Altman, privacy management

can be regarded as an ongoing process of regulating boundaries. Altman's theory speaks of ways in which people achieve optimum level of privacy, ideal state of social interaction. Altman identifies five properties of privacy. First, temporal *dynamic processes of interpersonal boundaries* help us regulate how open or closed we are in response to changes in our internal states and external conditions. Second, Altman differentiates *desired and actual levels of privacy*. Third, privacy is described as *non-monotonic* function with an optimal level of privacy. This Optimal level is achieved when desired level is equal to the actual level. Altman's theory explains that more privacy is not always better, and that a person adjusts their privacy level according to the actual internal state and external conditions, in that the person may engage in crowding when there is too little privacy (desired < actual level); or feel isolated if there is too much privacy (desired > actual level) (See Figure 2-1). Fourth, privacy is *bi-directional*, involving inputs from others and outputs to others. Fifth, privacy can be analysed at two levels: *individual's privacy* and *group's privacy*.

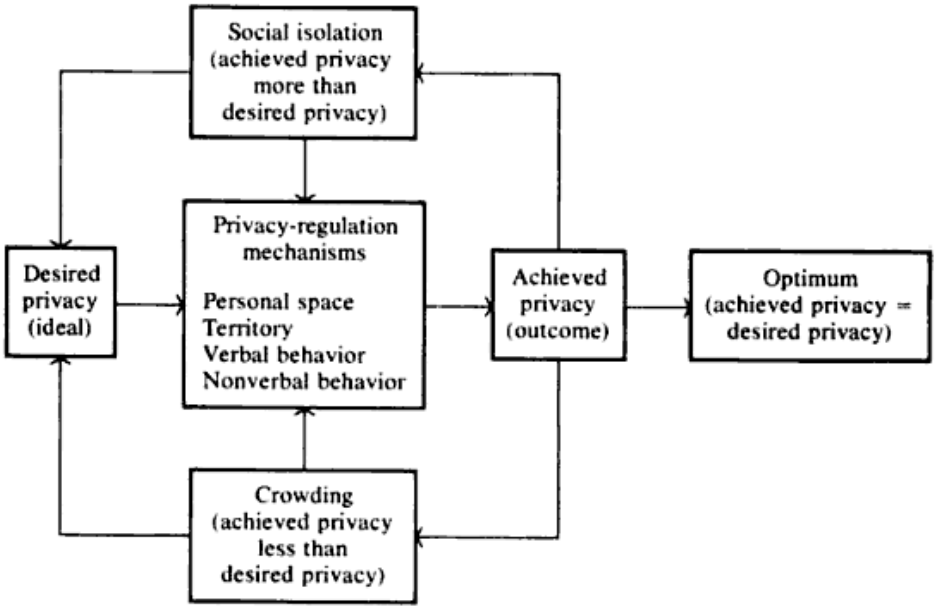


Figure 2-1. Overview of relations among privacy, personal space, territory, and crowding (Altman 1975).

The crucial idea of Altman's theory is that privacy is a central concept that provides a bridge between personal space, territory, and other realms of social behaviour. In this model, privacy is an interpersonal boundary regulation process by which a person or a group regulates interaction with others. Privacy regulation permits people to be open to others on some occasions and to be closed off from interaction at other times. Privacy is, therefore, a changing process whereby people attempt to regulate their openness/closedness to others (Altman 1975; Altman 1980; Margulis 2003).

Both Westin's and Altman's theories have much in common (Margulis 2003). Similarly to Westin, Altman sees privacy as a dynamic process of regulating access to ourselves by others to fulfil temporal needs and the actual role (e.g. individual or group member). They both agree that privacy is culturally universal and they share the non-monotonic view on privacy function: neither more privacy is good; nor less privacy is bad. What is more specific to Altman's theory is an environment that provides tools and mechanisms for regulating privacy (Margulis 2003). The environment can be regarded as physical structures (walls, position of physical items), systems, meaningful places, social actions, circumstances or events that determine our behaviour (Archea 1977; Kupritz 2000; Heft 2001; Irvin Altman 1975; Palen and Dourish 2003).

In this thesis we see the environment as an important element in the privacy management process because the cumulative effect of longitudinal accumulation of experience with an environment builds social awareness, a shared knowledge that helps us structure our interactions with one another (Erickson and Kellogg 2000). According to Dourish and Bellotti "*awareness is an understanding of the activities of others, which provides a context for your own activity*" (Dourish and Bellotti 1992).

Evidence from the literature shows that awareness is an important element of the privacy management process, because it conditions our social interaction (Erickson and Kellogg 2000), affects our privacy decisions, improves the understanding of the data flow within the system

(Nguyen and Mynatt 2002), impacts our comfort in sharing information (J. Y. Tsai et al. 2009) and can minimize potential privacy risks in the future (Adams 2000). Information from the environment is also used in privacy rule development, the process during which people "*develop new rules, learn preexisting privacy rules or negotiate rules that manage boundaries*" (Petronio 2002).

Awareness is also an element of the Altman's bi-directional function of privacy, which says that privacy regulation requires both *output* to others (communication) and *input* from others (i.e. noise, previous experience). Input in this context represents the information from the environment, which in consequence supports awareness.

More recently, Palen and Dourish (2003) recognized privacy as a dominant concern for the development of novel interactive technologies. They highlighted our weakness in ability to reason analytically about privacy in real world settings, which is a limitation for the acceptance of new technologies (Palen and Dourish 2003). They suggested new way for thinking about privacy in sociotechnical environments (i.e. Ubiquitous Computing systems), they perceive privacy as a practical matter. Based on Altman's theory (Altman 1975; Altman 1977) they proposed a new definition for privacy as a continuous negotiation and management process: "*Privacy is not about setting rules and enforcing them; rather it's the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres*". This definition says that privacy is dynamic and is not binary, which was also indicated in the previous literature, see (Adams 2000; Westin 1967; Jiang, Hong, and Landay 2002). For example there may be different levels of privacy depending on relation between data owner and inquirer, type of data and sensitivity of data, broadly saying: context.

Another scholar that sees the importance of context in relation to privacy is Helen Nissenbaum, she conceptualized privacy as *contextual integrity*, which is described as contextual compliance with norms of information appropriateness and distribution (Nissenbaum 2004). It has been suggested by Dourish and Anderson that technological impact on privacy not to be studied in

the isolation of the context, because privacy is not just a technical phenomenon. It is rather embedded into the social and cultural contexts of information practices (Dourish and Anderson 2006), which suggests how privacy should be studied in the HCI community.

2.1.2. Privacy Threats in Ubiquitous Computing

A hundred years after Kodak's invention, we stepped into the new era of computing, called Ubiquitous Computing (ubicomp) (Weiser 1991). Ubicomp technology became embedded into the fabric of our life and became part of its personal and professional aspects.

Undoubtedly, ubicomp technologies have a huge potential to improve our lives, work, wellbeing and safety. Several visionary examples present positive aspects of novel technologies portraying how individuals' lives can be enhanced and made easier [3, 4, 5 or 6]. In those examples, the technology cares for a user, the interaction between the user and the technology-enhanced environment is smooth, and problems-free (Vildjiounqite et al. 2008). The environment is unobtrusive, context-aware, intelligent and reacts to the user appropriately when and as needed.

Despite the positive aspects of ubicomp technology it is unclear how the users' information is treated, how it is stored and who has access to the information. As Mark Weiser notes, "*The problem, while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to what, where information is flowing, how it is being used, what is broken (as compared to what is working correctly, but not helpfully), and what are the consequences of any given action (including simply walking into a room).*" (Weiser 1991).

What is especially interesting in Weiser's quote is the notion of *future consequences*. Ubicomp technologies offer the potential of capturing and storing large datasets of users' behaviour,

[3] "Nokia future vision," http://www.youtube.com/watch?v=A4pDf7m2UPE, [Accessed June 9, 2011]
[4] "Microsoft Future Vision : Healthcare," http://www.youtube.com/watch?v=V35Kv6-ZNGA, [Accessed June 9, 2011]
[5] "Microsoft Sustainability : Productivity, future vision," http://www.youtube.com/watch?v=HvA9lA7_5FE, [Accessed June 9, 2011]
[6] "Apple Computer Knowledge Navigator," http://video.google.com/videoplay?docid=-514409492884268363 2, [Accessed June 9, 2011]

preferences, activities or movements. Ubicomp allows looking into the past, to check what we like, where we have been or what we did. Orwell's Big Brother has been brought to life, and there is no way back.

Enforcing the *right to be let alone* becomes very hard in the age of Ubiquitous Computing. Company owners can track their assets using GPS devices, parents can track their children via mobile phones, big supermarkets can monitor our purchases using loyalty cards and banks can find our location when we are using cash machines. CCTV[7], Google Maps Street View[8] and Webcam technologies allow us to access remote locations simply by observing those locations or objects and people inside. Technological advances in storage, aggregation, and extraction of information both online and offline raise several privacy concerns that have an impact on the acceptance of the new technologies (Iachello and Hong 2007; Palen and Dourish 2003).

Whilst, one reason for this problem is technological invention, we cannot blame the technology for all privacy problems in Ubiquitous Computing. According to Nguyen and Mynatt *the ubicomp system* is not limited to devices of different sizes connected through the wireless network. Ubicomp encompasses three environments, in which people live, work and interact with each other: technical, physical and social. A ubicomp system is an ecology of devices (technology layer) situated in the physical space (physical layer), in which people are connected (social layer).

Ubicomp technology is just a beginning of the new information society, in which the human and the technology co-exist. It changes our culture and the way we interact with information and other people. Technology opened new ways for communication, in which sharing personal information becomes a part of communication practice. The privacy risk we see here is sharing without realizing the consequences.

[7] http://en.wikipedia.org/wiki/Closed-circuit_television
[8] http://maps.google.com/help/maps/streetview/

2.1.3. Our Perspective on Privacy Management

Whilst privacy is a highly fluid concept (Jiang et al.2002), and its multidisciplinary nature makes its universal definition elusive, our goal here is not to redefine it. Rather we attempt to define what we understand by the process of *privacy management* in order to scope the practical problems of privacy investigated in this thesis:

i. we see privacy as a practical problem of regulating boundaries, namely privacy management;
ii. privacy management is an ongoing process of selective disclosure of the information in reaction to the environment (situation dependent);
iii. the process involves tools for expressing how our information should be communicated to others (control) and means for absorbing information from the environment (support for awareness).

2.2. Privacy Enhancing Technologies for Ubiquitous Computing

In this section we will look at technology from a privacy perspective in order to understand how privacy can be protected in the networked world and what privacy enhancing technologies exist that protect personal information from being misused. Our goal is to provide an overview of privacy research in the area of HCI and ubicomp in order to point out timely research problems driving ideas described in this thesis.

We start by discussing how privacy can be protected by technical means, such as access control, privacy policies, privacy-aware architectures or anonymization methods. We then survey design guidelines and show how guidelines influence the design of privacy sensitive systems. This is followed by the review of existing interfaces for managing privacy. Lastly we describe the role of awareness in the privacy management process and survey previous attempts to incorporate awareness in ubicomp systems. We conclude with a summary of different research approaches towards privacy protection in Ubiquitous Computing and frame our research within the context of wider privacy research.

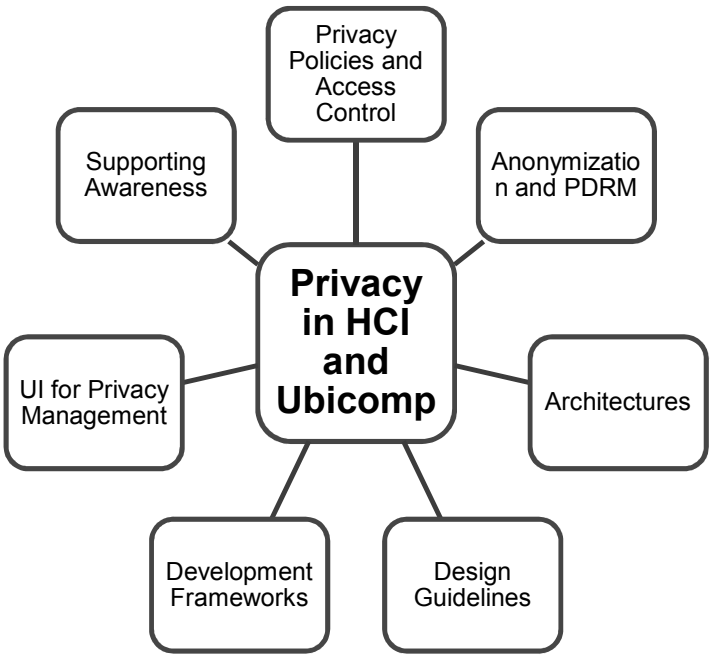


Figure 2-2. Privacy research in fields of Human Computer Interaction and Ubiquitous Computing.

Different directions of privacy research in fields of Human Computer Interaction and Ubiquitous Computing surveyed in this thesis are presented in the Figure 2-2. The diagram does not intend to cover all aspects of privacy related research interests in the field, but focuses on privacy protection strategies that (a) provide infrastructures for building privacy-aware systems and (b) support the design of privacy management tools and (c) help end-users understand and control her privacy settings.

2.2.1. Selective Disclosure: Privacy Policies and Access Control

One of the earliest work in the domain of privacy policies is P3P (Cranor et al. 2002), namely the Platform for Privacy Preferences agreed as a standard by W3C (the World Wide Web consortium). P3P is a specification for a user's privacy requirements based on user agents and privacy policies (expressed in APPEL – A P3P Preference Exchange Language). Users can define their own privacy policy and when accessing a P3P enabled website the user agent compares the user's preferences with the privacy policy of the visited website and informs the user about inconsistencies between policies. The P3P user agent has been implemented in the

Privacy Bird project (Cranor, Guduru, and Arjula 2006). The disadvantage of this technology is that P3P does not enforce a user's privacy policy but relies on the assumption that companies actually manipulate our data according to their published policies. Since 2002 P3P has been a W3C official standard for expressing privacy preferences in web applications, and the technology was adapted and advanced by others, see (Langheinrich 2002; Hong, Yuan, and Shen 2005; Myles, Friday, and Davies 2003). Example user interfaces for managing P3P privacy policies were proposed in (Hong, Yuan, and Shen 2005; Reeder et al. 2008).

One technology that fills the enforcement gap (i.e. the reliance on the website's privacy policy to reflect reality) in P3P, is EPAL (Enterprise Privacy Authorization Language) developed by IBM (Ashley et al. 2003). Although P3P is a specification dedicated for websites and a wide population of web-users, EPAL's purpose is to write enterprise privacy policies. One advantage of EPAL is that it not only allows specifying rules in privacy policy form, but also delivers a language that can be imported and enforced by privacy-enforcement systems. Ni points out (Ni et al. 2007) that EPAL's sequential semantics cause problems within the EPAL rules related to conflict detection between permission assignments. This problem was addressed in Privacy-Aware Role Based Access Control (P-RBAC), which is a family of access control systems, being extension for classic RBAC (Role Based Access Control).

Due to the complexity of privacy policies and access control systems, both authoring (Reeder, Bauer, et al. 2008) and understanding privacy policies is still a big challenge. Iachello and Hong (Iachello and Hong 2007) argue that the most significant project in the domain of privacy policy creation, management and enforcement is SPARCLE (Brodie et al. 2006). SPARCLE provides a grammar, which allows in-experienced users to specify privacy policies in natural language. The system does not require any interface, as it uses natural language processing methods to automatically parse human-readable privacy policy into machine-readable XML format. Although SPARCLE does not require any specific user interface for expressing privacy policy, which has been proved as an efficient way for defining organizational privacy policies (Karat et

al. 2006), there is no evidence in the literature proving SPARCLE as usable and efficient method for managing personal privacy.

Another problem related to privacy policies is related to their presentation and understanding. Several researchers study how to communicate current privacy policy, either of an organization or a website, to the user in an understandable manner. Recent work aiming at exploring this problem includes expandable grids (Reeder, Bauer, et al. 2008), privacy notices (Kelley et al. 2010) and textured agreements (Kay and Terry 2010).

2.2.2. Hiding Information: Anonymization and PDRM Methods

While both access control and privacy policies enable the user to express her privacy settings, the goal of anonymization tools and PDRM (Privacy Digital Rights Management) is to prevent others from accessing one's personal information or minimizing the accuracy of disclosed location according to the data owner's privacy policy.

"*The ability to prevent other parties from learning one's current or past location*" was the motivation for Beresford and Stajano (Beresford and Stajano 2003) to work on privacy-protecting framework based on frequently changing pseudonyms that avoids re-identification by the locations users visited. To protect location privacy, they used pseudonymization method that belongs to wider group of anonymization techniques proposed by (Pfitzmann and Köhntopp 2001):

- anonymity ("the state of being not identifiable within a set of subjects, the anonymity set"),
- unobservability ("state of IOIs (items of interest) being indistinguishable from any IOI at all"),
- unlinkability (says that two or more items within the system can not be related),
- pseudonymity ("use of pseudonyms as IDs").

Thus pseudonymization can hide the real identity of a person; his or her identity can often be inferred from the user's location - Beresford and Stajano presented how using simple heuristics can be useful in de-anonymizing pseudonyms, which comes to the conclusion that using anonymity as a single privacy protection cannot guarantee total privacy of location (Beresford and Stajano 2003).

Kulik and Duckham proposed a method for protecting location privacy using obfuscation (Duckham and Kulik 2006). Obfuscation is the process of decreasing the quality of information about one's location focused on providing optimal privacy level, it ensures that individuals release enough information to service provider. Another method that allows hiding location information from others is PDRM (Personal Digital Rights Management). PDRM treats location as a digital property and enables users to license their location information using an encryption key, which is necessary in order to read the data.

A Digital Rights Management (DRM) technique was used in pawS's module called *pawDB* (Langheinrich 2002) or *Confab's data tuple* (Hong 2005). PawS is a privacy awareness system for ubicomp environments that incorporates labelling protocols similar to P3P (see section 2.2.1) to express such things as type of data available about individuals or kinds of data recorded by the ubicomp environment. It allows data collectors both announce and implement data usage policies, as well as introduces mechanisms for data subjects for keeping track of their private information as it is stored and used (Langheinrich 2002). Confab's data tuple is a container that decribes individual pieces of contextual data. Tuples contain metadata such as data value, history and privacy tag that describes end-user's preferences (J. I. Hong 2005). Another architecture based on PDRM has been presented by (Gunter, May, and Stubblebine 2005). They use DRM concept as a foundation for specification and negotiation of privacy risks. Their prototype adLoc, has been evaluated in LBA (Location Based Advertising) domain. adLoc license is defined using combination of XrML (eXtensible rights Markup Language) and P3P.

It is worth saying that anonymization techniques and PDRM are not standalone solutions to privacy, as they do not address *the need for continuous sharing* (Hong and Landay 2004). Those solutions are mainly used to ensure the security of the information, blur the information accordingly to the data owner's privacy policy or ensure that private information is used in the right context (pawDB (Langheinrich 2002), Confab (Hong 2005)).

2.2.3. Controlling Data Flow: Privacy by Architecture

According to Spiekerman and Cranor (2009) the privacy by architecture approach focuses on minimizing the collection of personally identifiable information and emphasizing the anonymization and client-side data storage. The privacy by architecture approaches provide low degree of the network centricity and provide high protection against re-identification.

A symmetrical location service architecture was proposed by Rodden (Rodden et al. 2002). He suggests that rather than using a long-life pseudonym to share location, the system should incorporate a temporal and random pseudonym, which will be used to sign the disclosed data. This solution ensures the unlinkability between historical location information and the data owner as it is based on the temporal contract between the data owner and the service provider.

Another privacy aware architecture is pawS, (Langheinrich 2002). The system incorporates Fair Information Practices (described in section 2.2.4 below), and its fundamental principles are to *give people the ability to respect other's people privacy and rely on social norms and law enforcement to create a reasonable expectation that people will follow such rules*. pawS uses an advanced version of P3P that includes an extended data scheme (i.e. perception or location data support). This architecture addresses awareness, which is supported by *privacy assistant service*, an interface presenting current privacy contracts between the data owner and the system (Langheinrich 2005).

Brar and Kay proposed an architecture called SPE - Secure Persona Exchange (Brar and Kay 2004). Their work focuses on the limitation of data access and retention by storing users' data on the mobile device. Explicit consent from the user is required before SPE can be accessed by

ubiquitous services. Similarly to pawS and Rodden's architecture, SPE uses machine-readable policies in P3P.

In order to protect location privacy Hengartner proposed an architecture for Location Based Services (LBS) that incorporates secure location information encryption and a disclosure mechanism between the service provider, network provider and a customer. The advantage of the proposed architecture is that it protects the user against re-identification by service provider (Hengartner 2007). Another architecture addressing privacy problem in ubicomp is a privacy rights management system proposed by Fahrmair. His solution incorporates DRM techniques and a License Server entity with a third party element acting as the certification authority (Fahrmair, Sitou, and Spanfelner 2005).

A DRM type solution is also used in the Confab architecture (Hong 2005). Confab originally started out as a development framework for context-aware applications, it evolved to the comprehensive tool supporting the design and development of privacy-aware ubiquitous systems. Hong suggests that information should be encapsulated into *infospace*, a set of *data tuples* containing actual information (i.e. location, activity) and *metadata* describing the source of the information, expiry date or access conditions (described in privacy tag). Similarly to work presented in (J. Y. Tsai et al. 2009), Confab provides support for reciprocity, which enables designers to build interfaces controlling data flow.

2.2.4. Privacy by Design: Design Guidelines and Frameworks

According to Ann Cavoukian *Privacy by Design (PbD) refers to the philosophy of embedding privacy into the design specifications of various technologies* (Cavoukian 2009). Several design frameworks and methods support privacy by providing design guidelines aimed at embedding privacy into system requirements.

The earliest and the most influential framework addressing privacy issues in the system design are the Fair Information Practices (FIPs) initially based on the OECD guidelines (see section 2.3). Initially, FIPs were developed specifically to support the design of large databases of

personal information, such as health records and financial records. Over time, FIPs have been adapted in several data protection laws. It is the only framework that has been used extensively in legislation (e.g.EU data protection directive and UK Data Protection Act (1998)) and privacy-aware systems design (P3P, pawS, SPE).

Fair Information Practices described in "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" include [9]:

1. Collection Limitation. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. Data quality principle. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. Purpose specification. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use limitation principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3, except:
    a. with the consent of the data subject; or
    b. by the authority of law.
5. Security safeguards principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available

[9] Reprinted from http://www.privacyrights.org/ar/fairinfo.htm#2

of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.

7. Individual participation principle. An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him
        i. within a reasonable time;
        ii. at a charge, if any, that is not excessive;
        iii. in a reasonable manner; and
        iv. in a form that is readily intelligible to him
    c. to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    d. to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.
8. Accountability principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

While FIPs are more general principles, specific design guidelines and design frameworks were proposed to guide the development of privacy-aware applications. The GSMA (Groupe Special Mobile Association), representing over 800 mobile operators worldwide, has published a set of design guidelines for mobile applications and service providers[10]. Informed by commonly accepted privacy principles set out in international instruments, privacy guidelines and data protection, they describe high-level privacy principles for applications and services that may impact users' privacy. Privacy principles proposed by GSMA are: openness, transparency and notice; purpose and use; user choice and control; data minimisations and retention; respect user rights; security; education; children and adolescents; and accountability and enforcement. The key objective of GSMA's principles is to *foster business practices and standards that deliver*

[10] "Mobile and Privacy" http://www.gsma.com/mobile-and-privacy/, [Accessed April 23, 2012]

meaningful transparency, notice, choice and control for users, respecting their private information.

Experience gathered during the evaluation of the RAVE system developed at EuroParc motivated Bellotti and Sellen to publish the Question-Options-Criteria framework for addressing privacy in media spaces (Bellotti and Sellen 1993). In order to support evaluation of alternative design options for privacy-aware systems they proposed a framework based on a set of four questions about control and feedback over information capture, construction, accessibility and purpose (Figure 2-3). The framework can be extended using a set of eleven criteria representing additional concerns, which help designers to assess and distinguish potential design solutions for feedback and control: trustworthiness, appropriate timing, perceptibility, unobtrusiveness, minimal intrusiveness, fail-safety, flexibility, low effort, meaningfulness, learnability and low cost.

Though Bellotti and Sellen's framework has been recognized as a real improvement over the high level FIPs guidelines, there is no evidence in the literature of their widespread use. Jensen criticized this framework because it does not take into account iterative nature of design process and it means that the framework cannot be a part of iterative design process, but is *more likely to be employed once, at the end of design cycle* (Jensen et al. 2005). Using this framework might be expensive in case of any change, because it requires re-evaluation of the whole system. Jensen proposed another design framework that aids designers of privacy-aware systems, called STRAP (a structured analysis framework for privacy). STRAP is a light-weight method that incorporates techniques adapted from the requirements engineering literature for the structured analysis of privacy vulnerabilities in design and the iterative adaptation of preferences (Jensen et al. 2005).

Jensen's evaluation of STRAP and Bellotti & Sellen framework showed that STRAP requires less time (though no significant difference reported) and resulted in more privacy-aware vulnerabilities discovered. The Bellotti & Sellen framework however is not intended to cover

privacy-aware design in general, as its main goal was to support the development of systems aiming at protecting privacy by providing feedback and control. Therefore, the Bellotti and Sellen framework is more appropriate to interface design, as it addresses additional goals guiding the design process.

	Feedback About	**Control Over**
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Figure 2-3. A framework for designing for feedback and control in ubiquitous computing environments: Each cell contains a description of the ideal state of affairs with respect to feedback or control of each of four types of behaviour (Bellotti and Sellen 1993).

Another design approach adapted by the HCI community is social translucence (Erickson and Kellogg 2000). The social translucence framework supports the design of communication and collaboration systems for large groups of people working in networked environments. The main principle of this framework is to *enable people to draw upon their social experience and expertise to structure their interactions by making things visible to one another*. Although it was originally developed for supporting computer supported collaborative work, we see a similarity

between this framework and Altman's bi-directional function of privacy (see section 2.1.1). Similarly to Altman, social translucence emphasizes visibility (in Altman's terminology - input) as an important element for achieving coherent communication. In Altman, input from the environment, is one of the elements that help us achieve the optimal level of privacy.

The combination of social translucence, Bellotti's and Sellen's framework and findings from environmental psychology (Kaplan and Kaplan 1982) resulted in the Privacy Mirrors framework (Nguyen and Mynatt 2002). This framework is concerned with addressing an oft-cited anti-privacy feature of ubicomp – *invisibility* (Weiser, Gold, and Brown 2010). Nguyen and Mynatt propose five characteristics that help the user engage in the sociotechnical environments: *history* and *feedback* for *awareness* and *accountability* that results in better understanding of the system, which help the user make an informed *change* to their privacy settings. Although the framework was used to critique an early prototype of the web server log mirror, there is no evidence in the literature that confirms the impact of awareness and accountability on change and users' understanding of the system.

A Principle of Minimum Asymmetry was proposed to help better understand interactions between the various stakeholders within the system (Jiang, Hong, and Landay 2002). Jiang argues the role of technical approaches to privacy problems is to *minimize the asymmetry of information flow between the data owners and data collectors and data users, by decreasing the flow of information from data owners to data collectors and users, and increasing the flow of information from data collectors and users back to data owners*. He also proposed a design space (Approximate Information Flow - AIF) that helps categorize privacy features by contrasting data lifecycle (described as collection, access and second use) with themes for minimizing asymmetry (prevention, avoidance and detection). Although AIF was shown to be useful as an analytical tool to measure the level of privacy protection, it has not been used widely as a design model (Iachello et al. 2005).

Lederer proposed a specific set of five design suggestions described in the form of pitfalls (Lederer et al. 2004): (1) obscuring potential information flow, (2) obscuring actual information flow, (3) emphasizing configuration over action, (4) lacking coarse-grained control and (5) inhibiting existing practice.

Lederer indicates that "*avoiding any of the pitfalls does not ensure success, but ignoring one can potentially lead to disaster*". The above pitfalls do not intend to be guidelines for privacy aware systems design, but systems which ignore any of the pitfalls will inhibit the user's abilities to manage their privacy. Another framework for facilitating the development of privacy-aware ubicomp systems is Confab (Hong and Landay 2004). Confab is a development toolkit providing a framework as well as customizable privacy mechanism, including an extension for managing location privacy. Confab is based on a set of end-user and developer requirements, which have been identified as success metrics for privacy-aware systems.

Drawing from his experience on the development and real-world evaluation of Reno, Iachello suggested specific design guidelines for incorporating privacy into location sharing applications (Iachello et al. 2005). His guidelines describe how users' location should be handled, but also specify control features users should equipped with in order to manage the disclosure of location information effectively. Iachello also considers very specific aspects of human-human interaction, such as use of the deception. The role of deception in balancing privacy needs in the context of location sharing mobile applications was researched extensively by Adam. In his PhD thesis (Adam 2009) he proposed a Deception-Based Privacy Control model providing an additional layer of flexibility, in which social practices, such as presenting obfuscated or untrue information, can be implemented into location sharing applications.

Patrick and Kenny developed Privacy Interface Analysis (Patrick and Kenny 2003), where they describe a set of privacy principles derived from the European Privacy directive in the form of HCI requirements. The Privacy Interface Analysis method requires that functionality of the application is specified in UML and then thoroughly analyzed against four privacy principles,

namely *transparency*, *finality & purpose limitation*, *legitimate processing* and *rights*. This method guides not only the design of the data flow, but also helps designers understand potential interface design solutions.

Although the Privacy Interface Analysis method provides support for legislative compliance checking, it has been criticized for its complexity and lack of support for fairness, which was introduced in the Proportionality Method (Iachello and Abowd 2008). The Proportionality Method (PM) advocates the balance between the benefits of data collection and stakeholder's interest in controlling the collection and dissemination of the information. It is a lightweight design that borrows from data protection authorities (DPA) – *supervisory entities with regulatory and enforcement powers on data protection matters* (Iachello and Abowd 2005). PM encompasses three evaluation steps *that DPAs and courts use in the evaluation of the technology: desirability, appropriateness and adequacy*. PM requires that designers consider privacy tradeoffs in order to ensure that the privacy burden is acceptable to all stakeholders (*desirability*); next step involves technical knowledge, as the designers need to propose a technology (*appropriateness*); and lastly designers must ensure the chosen technology and its features (those affecting stakeholder's privacy) are necessary (*adequacy*). What is especially novel in this method is that it does not frame the design process on the predefined list of principles, but focuses on collaboration and stimulates creativity, which is useful in designing privacy features for novel concepts (Fallman 2003; Iachello et al. 2005).

2.2.5. Privacy Control: Interfaces for Managing Privacy

At the core of privacy problems investigated in this thesis, lies privacy regulation. The term privacy regulation is borrowed from Altman (Altman 1975) and describes a continual process of regulating boundaries between the data owner and the environment. Privacy regulation in that context can be regarded as "*a selective control of access to the self or to one's group*" (Altman 1975). In the HCI literature this is often called privacy management, and is described as the process in which the user instructs the system how his personal information should be disclosed or disseminated. Bellotti and Sellen also use term control to refer to privacy management; they

define control as "*empowering people to stipulate what information they project and who can get hold of it*" (Bellotti and Sellen 1993).

While *privacy regulation* and *privacy management* are just different names to describe the process of managing the dissemination of personal information, we use the term *privacy control* to describe a group of tools (e.g. user interfaces) by which users instruct the system how their information should be disseminated. Recall that in section 2.1.3 we said that privacy management involves tools for expressing how our information should be communicated to others (privacy controls) and the means for absorbing information from the environment (support for awareness). The latter are described in the next section.

According to Altman's theory (see section 2.1.1) at the heart of privacy regulation is an environment that provides tools and mechanisms for managing privacy. Computer systems are part of the environment and provide tools (user interfaces) for controlling the dissemination of personal information. In this section we present several design approaches towards usable privacy management interfaces informed by theoretical frameworks (Lederer et al. 2004), previous privacy studies in ubicomp (Adams 2000; Consolvo et al. 2005) and an underlying privacy policy (Cranor et al. 2002).

We survey the existing work on user interfaces for managing privacy using Hong's and Iachello's classification for privacy management models which distinguished three groups of interfaces *pessimistic*, *optimistic* and *interactive* (Iachello and Hong 2007).

In the pessimistic model the user is required to define his privacy preferences prior to using the system to prevent privacy violations. This model guarantees a high level of anonymity but limits social interaction. This model can be found in systems with strong focus on information security, e.g. SPARCLE (Brodie et al. 2006) or Expandable Grids (Reeder, Bauer, et al. 2008) .

Lederer and Hong (Lederer et al. 2004) proposed the *faces* interface for managing the disclosure of personal information in ubiquitous computing, informed by Goffman's identity management

theory (Goffman 1978). In their approach the user could set up faces, which encapsulated different privacy preferences that could be easily adapted according to the context (Lederer et al. 2004). This solution is similar to Brar's Secure Persona Exchange, in which user can reveal different persona in reaction to the service request (Brar and Kay 2004). Another interface for managing complex privacy rules was proposed by Hong et al. (Hong, Yuan, and Shen 2005) who designed the User Preference Manager interface based on a pessimistic approach with the underlying P3P privacy policy engine (see section 2.4.1. for more details).

In the optimistic approach, the system helps the user trace potential misuses and supports the user in reacting to potential violations by specifying additional access rules. Optimistic interaction borrows from *social translucence* (Erickson and Kellogg 2000) and is based on reciprocal interaction, in which stakeholders are aware of each other actions. Examples using this approach include work that of (J. Y. Tsai et al. 2009; Raento and Oulasvirta 2005; Mancini et al. 2011; Jedrzejczyk et al. 2010a; Nguyen and Mynatt 2001).

The objective of the interactive model is to provide information that helps the user make informed decisions about sharing information. Another important aspect of this privacy management model is that the user communicates privacy preferences in reaction to the information request. While this model supports continuous privacy management and understanding of the information flow, data owners are interrupted each time someone requests their information. Due to the human tendency to automatic behaviour, user confirmation is often executed subconsciously and is not really trustworthy (Raskin 2000).

Evidence from the literature also shows that too many *consent clicks* (Iachello and Hong 2007) leads people to ignoring consent requests without reading them (Pettersson et al. 2005). Solutions using this approach were adapted by (Iachello et al. 2005) in the Reno system; (Patrick and Kenny 2003), they used *Just-In-Time Click-Through Agreement* (JITCTA). Other examples of interactive privacy interfaces include Hong's access notification interface (Hong

2005, Figure 5-9) and the privacy warning and security alert interface presented in (Jedrzejczyk et al. 2010b).

Several hybrid approaches to privacy management have been proposed, in which pessimistic, optimistic and interactive models were implemented into one system. For example, additional options for privacy management can be found in Lederer and Hong's (2004) work that extends the pessimistic approach used in the faces interface. Here, the access notification interface supports continuous privacy management by providing timely information about location requests, which supports users' awareness and understanding the extent to which the personal information is disclosed in the system. A place bar widget allows the user to control the disclosure and granularity of location with a web page as part of the browsing activity (Hong et al. 2003; Hong 2005, Figure 5-11). The Nexus Personal Information Manager provides a disclosure log with a simple option to manage the disclosure of location information between (1) the data owner and services; and (2) between the data owner and other users (Hong 2005, Figure 5-10). A combination of these interfaces creates a new hybrid approach, in which pessimistic, optimistic and interactive approaches are mixed together.

Tsai et al. combined the pessimistic and optimistic approach in their Locyoution system where users could create privacy rules using a web-based system, and refine rules by analysing the disclosure log (J. Y. Tsai et al. 2009). A similar approach was used in the Friend Finder application described in (Sadeh et al. 2009), further advanced by (Toch et al. 2010) in the Locaccino system for location sharing.

2.2.6. Supporting Awareness: Introducing Feedback

In section 2.1.3 we said that the privacy management process involves tools for expressing how one's information should be communicated to others (several approaches describing control mechanisms are described in the section 2.2.5) and tools for supporting awareness. Awareness in this context relates to the user's understanding of the sociotechnical system and its capabilities (the sociotechnical nature of ubicomp is explained in the section 2.1.2).

According to Dourish and Bellotti (1992) *awareness is an understanding of the activities of others, which provides a context for your own activity.* Nguyen and Mynatt argue that *lack of awareness and control is not simply a privacy issue, characterized as 'Do the wrong people know things about me?', but it strikes fundamental issues in people understanding the capabilities of a system, and then being able to shape that system to meet their particular needs.* They conclude that *shaping the system is impossible without the understanding of the system* (Nguyen and Mynatt 2002; Nguyen and Mynatt 2001). This conforms to Altman's findings that privacy regulation requires both *output* and *input* from the environment, in our case, a ubicomp system.

The conclusion here is that the user of a ubicomp system requires methods and interfaces that help her not only *shape* the system (control the dissemination of personal information) but also *understand* how it affects the social interaction (by collecting feedback from the system).

While awareness has assigned a more social meaning in the HCI literature (Dourish and Bellotti 1992), we use term *feedback* to describe technical aspects of awareness in ubicomp. We borrowed this term from Bellotti's and Sellen's work on media spaces that define feedback as "*informing people when and what information about them is being captured and to whom the information is being available*" (Bellotti and Sellen 1993). Feedback can be regarded as an information unit describing the data flow and stakeholders accessing the information in a ubicomp system.

HCI researchers consider feedback as an important privacy feature for context-aware applications, which has been discussed extensively in prior work (J. Y. Tsai et al. 2009; Bellotti and Sellen 1993; Raento and Oulasvirta 2005; Hsieh et al. 2007). Feedback has been recognized as an important factor allaying users' privacy concerns and increasing comfort of sharing location (J. Y. Tsai et al. 2009). Research has also shown that feedback can affect users' behaviour, improves the understanding of the data flow within the system (Nguyen and Mynatt 2002) and can minimize potential privacy risks in the future (Adams 2000).

Beyond examining the social consequences of using feedback, a number of researchers have proposed design solutions for representing feedback for different contexts and activities. Bellotti and Sellen (1993) studied the use of feedback to show users of the RAVE environment that they were being recorded. They found that feedback in the form of an LED light is a good communication tool but that displaying the full information about people watching is too intrusive. A similar approach for providing feedback was proposed by Neustaedter and Greenberg, but they added sound to LED feedback (Neustaedter and Greenberg 2003).

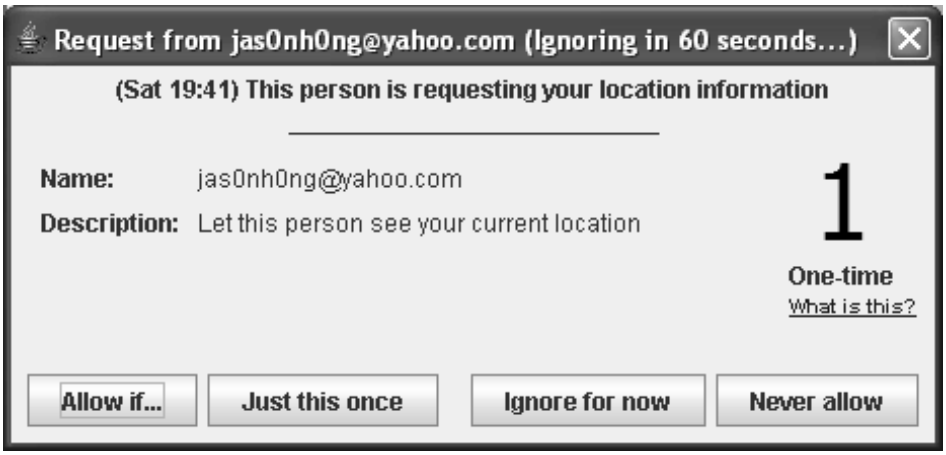


Figure 2-4. Access notification interface presenting just-in-time description of who is requesting information and why (Hong 2005).

To provide a real-time descriptions of who is requesting information and why, Hong proposed the concept of *access notifications* represented as a dialog window with additional controls for accepting, denying or ignoring the request. Access notifications support plausible deniability for the trackee and also act as a privacy management tool (Figure 2-4). The shortcoming of access notification is that people tend to ignore consent requests without reading them (Pettersson et al. 2005).

Sellen et al. proposed a novel design for a situated device, The Whereabouts Clock, presenting real-time information of "what the group is up to" based on a fictional device described in J.K.

Rowling's Harry Potter books (Sellen et al. 2006). While this tool was used to improve family awareness, it could be adapted to present information about "what the group knows about me".

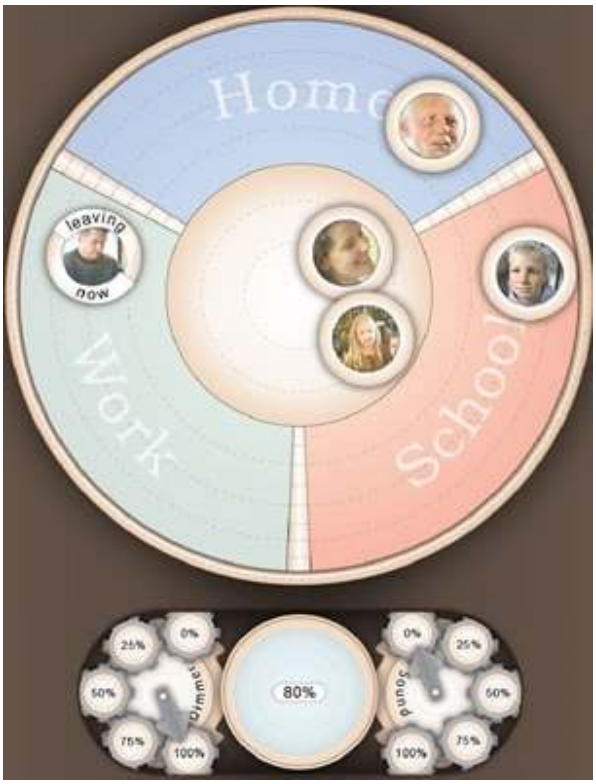


Figure 2-5. The Whereabouts Clock interface (Sellen et al. 2006).

Another attempt to provide feedback about location requests was presented by Sadeh et al. (2009). They proposed a design for both real-time and aggregated feedback mechanisms. The first was a bubble notification (as used in the Windows Operating Systems). The bubble (Figure 2-6) was found as a minimally disruptive method for supporting awareness, which is one of the goals of our research. Sadeh et al. do not report on the effectiveness of bubble interface in delivering feedback information in the real-time. The second was a location request history list, showing who had access to what information and when (Figure 2-7).

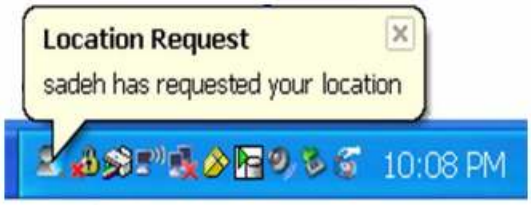


Figure 2-6. Real-time feedback in the form of bubble, notifying users of incoming queries help maintain awareness while being minimally disruptive (Sadeh et al. 2009).

Figure 2-7. Historical (aggregated) feedback tool helps users understand how their privacy policies work and enables them to more effectively refine their policies (Sadeh et al. 2009).

A similar interface was presented by Lederer et al. (2004) who also designed an interface for a disclosure log to help people understand their privacy policies. A shortcoming of the latter design is that it does not provide a mechanism for making suggestions and refining privacy preferences ad-hoc. A similar interface for a disclosure log was proposed in (J. Y. Tsai et al. 2009), interface is presented in Figure 3-3. They continued the work of Sadeh (2009), and combined historical feedback with the control mechanism.

Since most of the work in the awareness interfaces design area has been focused on the design aspects, Tsai has expanded the work in the area and investigated the social aspects of feedback and its importance at supporting privacy. They conducted *in the wild* (Rogers 2011) study aimed

at examining the impact of feedback for sharing location within the social groups. Tsai et al. found that feedback is a very important design feature supporting user's acceptance of location-sharing technologies and improving the comfort of sharing location. They also highlighted the positive correlation between the feedback availability and openness. Tsai's study provided new insights about the importance of feedback for managing personal privacy in ubiquitous computing system. However, their efforts have focused on feedback's utility from the data owner's perspective, not extended field explorations of the data requester behaviour. The latter is explored in this thesis.

Hsieh et al. provided a set of different feedback designs for push and pull based interaction in the area of instant messaging systems (Hsieh et al. 2007). They also provided some insights about unobtrusive interaction design for real-time feedback. Ackerman and Cranor proposed the privacy critics concept to support awareness and warn web users about potential privacy risks of sharing personal information with a particular website (Ackerman and Cranor 1999). While the concept of a semi-autonomous agent offering privacy warnings and suggestions to Internet users could support users' awareness, the proposed design was very intrusive. A more efficient design solution aiming at solving a similar problem was later proposed in (Cranor, Guduru, and Arjula 2006).

A relatively small number of researchers discuss the concept of historical feedback in the form of disclosure logs for location information on mobile devices (Raento and Oulasvirta 2005; Lederer 2003). Raento and Oulasirta's interface provides both coarse-grained location request information, and fine-grained view available on demand (Raento and Oulasvirta 2005). Another attempt to provide feedback in the context of mobile devices is Locaccino, which provides an on-demand list of most recent location requesters (Toch et al. 2010). Marmasse proposed a real-time feedback as "*thinking of you*" information. In her Watch Me system (Marmasse 2004), a data requester picture was displayed on the screen to provide timely information about who is requesting one's information.

A number of design considerations for real-time feedback were proposed for large screen devices (Hong 2005; Sadeh et al. 2009; Hsieh et al. 2007). Although mobile devices have been considered *the most widely used ubiquitous computing technology* (Barkhuus and Dey 2003) for quite a while, little work has been done on the real-time feedback in mobile context. These are clearly very different from traditional, large screen computers due to the diversity of their context of use, relation with the owner and their ubiquitous nature.

The work described so far has strongly focused on visual feedback, which might not be appropriate in a mobile context. For example, vibro-tactile and auditory feedback has been used successfully in other domains such as mobile search (Robinson, Eslambolchilar, and Jones 2009), navigation (Holland, Morse, and Gedenryd 2002) or supporting visually impaired people in reading graphs activities (Wall and Brewster 2006).

2.2.7. Summary of Research Approaches for Privacy Protection in Ubicomp

As a conclusion for this section, we will use the description of privacy management presented in section 2.1.3 and review the existing work on privacy in ubicomp by looking at how a particular privacy protection strategy addresses the principles of privacy management. The goal of this summary is to identify gaps in the privacy literature by providing answers to the following questions:

i. How does a particular technology address privacy management?
ii. Does the technology support bi-direction by providing feedback from the environment?
iii. What interfaces are provided to support privacy management?
iv. How does the technology support/influence interface design?
v. How does the technology support awareness?
vi. Since mobile devices are the most common ubicomp technology, how does the particular privacy protection strategy consider the mobility aspect of use?

The results of this analysis are presented in the Table 1.

Table 1. The summary of strategies for protecting privacy in Ubiquitous Computing. A "□" in a cell means that particular work addresses a particular aspect of privacy.

Solution \ Strategy	Privacy policies and access control	Architectures	Anonymization and PDRM methods	Design framework, design guidelines	Support for control	Support for eedback	Proposal of the user interface for control	Proposal of the user interface for feedback	Domain
Bellotti & Sellen, 1993		□		□	□	□		□	Media Spaces
Early version of P3P, 1997/1998	□				□	□			Web
Whitten & Tygar, 1999					□		□	□	PGP, email security
Ackerman & Cranor, 1999 (privacy critics)					□	□	□	□	Web
Jendricke & Markotten, 2000 (iManager)	□				□		□		Identity Management, Web
Langheinrich, 2001			□	□		□			Ubicomp
Ackerman, 2001					□	□	□	□	Web
Jiang, 2002 (AIF)				□	□				Ubicomp
Rodden et al., 2002	□	□							LBS
Nguyen & Mynatt, 2002 (Privacy Mirrors)		□		□	□	□		□	Ubicomp
Langheinrich, 2002	□	□		□	□	□			Ubicomp
Lederer et al., 2003									Ubicomp
Ginger et al., 2003	□	□			□	□			LBS
Beresford & Stajano, 2003			□						LBS
Patrick & Kenny, 2003				□	□	□	□	□	Web
Hong et al., 2004 (Confab)	□	□	□	□	□	□	□	□	Ubicomp
Lederer et al., 2004 (5 pitfalls)				□	□	□			Ubicomp
Marmasse, 2004 (WatchMe)						□		□	Ubicomp
Smith et al., 2005 (Reno)				□					LBS

Solution \ Strategy	Privacy policies and access control	Architectures	Anonymization and PDRM methods	Design framework, design guidelines	Support for control	Support for eedback	Proposal of the user interface for control	Proposal of the user interface for feedback	Domain
Raento et al., 2005					□	□		□	Ubicomp, social awareness
Brar & Key, 2005 (SPE)	□	□			□		□		Ubicomp
Hong et al., 2005 (UI for P3P)	□				□		□		Ubicomp
Sellen et al., 2006 (Whereabouts Clock)						□		□	Ubicomp
Cranor et al., 2006	□				□	□	□	□	Web
Brodie et al., 2006 (SPARCLE)	□				□		□		Policy authoring, usability
Hsieh et al., 2007 (ImBuddy)							□	□	IM
Sadeh et al., 2007	□				□	□	□	□	LBS
Hengartner, 2007		□							LBS
Reeder, 2008 (expandable grid)	□				□		□		Policy authoring, usability
Tsai, 2009	□				□	□	□	□	LBS
Toch et al., 2010 (Locaccino)	□				□	□	□	□	LBS

In the above table we compare different strategies towards protecting privacy in ubicomp. We focus on practical aspects of privacy and feedback and control features that indicate bi-directional function of privacy in the technology. Our analysis identifies the following areas that need more attention:

i. Insufficient support for traditional (non-digital) behaviour and lack of support for social norms does not enable end-users to draw upon their real-world (non-digitally mediated)

experience to structure interactions with others in digital systems. Therefore novel interactions are needed that will support participation in socio-technical systems and allow social norms to be upheld. A question of how to build a new informational society, in which behaviours in the face-to-face word and digital system are consistent, is still unexplored.

ii. Lack of usable interfaces that help end-users understand the system which inhibit adoption. Although several attempts have been made to support awareness in the digital systems, usable awareness interfaces design remains a big challenge. Previous work does not address an important issue for awareness interfaces: how to deliver timely information in the meaningful manner in order to help users understand the extent to which the (invisible) system manipulates information.

iii. Inadequate and non-effective feedback which result in lack of awareness. With few exceptions, most of the awareness interfaces focus only on historical aspects of feedback, and there is no evidence in the literature that end-users actually use the historical feedback feature. Consequently, there is lack of evidence that historical feedback has an impact on users' behaviour, apart from improving the comfort of sharing location information.

iv. There is an over-emphasis on visual representations for feedback. Although novel ubicomp devices support several ways of human-computer-interaction, current solutions are mainly focused on the visual feedback, which is not appropriate in the dynamic environments of ubicomp.

v. Mobility aspects of ubicomp are overlooked. Since mobile devices have been recognized as the most ubiquitous device nowadays, mobile interaction design for supporting awareness is still lagging. Most feedback solutions are focused on large screen devices and do not address the mobility aspects of use and different sensory dimensions of delivering the information.

2.3. Chapter Summary

In this chapter we defined the scope of privacy problems in ubicomp, which are discussed in this thesis. We then presented several technologies for protecting privacy in ubicomp, such as access control, privacy policies, privacy-aware architectures or anonymization methods. Next we surveyed design guidelines and showed how guidelines influence the design of privacy sensitive systems. We also reviewed existing interfaces for managing privacy.

Finally we described the role of awareness in the privacy management process and surveyed previous attempts to incorporate awareness in ubicomp systems. We concluded with a summary of different research approaches towards privacy protection in Ubiquitous Computing and presented several gaps in the literature to frame the research interests presented in this thesis.

In the next chapter we present our approach for implementing awareness into daily practice of ubicomp users. Drawing from theoretical frameworks and the shortcomings of existing privacy awareness solutions, we propose design criteria for awareness system supporting privacy management. An example implementation based on our approach is also presented.

Chapter 3. Designing for Privacy Awareness

> "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.*"
>
> Mark Weiser

In the previous section we presented numerous approaches towards supporting awareness in ubicomp. We concluded with a list of gaps in existing literature on privacy management. In this chapter we describe our approach for implementing awareness into daily practice of ubicomp systems users. We start by describing the theoretical foundations of our approach. We then enumerate design criteria for privacy management system supporting awareness. Next, we present a framework for classifying feedback in ubicomp applications and describe three feedback dimensions: sensory, interaction and time. We continue by presenting specific mobile interfaces for feedback and conclude with a description of Buddy Tracker, a mobile location-sharing application incorporating the design criteria for privacy awareness system supporting ongoing privacy management.

3.1. Theoretical Foundations

Our work is influenced by numerous researchers, but the most influential work that we draw on include:

- Altman's privacy regulation theory and the property of bi-directionality (Altman 1975; Altman 1977),
- Bellotti's and Sellen's framework for feedback and control (Bellotti and Sellen 1993),
- Erickson's and Kellog's social translucence (Erickson and Kellogg 2000).

In the spirit of Altman's theory our approach emphasizes the importance of the environment in the privacy management process; we also highlight the importance of *context* as a mean for

providing *input* that influences users' privacy related decisions (*bi-direction*). We borrow the principles of *feedback* and *control* from Bellotti and Sellen to provide a technical means for awareness and expressing privacy preferences. We also use Bellotti's and Sellen's framework to guide the development and evaluation of feedback interfaces.

The input from the environment is the first step towards building a socially translucent ubicomp system that provides a basis for respecting social norms. Characteristics of social translucence are described in detail below in section 3.1.1.

Our work is partially similar to the Privacy Mirrors framework (Nguyen and Mynatt 2002) presented in section 2.2.4. Similarly to Nguyen and Mynatt we borrow from the same work (social translucence and Bellotti and Sellen); and we also advocate the importance of awareness in the privacy management process. Hand in hand with Privacy Mirrors, in our approach we attempt to make ubicomp data visible, by providing feedback about the information flow.

What differentiates the work presented in this thesis is that we are interested in the interaction and user interface design aspects of providing awareness. Since the Privacy Mirrors framework was never formally evaluated (Iachello and Hong 2007), the effectiveness of this framework is not clear. In contrast, we aim at providing more specific answers about the effectiveness, representation and usability of feedback by building and evaluating real-world applications.

3.1.1. Characteristics of Social Translucence: Visibility, Awareness, Accountability

To explain the concept of social translucence we use the *glass door scenario* borrowed from Erickson and Kellog (Erickson and Kellogg 2000). Consider two door designs presented in the Figure 3-1. Option (A) does not allow the person to see what is on the other side, therefore opened quickly, it is likely to slam anyone who is about to enter from the other direction. The problem is that the user is not aware if there is another person on the other side of the door, therefore he cannot be accountable for his actions.

Option (B) illustrates a similar situation, but in contrast, the door allows the person to see whether someone else is on the other side, if so, he can adapt his behaviour to the situation. Design (B) is a simple example of social translucent system.

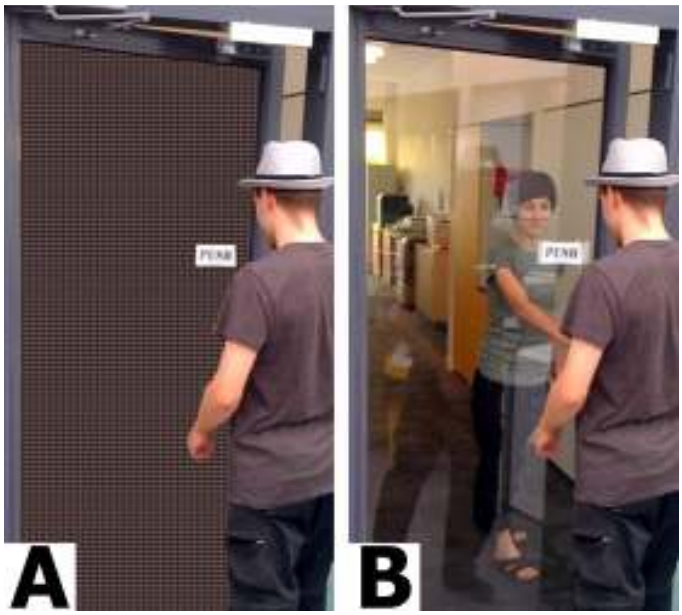


Figure 3-1. The impact of design features on social norms enforcement. Design (A) does not support social translucence. Design (B) supports social translucence.

While it is obvious why the socially translucent design solution works, Erickson and Kellog attempt to understand what makes the glass door effective. They found three reasons for that (Erickson and Kellogg 2000):

Visibility - the glass window makes socially significant information *visible*.

Awareness - the glass window supports *awareness*: I do not open the door quickly because I know that you are on the other side. This awareness brings our social rules into play to govern our actions: we have been raised in a culture in which slamming doors into other people is not sanctioned.

Accountability - a third, somewhat subtler reason for the efficacy of the glass window. Suppose that I do not care whether I hurt others: nevertheless, I will open the door

slowly because *I know that you know that I know* you are there, and therefore I will be held *accountable* for my actions. (This distinction is useful because, while accountability and awareness are usually concurrent in the physical world, they are not necessarily coupled in the digital realm.) It is through such individual feelings of accountability that norms, rules, and customs become effective mechanisms for social control.

Erickson and Kellog conclude that visibility, awareness and accountability are *building blocks of social interaction*. They argue that social translucence is a fundamental requirement for supporting all types of collaboration and communication. While their approach was mainly addressed to the computer supported collaborative work (CSCW) domain, we see a strong benefit for incorporating social translucence into privacy-aware ubicomp systems, for the following reasons:

- First, since ubicomp encompasses technical, physical and social environments, social translucence offers more natural approach towards communication, in which the information flow between the three environments can be more effective.
- Second, despite support for visibility and awareness, a third characteristic of social translucence – accountability, offers great promise for stimulating privacy-respecting behaviour and enforcing social norms in digital systems. It is a useful design feature as it might minimize the practical burden of privacy management as highlighted by Hong (Hong 2005).

3.2. Design Criteria for Privacy Awareness System

The design criteria of our system are based on the principles of privacy management described in the section 2.1.3 and gaps identified in the literature, presented in section 2.2.7. The main criteria for our privacy awareness system include:

i. privacy management should be treated as an ongoing process of selective disclosure of the information in reaction to the environment,
ii. the system should emphasize the hybrid model of privacy management,
iii. tools for expressing users' privacy preferences (control) and means for absorbing information from the environment (support for bi-direction) should be incorporated,
iv. control and feedback interfaces should not be intrusive and should reflect the dynamic nature of ubicomp applications,
v. end-users should be able to draw upon their real-world experience to structure interactions with others in order to reflect the natural behaviour from the real-world (support for social translucence),
vi. social norms should be enforced in order to minimize the practical burden of privacy,
vii. feedback information should be delivered in a timely and meaningful manner, and
viii. feedback interfaces should be extended by non-visual representations in order to enrich the user experience and minimize disruptions.

3.3. Representing Awareness - Feedback Classification

Our work seeks to find appropriate awareness mechanisms for a variety of contexts. We have designed a model for studying the role of feedback in location privacy management by classifying feedback along three dimensions: sensory, interaction and time. Consider the following example context scenarios:

> **SCENARIO 1:** Alice and Bob are users of the Buddy Tracker application. Bob checks on Alice's location when she is giving a presentation in a meeting. A blue LED light on her phone started flashing when she was presenting her slides (the blue light indicates that someone is checking her location). She glanced at her phone and after the meeting Alice checked who was checking her location.

SCENARIO 2: Alice is playing the favorite game on her mobile phone. While she was playing, a warning pop-up appeared saying that 'Bob just checked your location'. The game paused. She felt very annoyed as she lost her place in the game due to the alert.

These sample scenarios show a positive and negative example of how we can incorporate the real-time feedback within the spectrum of mobile privacy interaction. They also show how feedback can be delivered, describe the time when information is delivered, and also what triggers delivery of real-time notification. In order to support our studies on feedback in privacy management we have distinguished the following three feedback dimensions.

3.3.1. Sensory Dimension

The sensory dimension relates to the feedback representation, describing how information will be communicated to users. We have identified three subgroups of the sensory dimension:

- Auditory feedback - describes any audio interaction between the system and the user, which has been recognized as an intuitive and unobtrusive medium for communication (Gaver 1991). It can be as simple as a distinct musical tone playing when the event occurs or it can incorporate fully descriptive natural language feedback.
- Visual feedback - relates to any visual element or feature on a mobile device that supports interaction including GUI elements used in ad-hoc communication. It can be used to represent the current state of the system, and also to display aggregated information based on historical data, i.e. icons, warnings, dialog boxes, privacy critics (Ackerman and Cranor 1999), disclosure logs (Raento and Oulasvirta 2005; J. Y. Tsai et al. 2009), or map visualizations. Visual feedback can be also represented via hardware features, which relates to any visual feature of mobile device design that can be managed programmatically and used for communication (e.g. the LED light in HTC Dream[11] and other Android phones).

[11] http://www.htc.com/sea/product/dream/overview.html

- Tactile feedback - describes the vibro-tactile interaction between the system and the user such as the phone vibrating when an event occurs.

3.3.2. Interaction Dimension

The interaction dimension (I) describes how the sensory representation of feedback is triggered. Feedback can be released automatically or on demand.

- Automatic feedback - is released without user's intervention, every time the event occurs. Example: as soon as Bob checks the current position of Alice her phone immediately vibrates and plays a sound.
- On demand feedback - refers to a manual request made by the user, e.g. Bob shakes his phone to display a list of friends that accessed his location within last hour, or he chooses a menu option to access the disclosure log.

3.3.3. Time Dimension

The time dimension describes the temporal freshness of the information communicated via feedback mechanisms characterized by the sensory dimension. It can be divided into two categories:

- Real-time feedback - is designed to support users' awareness and visibility by providing timely information about the information flow, e.g. Bob's phone vibrates while Alice is accessing his current location.
- Aggregated feedback - relates to any aggregated information based on historical data from disclosure logs, examples include (J. Y. Tsai et al. 2009; Lederer et al. 2004).

3.4. Mobile Interfaces for Feedback

In the previous section we presented a feedback classification model. Our model uses three feedback dimensions that cover wide spectrum of mobile interactions: sensory, interaction and time dimensions. We used our model to survey existing HCI work in the area of privacy

awareness interfaces to highlight the timely but lagging research areas in the domain of interfaces for privacy awareness.

Table 2 presents a comparison of previous attempts to design awareness into privacy-sensitive systems. Numerous researchers have addressed the problem of real-time awareness in media spaces (Neustaedter and Greenberg 2003; Bellotti and Sellen 1993), awareness systems for collaborative living (Marmasse 2004; Sellen et al. 2006), Instant Messaging services (Hsieh et al. 2007) and location-sharing services (Sadeh et al. 2009). We also found several approaches for representing aggregated feedback information in ubicomp scenarios on demand, i.e. (Raento and Oulasvirta 2005) or (J. Y. Tsai et al. 2009). We could not, however, find any work aimed at exploring the utility of different sensory dimensions for providing real time feedback in the context of mobile applications.

Table 2. Comparison of existing awareness interfaces in ubicomp systems.

Interaction / Time	Automatic	On demand
Real time	(Bellotti and Sellen 1993) – LED (media spaces) (Neustaedter and Greenberg 2003) – audio (home media spaces) (Hsieh et al. 2007) – visual (large screen) – LED and audio (home media spaces) (Marmasse 2004) – visual (mobile device) (Sellen et al. 2006) – visual (situated device, large screen) (Hong 2005) – visual (large screen) (Sadeh et al. 2009) – visual (bubble, large screen)	We could not find any work that covers this group explicitly. However, aggregated on demand feedback interfaces could fit into this category, assuming that the interface provides a filter that allows the data owner show only recent requests mode on his data.
Aggregated	We could not find any work that covers this group of interfaces.	(Sadeh et al. 2009) – disclosure log (large screen) (J. Y. Tsai et al. 2009) – disclosure log (large screen) (Raento and Oulasvirta 2005) – disclosure log (mobile devices) (Toch et al. 2010) – disclosure log (mobile and web)

We also observed that there is no interface that displays aggregated feedback automatically, i.e. a system that could display information about disclosure of personal information automatically if an unusual pattern was detected. This function might be especially useful for people that do not have a need for continuous real-time automatic feedback, but are still concerned about their privacy. Although on-demand feedback information have been adapted in e-commerce solutions (i.e. an ecommerce system allows the administrator to see what products are being watched), we have not found any privacy awareness interface for representing real-time feedback information on demand.

While several design approaches for real-time feedback have been proposed, feedback interaction design for privacy awareness in the mobile domain is still lagging. In the next section we present how feedback information can be represented on mobile devices. Interfaces that could be used to cover different combinations of sensory, interaction and time dimensions are proposed.

3.4.1. Interfaces for the Real-Time Feedback

Below we describe examples of interfaces that could be used to provide feedback on or through mobile devices. Each interface element supports different sensory representations of feedback, including real-time and aggregated information delivery through automatic interaction. We used the Google Android platform to explore potential design solutions for feedback therefore some functionalities are platform or device specific, e.g., there is no support for LED light in iPhone devices, and the notification bar was specific to Android (note: the latest version of iOS5 provides new functionality called notification centre[12], which is similar to notification bar). Potential design solutions for the real-time feedback include:

- Dialog box (DIA) – pop-up like window provides controls for specifying privacy choices. When the dialog box is open the user can not perform any action until it is closed. One benefit of a dialog box is that it allows the designer to provide more

[12] "Apple - iOS 5 - See new features included in iOS 5.", http://www.apple.com/ios/features.html#notification [Accessed April 23, 2012]

context-sensitive controls for privacy management, i.e. the system can ask the user if his decision should be saved for the future (see Figure 3-2A).

- Toast (TOA) – small floating window displaying few lines of text in the bottom of the screen which disappears automatically after 2 seconds. It is less intrusive than dialog box as it does not prevent user from using the phone and does not require user's action (see Figure 3-2B).
- Notification bar (NB) – notification on the status bar (top part of the screen), adds an icon indicating type of event, with an optional ticker-text message. It does not prevent use of the phone and allows the user to see more information about the event by pulling the status bar down. An example of this notification inerface is presented in Figure 3-2C.
- LED Light (LED) – flashing LED light, in Buddy Tracker, a blue light means that someone is checking user's location (hardware specific, i.e. LED is common hardware feature for Android devices, while it is missing on the iPhone), see Figure 3-2D.
- Flashlight (FLA) – screen flashes a few times and then goes back to the previous state. The disadvantage of this solution is that it is potentially intrusive while the user uses the device, but its perceptibility is much higher than the LED's (see Figure 3-2E).
- Vibration (VIB) – special pattern indicates a location-checking event. It might be useful while the phone is not in use, i.e. phone in the pocket.
- Sound (SOU) – feedback is represented as a distinct musical tone playing when the event occurs or it can incorporate fully descriptive natural language feedback, e.g. playing synthesized or recorded speech: "Bob is checking your location".
- Security alert (ALE) - this type of visual feedback is used to display aggregated information in the event of unusual events, i.e. user X has checked Y's location 50 times in last two days. It can be used to present both real-time and aggregated information. In addition to verbal message Security Alert can incorporate a map visualization to convey richer feedback information about the event (see Figure 3-2F).

Figure 3-2. Selected visual representations of real-time feedback interfaces.

3.4.2. Interfaces for Aggregated Feedback

While interfaces presented in the previous section aim at presenting timely and meaningful information automatically in the real-time, in this section we present several design solutions for presenting the history of disclosures to the user. Although this type of feedback was explored extensively in previous research, in this section we will present alternative prototypes for touch screen mobile devices.

A number of design considerations for aggregated feedback were proposed in the recent literature, i.e. (Tsai et al. 2009; Sadeh et al. 2009; Raento and Oulasvirta 2005; Hong 2005). However, in previous work the feedback design has the information presented only in the form of a one-dimensional list representing disclosure logs. Moreover, only the prototype of Raento and Oulasvirta (Raento and Oulasvirta 2005) explicitly targeted the mobile applications domain.

Figure 3-3. Feedback in "Locyoution", a location-sharing application described in (J. Y. Tsai et al. 2009). Original, web-based version presented in section (A). Mobile version, proposed by us presented in (B).

Figure 3-3 shows a feedback interface that displays the disclosure log in the Locyoution application (J. Y. Tsai et al. 2009). Data owners can view the location requests made of them. Colors represents if the request was successful or not: a request is colored green when was

successful and red, when user's location was not displayed to the requester. Thumbs up and down icons allows the user to indicate the satisfaction with the decision made by the system, which can be used to change the privacy policy. While this is the most recent work on feedback and its role in privacy protection, we used Tsai's interface (Figure 3-3A) as a basis for designing a similar interface, for mobile touch screen applications. We present a mobile version of this interface for the iPhone device in Figure 3-3B.

Figure 3-4. Interactive Feedback GUI - a proposal for an interactive aggregated feedback module for touch screen devices (here an iPhone example). The interface allows the data owner to navigate between different types of information and apply additional filters by tapping on the "Filter" button in the top right corner (A). Visualization presenting requesters is presented in (B). Lastly, the user can tap on the selected data requester's icon for more details about particular situation (C).

An alternative mobile solution is presented in Figure 3-4, we call this interface Interactive Feedback. This interface provides full support for Schneiderman's Visualization Seeking Mantra (Shneiderman 1996):

1. it allows the user to glance at who viewed his location (overview first);
2. it provides filter mechanism for both the data type and time (zoom and filter);

3. and finally, Interactive Feedback enables the user to see details of the request (details-on-demand).

Another interface for representing aggregated feedback on touch screen mobile devices is presented in Figure 3-10. A full description of the interface is presented in section 3.5.4.2.

3.5. Buddy Tracker - Privacy Awareness Application

To evaluate our design approach for privacy awareness we built Buddy Tracker, a mobile application that allows users to share their location amongst a group of people. We start by motivating the domain choice for designing a privacy awareness system. Then, we discuss technical details of Buddy Tracker. We present its architecture and describe the main components of our system: a server and the client application. We also discuss how the design criteria based on theoretical frameworks and our literature review affected the architecture of our application. We conclude with the presentation of Buddy Tracker's functionality and privacy features.

3.5.1. Why Mobile Location-Sharing?

Although Ubiquitous Computing incorporates several types of devices and services, we decided to evaluate our approach in the domain of mobile location-sharing applications. We see location-sharing in mobile computing as a challenging design domain for awareness systems and interfaces for the following reasons:

- First, design guidelines have been proposed for building privacy-aware location-sharing applications (Iachello et al. 2005), but examples from the literature (Jedrzejczyk et al. 2009; Krumm 2007) and online articles[13] show that location is a very specific type of context and many users of location-sharing applications still do not understand what it means to share location. Survey by Tsai et al. (2009) shows that feel that risks of using

[13] "Please Rob Me Makes Foursquare Super Useful For Burglars", http://techcrunch.com/2010/02/17/please-rob-me-makes-foursquare-super-useful-for-burglars/, [Accessed June 9, 2011]

location-sharing applications outweigh the benefits, hence people are concerned about controlling who has access to their location.

- Second, location-sharing applications are not limited to one specific domain, i.e. media spaces or desktop computers. Hundreds of millions of cameras, PDAs and smart phones are now running thousands of different location-aware applications which make use of WiFi base station proximity/triangulation, GPS, or in some cases manual geo-tagging. In 2009, one third of new mobile phones launched had GPS capability. According to the 2009 report from Research and Markets[14], this ratio will likely rise to one half of all handsets by 2013.
- Third, growth in mobile location-sharing market suggests an increasing trend in popularity of location-sharing services. With cheap ubiquitous mobile broadband access and the widespread use of social networking both active and passive sharing of data, including location data, has become endemic [15].
- Fourth, mobile devices provide multimodal interaction styles. Interaction between the user and the device is not limited to the graphical user interface. Context-awareness, richness of input and output methods and robust hardware offer a great promise for designing novel interactions for feedback and control on mobile devices.

3.5.2. Technical Details

Figure 3-5 illustrates the architecture for Buddy Tracker, a mobile location-sharing service that supports bi-direction and the three characteristics of social translucence: visibility, awareness and accountability by incorporating real-time feedback.

We combined several separate services in our design, allowing us to develop prototypes quickly, deploy them automatically, and update services for users in the field without user

[14] "United Kingdom Location Based Services (LBS) Market Forecast, 2009 - 2013: Total spend in the LBS market in the UK to rise to $406 million in 2013 - Market Research Reports - Research and Markets." http://www.researchandmarkets.com/reportinfo.asp?report_id=1080767, [Accessed October 22, 2009]

[15] "Location Apps Research", http://www.skyhookwireless.com/locationapps/, [Accessed June 1, 2011]

intervention. Our application uses the Navizon[16] service which updates our server every 10 minutes using the most accurate positioning system visible to the device at the time: GPS, Wi-fi, or cell-id. Our application provides several options for managing privacy, which are described in section 4.3.

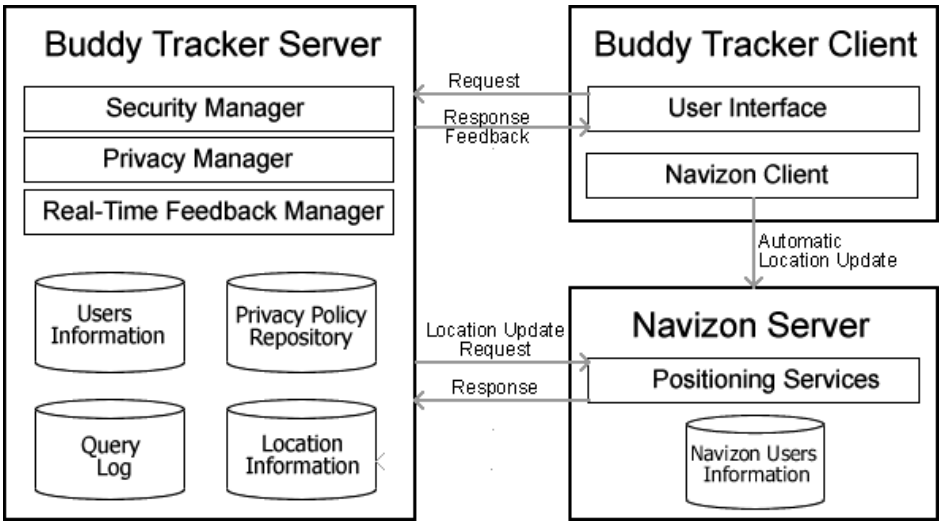


Figure 3-5. Early architecture of the Buddy Tracker.

3.5.2.1. Buddy Tracker Server

The server implements three modules (Security Manager, Privacy Manager and Real-Time Feedback Manager), and uses four data repositories (Users Information, Location Information Privacy Policy Repository and Query Log). The User Information repository contains information about users, such as their name, login, and password. The Location Information repository stores the users' positioning data as triple: time, location and user reference. Users' privacy preferences and real-time feedback preferences are stored in a Privacy Policy Repository and the Query Log contains information about location requests. This last repository is used by the aggregated feedback module provided in Buddy Tracker (Figure 3-5) to enable users to view who had accessed their location in the past.

[16] "Navizon, Location-enable solutions & apps with Wi-Fi, cell ids and GPS", http://www.navizon.com, [Accessed April 23, 2012]

We will now explain functionality of Buddy Tracker modules by illustrating an example location request, in which one user looks up location of another user in Buddy Tracker. Modules taking part in this interaction are presented in the Figure 3-5.

The first module that takes part in that request is the Security Manager; it is responsible for each user's authentication. After a successful check of a user's details in the Users Information repository, the location query is forwarded to the Privacy Policy Repository which analyzes the data owner's privacy policy. The system sends a response to the user based on requester's details and data owner's privacy policy. Information about the location query (data requester, data owner, location, granularity level of disclosed location) is then forwarded to the Real-Time Feedback Manager. The Real-Time Feedback Manager first checks the data owner's preferences for real-time feedback and then sends the feedback notification based on that information. Secondly, the Real-Time Feedback Manager saves the location request information in a Query Log for future reference.

3.5.2.2. Positioning service

The early version of the Buddy Tracker used Navizon[17] for user's location positioning, which provides a user's current location information. It is a third party service; therefore we had to develop a connector that integrates the Users Location repository with Navizon's database. Navizon is configured to update the user's position in its server repository every 10 minutes. The Buddy Tracker server sends a request to the Navizon service at the same frequency and retrieves an XML file containing the user's location information.

3.5.3. Social Translucence in Buddy Tracker

Our main objective when designing Buddy Tracker was to support the data owner's privacy. To this end we have created a system that helps people understand each other's actions with respect to their privacy and social relationships. Buddy Tracker's architecture is grounded on Altman's bi-directional function of privacy and the concept of social translucence, which has been

[17] http://www.navizon.com/

highlighted as a method supporting awareness, a shared knowledge that enforces accountability by making people's actions visible one to another.

We use an example scenario to illustrate how social translucence is implemented in Buddy Tracker. Figure 3-6 presents the interaction between two users of Buddy Tracker: data requester (U1) and data owner (U2). (1) A user of the client application (U1) sends a request to view the location of a fellow user (U2) to the Buddy Tracker server. (2a) The server generates a response containing U2's location information and sends it to U1. Additionally, (2b) the server generates a feedback response, which is sent to U2, informing them that U1 viewed their location. Here feedback supports the first characteristic of social translucence, visibility (3).

Each location request is only temporal in nature, but the cumulative effect of these requests creates a context which affects the interpretation of each subsequent request. This context we call awareness or *shared knowledge*, which is gathered by the user through their longitudinal accumulation of experience. Our intention in supporting social translucence was to help people build their shared knowledge about others by providing visibility.

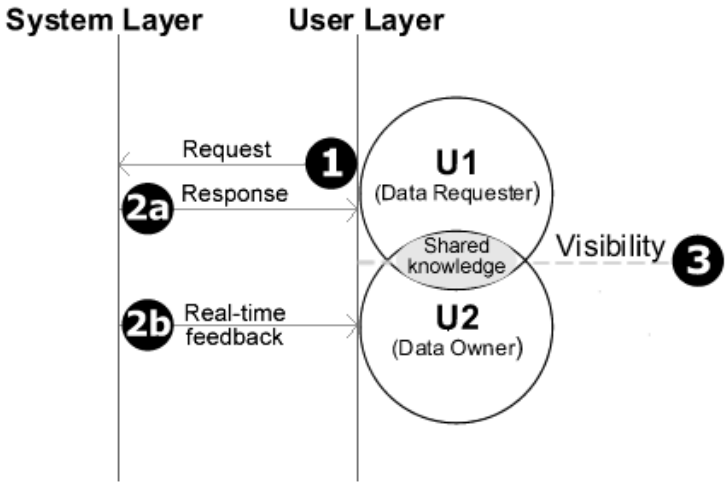


Figure 3-6. Social Translucence in Buddy Tracker. (1) A user of the client application (U1) sends a request to view the location of a fellow user (U2) to the Buddy Tracker server. (2a) The server generates a response containing U2's location information and sends it to U1. Additionally, (2b) the server generates a feedback response, which is sent to U2, informing them that U1 viewed their location. This feedback supports the first characteristic of social translucence, visibility (3).

The technical consequences of social translucence are twofold:

- First, the system needs to collect and store information about location requests (this function is implemented in the Query Log repository);
- Second, the system needs to represent the information in a meaningful manner to the user. According to Nguyen and Mynatt (Nguyen and Mynatt 2002), awareness arises when people process information about the information flow; therefore interfaces are needed to support visibility, which is the key to support awareness (see section 3.4 for information about feedback interfaces).

3.5.4. Client Application and Functionality

The Buddy Tracker client application is implemented as a web application, which appears and functions much like a native application on the iPhone and Android architectures, using the jQTouch library[18]. The interface can be also used on other mobile devices which support WebKit engine for rendering web pages, such as Google Android powered phones. This allowed us to activate and deactivate features instantly by changing the files on the server. It also allowed us to monitor usage of the system in order to send users instant experience sampling requests and to send real-time feedback to people whose location had just been viewed (a feature absent on all the other mobile location sharing services we considered).

The Buddy Tracker interface consists of two main areas, shown in Figure 3-7. The first area, 'Your buddies' shows the list of all friends (Figure 3-7A) with link at the bottom of the list to the map, presenting all friends on a single map (Figure 3-7C). Clicking on a buddy's name opens their profile (Figure 3-7B), with more detailed information about current location as a text description with a link to open an interactive Google Maps application.

The second area on the main interface, 'Your profile', enables users to see how others see their profile, set location-sharing preferences (discussed in details later), define map preferences or

[18] http://jqtouch.com

set preferences for real-time feedback notifications (e.g., notify me in real-time only if someone is looking at me too often, or if my friends are nearby, see Figure 3-11).

Figure 3-7. The Buddy Tracker application. (A) home screen view; (B) user's profile view; (C) 'all-on-the-map' view, presenting all friends on a single map.

3.5.4.1. Privacy Controls in Buddy Tracker

Our application provides several options for managing privacy, including both coarse-grained and fine-grained controls. Buddy Tracker provides time-sensitive coarse-grained visibility setting (Figure 3-8) that allows the user to hide his location for a limited period of time (e.g., the user can make himself invisible for the next 3 hours). The user's location becomes visible automatically; however Buddy Tracker reminds the user about that by sending a notification 15 minutes before his location becomes visible again.

Due to the research prototype nature of this application, Buddy Tracker does not allow the user to hide his location for more than three hours. Obviously in a real-world deployment, the application could incorporate more flexible settings, in which the user could manually specify the amount of time he wants to hide himself.

Figure 3-8. Coarse-grained privacy control in Buddy Tracker. This module allows the user to hide his location from all his friends for the period of time. In the above example the user hides his location for one hour (A). Next, the system confirms user's action and displays additional information about the SMS reminder that will be sent to the user 15 minutes before his location becomes visible (B). The reminder is presented in (C).

Figure 3-9. Fine-grained privacy preferences in Buddy Tracker. The interface allows the data owner to specify peer-to-peer privacy settings, i.e. hide his location from the selected buddy, blur the location information disclosed to his friends or disable access to the history (list of previously visited locations). Buddies are represented as icons to minimize the space needed to represent the profile, obviously it requires that buddies use a meaningful avatar to represent their persona in the Buddy Tracker. The last row allows the data owner to change his privacy settings for strangers.

Peer to peer coarse and fine grained controls are also provided (e.g., the user can say that X can see his location only at city level). It also allows the user to define privacy preferences for strangers. We adapted our fine-grained privacy settings from Reeder's Expandable Grids (Reeder et al. 2008) using a matrix layout. The privacy management interface is presented in Figure 3-9.

3.5.4.2. Aggregated feedback in Buddy Tracker

Our application provides an aggregated feedback mechanism, which allows users to see who has viewed their profile, location or who accessed their location history. Every location request performed by system users is stored in the database together with time and location information. Users can then view all requests made by their buddies and see who has viewed them when and where. To convey that information we used a list visualization (Figure 3-10a), similar to that used by (Raento and Oulasvirta 2005) and Tsai (Tsai et al. 2009). By clicking on the list item, users can view the location they were looked-up at, on the map (Figure 3-10b). Alternative interfaces for aggregated feedback are presented in the section 3.4.2.

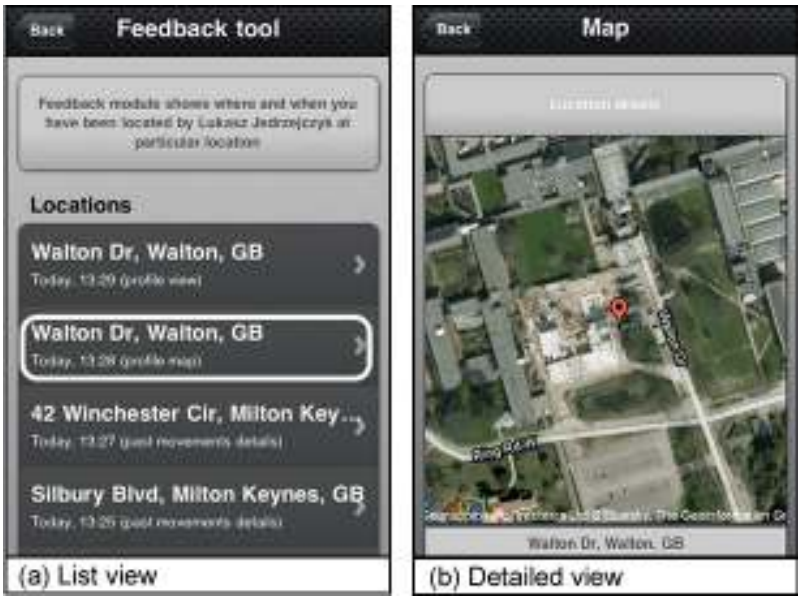


Figure 3-10. Aggregated feedback module in Buddy Tracker allows the data owner see who has accessed his location information.

3.5.4.3. Real-time feedback in Buddy Tracker

What differentiates Buddy Tracker from similar location-sharing applications is support for real-time feedback. Every time a user of Buddy Tracker checks another user's location the system automatically sends a notification to the data owner, which informs him about every check made on his location.

In the early version of the Buddy Tracker we implemented three types of real-time notifications:

1. Nearby friends – notification triggered if two or more friends are within the same area,
2. Who's checking my location – real-time automatic feedback about dissemination of location information,
3. Security alerts – aggregated feedback information delivered automatically every time the system detects unusual pattern in users' behaviour, i.e. system can inform data owner that one of his friends was checking on him very often.

Figure 3-11. Real-time notifications management in the Buddy Tracker. The user can switch on or off different types of notification. I.e. user can disable real-time feedback notifications about people checking his location while in the meeting.

While the nearby friends function was aiming at supporting social awareness of Buddy Tracker users, the goal of both real-time feedback and security alerts was to provide privacy awareness. By privacy awareness we mean understanding of activities of others that builds a context for own activities (in the spirit of Dourish and Bellotti (Dourish and Bellotti 1992)), which help the user understand the capabilities of a system, thus making him able to shape the system according to his needs (Nguyen and Mynatt 2002).

Buddy Tracker provides mechanism for controlling what types of notifications are actually used by the system. Users could easily switch different types of feedback on and off using real-time notifications module (see Figure 3-11).

3.6. Chapter Summary

In this chapter we presented the design criteria for privacy awareness systems that support a continuous privacy management process. We discussed the theoretical foundations of our approach and highlighted similarities and differences with the Privacy Mirrors framework, which is the closest to our approach.

We presented a model for classifying feedback interfaces for supporting awareness and surveyed a recent work on providing awareness in ubicomp scenarios. Our analysis showed a lack of non-visual awareness cues in the context of mobile devices, which have been recognized as the most ubiquitous devices these days. Next, we presented concrete examples of user interfaces for presenting feedback to the user. We designed both, real-time and aggregated feedback interfaces that could be used in a wide range of scenarios.

Drawing from previous attempts at visualizing feedback, we presented our own solutions for presenting feedback on touch screen mobile devices. A design for a novel Interactive Feedback interface was proposed that fulfills the requirements of Schneiderman's visualization seeking mantra.

Lastly, we presented Buddy Tracker, a mobile, location sharing application. We motivated our design choice and highlighted why we decided to investigate the role of feedback in privacy management in the context of mobile location sharing scenario. We explained the functionality of Buddy Tracker and discussed how the design criteria presented at the beginning of the chapter have been implemented in the application.

In the next chapter we will present results of the initial study aimed at exploring the role of feedback in supporting awareness and privacy management in mobile location sharing applications.

Chapter 4. In-lab Evaluation of Real-Time Feedback

> "*There is nothing like looking, if you want to find something. You certainly usually find something, if you look, but it is not always quite the something you were after.*"
>
> J. R. R. Tolkien

Effective privacy management requires that mobile systems' users be able to make informed privacy decisions as their experience and knowledge of the system progresses. Prior work has shown that making such privacy decisions is a difficult task for users because systems do not provide support for visibility, awareness and accountability when sharing privacy-sensitive information. In this section we present results of our investigation into the efficacy of real-time feedback as a mechanism for incorporating these features of social translucence in Buddy Tracker.

We explore the role of real-time feedback in privacy management in the context of Buddy Tracker by asking the following questions:

1. What is the impact of real-time feedback on users' behaviour? We investigate users' reactions to this technology and how it affects users' behaviour.
2. What are end-users' criteria for a socially accepted real-time feedback system? We are interested in how to build a context-aware real-time feedback manager system for supporting awareness that meets users' needs.

We decided to conduct two studies aimed at exploring the above questions:

1. A focus group discussion during which we presented the real-time feedback concept and explored its usability possibilities.
2. In-depth interviews with users of location-sharing applications.

Based on the data from the above studies we found that real-time feedback might have an impact on users' behaviour but the technology must consider the context of the user in order to minimize the intrusiveness of real-time notifications.

4.1. Focus Group Evaluation

In order to gauge initial user reaction to the range of interface methods, we conducted a focus group evaluation of the real time feedback notification methods suggested in section 3.4.

4.1.1. Study Objectives

The objective of this study was to investigate users' initial reactions to the real-time feedback technology presented in the previous chapter; in particular we were interested in:

i. exploring users' reactions to the concept of real-time feedback as a mean for supporting awareness and enforcing social norms in privacy-sensitive systems;
ii. understanding users' attitudes towards real-time feedback and study social issues that might affect the acceptance of the technology;
iii. eliciting requirements for socially acceptable feedback technology; and
iv. incorporating users' feedback at the early stage of the design process in order to address usability issues and design for positive user experience.

4.1.2. Methodology

Due to the exploratory nature of this study we decided to use a group discussion approach in order to collect a broad range of opinions about our technology.

The study lasted for 90 minutes. Although 4 participants said they had used location-sharing technology, none of them used it on a daily basis so we began the focus group with a short introduction of the Buddy Tracker application and the concept of real-time feedback. Participants were also presented with a working prototype of the real-time feedback mechanism installed on the mobile device running Android operating system.

During the next phase we presented the group with six different scenarios, showing examples of how our real-time privacy feedback works. Scenarios were presented in narrative form and were supported by videos and animations. We aimed to elicit a wider range of responses by incorporating a ContraVision method in the scenario design (Mancini et al. 2010). After the presentation, participants were guided into the discussion about the real-time technology and were asked to assign the most appropriate feedback representation for each scenario. Participant's opinions were audio recorded and transcribed, manual notes were taken by the interviewer. Collected data was categorized and grouped into affinity diagram (Beyer and Holtzblatt 1998), which helped us represent the hierarchy of problems/themes related to the real-time feedback technology. Main themes identified during the analysis were: social issues, privacy, usability and suggestions for improvements. Complete categorization scheme is presented at the end of section 4.1.4.

4.1.2.1. ContraVision Method for Eliciting Users' Reactions

The ContraVision method was developed in the course of the PRiMMA Project[19] (which the work of this thesis also contributes to). The method was originally described in (Mancini et al. 2010) and was motivated by the need for a new research approach for elicitation of privacy requirements of futuristic technologies. The underlying principle of ContraVision is to probe users' reactions to the technology by presenting two (positive and negative) representations of the same technology.

ContraVision borrows from the dual perspective in film-making, in which two films presenting the same topic could be compared and contrasted by common characteristics. Mancini et al. explain that "*the videos are comparable in that they present the same topic (i.e. ubicomp technology), use the same cinematic style, and are made of the same number of scenes representing the same situations with the same character(s) in the same locations. The videos are contrasting in that their main character has different attitudes and behaviours in relation to the technology and its adoption; the other characters also respond differently to the technology;*

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

the single respective scenes have different developments and the two stories have different outcomes" (Mancini et al. 2010).

Video, in that respect, works as a catalyst that provokes people and stimulates them to think about the technology in both, positive and negative ways. The main benefit of ContraVision lies in its exploratory nature, which allows the researcher to elicit a wider spectrum of reactions than using a single-view representation. Thus ContraVision was formally evaluated using videos as a presentation technique. However, Mancini argues that this approach can be applied to different techniques, such as scenarios or storyboards, which are less expensive.

4.1.2.2. Using ContraVision for Investigating Users' Reactions to the Real-Time Feedback Technology

Focus group participants were presented with six different scenarios, showing examples of how our real-time privacy feedback works. Our scenarios covered a rich set of different situations, in which the mobile technology is present. By using both negative and positive scenarios we also hoped to stimulate people to think about real-time feedback in the context of Bellotti and Sellen's (Bellotti and Sellen 1993) criteria for evaluating ubicomp systems, especially with respect to intrusiveness, appropriate timing, unobtrusiveness and perceptibility. Scenarios also covered different aspects of the real-time feedback technology, such as usability issues or social acceptance problems.

Figure 4-1 presents an example scenario showing both positive and negative reactions as the result of using real-time feedback for "nearby friends" notification. In the example scenario we highlighted the user's reaction as the measure of real-time feedback utility. All six scenarios used in this study are presented in the appendices section A.1.

After the presentation of all six scenarios, participants were asked to choose the best real-time feedback representation for each situation. Users could assign one or more feedback representations as the best choice. The goal of this task was to identify if there is a common preference for feedback interfaces or sensory dimension for particular scenario.

Figure 4-1. Stills from a video scenario presented during the focus group session. In this scenario Ed, a user of Buddy Tracker, is walking in a shopping mall. Suddenly his mobile phone plays synthesized speech: "Bob, is 50 yards from you" (1). Ed started looking around and noticed Bob looking in a shop window (2). In the positive scenario Ed decided to surprise Bob and calls his phone (3a). Bob, answered the phone, looked back and noticed his friend (4a). Both friends went into the coffee shop (5a). The Negative version of this scenario is slightly different. Ed, was very surprised that Bob is close to him (3b) and decided to hide behind trees (4b). Once he 'disappeared' in the physical environment he decides to hide himself in Buddy Tracker as well (5b).

4.1.3. Participants

We recruited eight participants (4 males and 4 females) aged from 24 to 40, offering a free lunch as compensation for completion of the study. We posted information about the study on our university's intranet page (potential population approximately 5,000 administrative, clerical, and academic staff plus approximately 200 PhD students). The group comprised 6 PhD students from different backgrounds (computer science, psychology, chemistry) and 2 administrative employees of the university.

4.1.4. Findings

All participants agreed that real-time feedback was necessary to some degree but none felt it was perfect. A common opinion was that it could help protect the data owner's privacy, but on the other hand, the nature of this technology is intrusive and needs to be really intelligent before it can be introduced in real applications. It was also suggested that "*people might stop using the (location-sharing) technology if they knew that whatever they did was visible to others*", which suggests a negative aspect of the real-time feedback to the adopters of the technology. While Tsai's (Tsai et al. 2009) observation was that feedback is a positive feature from the data owner's perspective - it increases the comfort level of sharing the location. The risk here is that some people might not be willing to use a socially translucent location sharing system. Participants reported that "*people might stop using the technology if they know that whatever they did is visible to others*". This problem is further explored in the field trial of Buddy Tracker, described in Chapter 5.

Another issue of the real-time feedback is that it could result in memory overload; one participant said that "*every time (someone) used it people might have a small, internal debate about 'should I do it?'*". However, this example confirms the effectiveness of social translucence in enforcing social norms. The goal of socially translucent systems is to enforce coherent social behaviour in digital systems by incorporating visibility that supports awareness. In this particular example, we observed that the participant's action would be governed by the

appropriateness of his behaviour, which in fact is an element of accountability enforced by awareness.

In the context of this study, on one hand, real-time feedback is desirable; on the other it is intrusive and decreases the comfort level of using the technology, both for data owner and data requester. The data owner might be interrupted with frequent annoying and incomprehensible messages and data requesters might stop using Buddy Tracker due to the transparency of technology.

Some participants suggested that real-time feedback would not be usable in the case of hundreds friends on a buddy list. They could not see the point of using real-time feedback for each friend, and suggested an option to define which friend/group of friends triggers real-time notifications. Participants also highlighted a need for aggregated feedback, which enables people to check who accessed their location information even if they missed a real-time notification. It has been also suggested that aggregated information about location requests could be used to automatically protect location information in a case of unusual usage, i.e. when someone tries to access location information of one person too often. Based on the number of requests the system could recognize unusual usage pattern and automatically decrease the accuracy of reported location.

Another important issue that raised by participants is appropriateness of the feedback interface for the situation. While interfaces provided by the Buddy Tracker were sufficient to cover wide range of scenarios in which the technology could be used, it became clear that the interface is just a first step towards designing a real-time feedback technology that is not only effective but also socially accepted. Participants highlighted a need for the *intelligent* and *situation-dependent* real-time feedback technology. Intelligence and context-awareness has been recognized a crucial element towards the acceptance of this technology. Interestingly, participants of the focus group suggested a number of contextual clues that could help determine the best notification for a given context. Examples of contextual clues that might

enhance the effectiveness of real-time feedback delivery include social context, mobile activity (e.g., browsing the Internet on the mobile device); position of the phone (e.g., in the pocket or on the table); visibility of the screen, real-world activity (e.g., being in a meeting or walking) or the presence of other people.

Participants also highlighted other factors that have an impact on the technology adoption and effectiveness, e.g., gender, lifestyle or the way one uses the phone:

Participant 1 (female): "*... what feedback display and when depends a lot on a social occasion, it depends on the person, like he* (Participant 2) *wants everything to vibrate*"
Researcher: (asking Participant 2) "*why vibration?*"
Participant 2 (male): "*Because it's in my pocket, nobody knows that. I'm free to check it later if I want. If I'm busy I can ignore it*". Participant continues and explains how vibration should be incorporated into the system: "*One vibration – text, two vibrations – someone's looking at me*"
Participant 1 (female): "*I don't have it in my pocket because I have no pockets. (...) when it is in my backpack I have lot of texts and missed calls. It depends in the person, how someone uses the phone…*"

The underlying concept of social translucence in Buddy Tracker was to increase awareness, support privacy management and increase the comfort of data owners in sharing their location. Our goal was to enforce accountability by providing visibility and awareness in the form of a timely and meaningful notices delivered via the mobile device. All participants agreed that the concept itself has the potential to protect privacy, but several conditions must be met before real-time feedback meets social expectations. Feedback representations presented during the study provided a set of rich interfaces, which in the opinion of participants, might help real-time feedback technology become an everyday thing, such as a new SMS notification. However, the usability of interfaces is only one part of technology adoption. The key to the success of real time feedback is context-awareness and intelligence; otherwise the balance between its utility and cost cannot be preserved.

Although this was a small study with a slight bias toward academics, it suggests that it is important that real-time feedback should enhance a system such that it provides meaningful information in the most appropriate way for a given context. Our participants also highlighted the need for aggregated feedback, i.e. social translucence cannot be achieved by real-time feedback alone, it has to be supported by aggregated feedback such as a disclosure log (e.g. Figure 3-10).

The focus group session helped us identify possible implications of using real-time feedback technology and highlighted usability problems of both the real-time feedback concept and proposed interfaces. This study also helped us draw an agenda for our studies on real-time feedback. Main themes and recurring problems related to real-time feedback technology identified during the focus group are presented in the Figure 4-2.

1.	Social aspects	
	1.1	Verbalizations show evidence that some users might not accept the technology.
	1.2	Verbalizations show evidence that feedback could result in memory overload.
	1.3	Verbalizations show evidence that feedback preferences depend on the lifestyle.
	1.4	Verbalizations show evidence of gender-related preferences.
2.	Privacy	
	2.1	Participants reported that technology might be intrusive, which affects privacy.
	2.2	Verbalizations show evidence of discomfort when using the location-sharing technology enhanced with feedback.
	2.3	Verbalizations show evidence that feedback technology has privacy-protection potential.
3.	Usability	
	3.1	Participants highlighted the problem of managing feedback preferences for different groups.
	3.2	Participants made suggestions for real-time and aggregated feedback design considerations.
	3.3	Verbalizations show evidence that usable real-time feedback technology requires multiple delivery channels and intelli
4.	Improvements	
	4.1	Participants made suggesstion for automated feedback in case of unusual locaion requests.
	4.2	Participants highlighted the need for the situation-dependent feedback.

Figure 4-2. Hierarchical groupings of themes and recurring problems related to the real-time feedback technology identified during the focus group.

While the focus group helped us identify several problems related to real-time feedback technology, we found that some participants could not see a value in the concept of location-sharing, which had an impact on their participation. Also, it is been suggested in the HCI

literature that one group could be unresponsive or unrepresentative (Krueger and Casey 2009). Therefore we decided to explore the same issues further, by interviewing more people. We recruited and interviewed users of applications with location-sharing functionality.

4.2. User Interviews

Due to the limitations of a single focus group and the low level of experience in using location-sharing services amongst the focus group participants we decided to validate and extend our findings through a number of in-depth interviews. Five people using applications with location sharing options were recruited to participate in this activity.

Comments from focus group discussions were very useful and helped us define the future path for studies on the real-time feedback concept. However, those participants based their views on a theoretical understanding of the technology rather than practical experience. To balance this, we interviewed active users of real location-sharing technologies to compare their opinions with the focus group results.

4.2.1. Study Objectives

Similarly to the focus group session presented in the previous section, the objective of this study was to investigate users' initial reactions to the real-time feedback technology. Interviews aimed to:

i. explore users' reactions to the concept of real-time feedback as a mean for supporting awareness and enforcing social norms in privacy-sensitive systems;
ii. understand users' attitudes towards real-time feedback and study social issues that might affect the acceptance of the technology;
iii. elicit requirements for socially acceptable feedback technology;
iv. understand users' expectations relating to usability and user experience.

4.2.2. Methodology

We interviewed 5 active users of location-sharing services. Interviews lasted between 40 and 90 minutes and were structured similarly to the focus group discussion:

1. introduction of the real-time feedback concept;
2. presentation of feedback interfaces on mobile device;
3. presentation of scenarios;
4. task - choosing the best representation for given scenario;
5. discussion – semi structured interview.

Similarly to the previous study, participant's opinions were audio recorded and transcribed, manual notes were taken by the interviewer. Affinity diagrams were used in the analysis session.

4.2.3. Participants

We recruited five participants (3 males and 2 females) aged from 15 to 35. We approached people directly by sending private messages to nearby people on two different location-sharing applications (Brightkite and Foursquare). We also posted requests on social networking sites, inviting experienced users of location-sharing applications to participate in our study.

4.2.4. Findings

Four participants said that the technology would definitely have an impact on their behaviour, and would stop curious people from making unreasonable location tracking actions. This corresponds to findings of the focus group discussion. The remaining participant said that real-time feedback would not have any impact on users' behaviour at all.

Since frequent real-time notifications can be intrusive, participants suggested different strategies for minimizing interruptions. Examples include automatic change of feedback delivery to less-intrusive in the situation when many people check one's location.

All participants said that real-time feedback should work according to the current state of the mobile device, e.g. do not use sound or vibration if phone is in the silent mode: one participant reported that "*it is easier to change modes of the phone than change settings of notifications*". An easy ON/OFF option and time sensitive settings were suggested as a method of avoiding distractions, especially at work. Some participants also suggested that they would like to be reminded about location look-up in next few minutes if there was no acknowledgment from them to the feedback (similar to Apple iPhone SMS notification system). A simple ON/OFF option was also suggested for controlling coarse-grained privacy settings.

The phone's position is the next contextual clue reported by our participants as having an impact on their preferences. Similar to the previous study, we observed that men prefer vibration more than women because they keep the phone in their pocket. The phone's ability to detect if it's in the pocket is desirable for males. Women prefer vibration less then men, especially when the phone is in the bag or on the desk (office workers), as it might cause a vibration of other items in the bag, i.e. keys or simply disrupt the owner and other people in the office. One participant's comment about vibration (female) "*Vibration is sometimes good, but if someone is checking my location too often and my phone vibrates – then it might disrupt me – especially at work*".

Another factor determining user's preferences for real-time feedback representation is mobile activity (it was also highlighted by focus group participants). Our participants reported that their preferences may be different when writing an SMS, playing a game or watching a video on their mobile device, e.g., users reported that toast is a good method of providing feedback while browsing the Internet but non-effective while talking on the phone. Therefore adaptation mechanisms should be in place, which maximize the effectiveness of the technology.

Changes in behaviour or distractions were not the only social implications of real-time feedback noted: participants were also concerned about disturbing other people, especially when using vibro-tactile and auditory representations.

All participants expressed interest in the real-time feedback technology and willingness to use it. Participants offered positive comments about the ability to control their data. It was perceived as a monitoring tool that empowers users, giving them full control over the information generated.

Like the focus group participants, interviewed participants expressed their concerns about the intrusiveness of the technology. Appropriate timing and unobtrusiveness seemed to be two main criteria affecting both the acceptance and level of comfort when using technology. Meaningful and timely information are the key factors determining trust in the technology. Other factors, such as perceptibility, flexibility or low effort, were also highlighted during interviews, but did not raise as many concerns as appropriate timing and unobtrusiveness.

Participants provided us with new insights about the nature of the mobile context and how contextual information can be used to provide a usable and unobtrusive feedback in real-time. For example: using phone settings to minimize the intrusiveness, not using auditory feedback in the presence of other people or using the phone's position and information about currently running application to determine the most appropriate notification. These findings suggest that work on real-time feedback should not be focused on designing new interactions and interfaces, but on the learning mechanisms and context-aware real-time feedback manager service, which decide how to tailor feedback to the user.

4.3. Discussion

Both the focus group session and interviews helped us identify potential problems related to real-time feedback technology. Participants highlighted several usability problems that might affect the social acceptance of real-time feedback, the findings suggest that we have done a good job at representing feedback information, but more effort is required at exploring novel interactions and methods supporting *contextual adaptation* (Dey and Abowd 1999). Interestingly, our studies equipped us with new insights about the nature of mobile context, and contextual factors that might influence the interface choices for feedback delivery. The most

common contextual factors described by participants include currently used applications (mobile task), screen orientation, current state of the phone or the company (people nearby).

While both studies confirmed that our approach might have an impact on people's behaviour (people would be more accountable for their actions), we had no empirical evidence to support that observation. Therefore our next step was to study the impact of socially translucent systems on people's behaviour in the real-world.

Since feedback has been recognized as an important factor allaying users' privacy concerns and increasing comfort of sharing location (J. Y. Tsai et al. 2009), our studies suggest that some people might not be willing to use a socially translucent location sharing system. However our participants' views were based on hypothetical situations, therefore we can not make a strong conclusion at this point. Both studies have shown that feedback has a potential to improve the understanding of the data flow within the system, which confirms previous findings of Nguyen and Mynatt (Nguyen and Mynatt 2002) and conforms to the underlying concept of social translucence theory (Erickson and Kellogg 2000) saying that *visibility* contributes towards greater *awareness* and enforces *accountability*.

Our agenda for studies on real-time feedback included:

i. evaluation of our system in the field trial in order to explore the effectiveness of our approach at supporting privacy management and social norms enforcement;
ii. implementing a context-collector – a new module for the Buddy Tracker that would allow the system to sense the environment and collect information about user's current situation;
iii. exploring methods that would allow us to build an intelligent tool for conveying the meaningful feedback information in the most appropriate way for the given context; and
iv. implementing a simple control mechanism for managing coarse grained privacy settings.

4.4. Chapter Summary

In this chapter we presented results of two studies aimed at exploring potential research issues related to the real-time feedback concept. Although the number of participants was small with limited demographic coverage, these initial users' reactions suggest that our technology is desirable but several criteria must be met before it can be socially accepted.

Although our work suggests that real-time feedback is a positive feature in terms of supporting one's privacy, we have no empirical evidence to prove the effectiveness of our approach. The results of our study addressing this problem are presented in Chapter 5.

The biggest issue highlighted by our participants is the lack of *intelligence* in delivering the feedback. We have designed several sensory representations of real-time feedback, which provide a diverse range of warnings for a given context. But we could not test them in the field trial with the first version of Buddy Tracker as it did not provide support for context-awareness and adaptation mechanism, which are the key towards the development of intelligent real-time feedback mechanism. We investigate the effectiveness of context-awareness and machine learning in ensuring social acceptance of real-time feedback using an improved version of Buddy Tracker in Chapter 6.

Another important issue highlighted in the above studies is lack of simple coarse grained privacy management. We address this issue by designing the Privacy-Shake interface, which is described in Chapter 7.

Chapter 5. Field-based User Evaluation of Real-Time Feedback

> "*The test is to recognize the mistake, admit it and correct it. To have tried to do something and failed is vastly better than to have tried to do nothing and succeeded.*"
>
> Dale E. Turner

In the previous chapter we presented the results of two initial studies aimed at exploring the effectiveness of real-time feedback in managing privacy. These exploratory studies helped us identify several issues relating to real-time technology, such as usability, social acceptance and lack of empirical evidence for the privacy protection potential of our approach.

In this chapter we report results of our investigation into the efficacy of real-time feedback as a mechanism for incorporating features of social translucence in location-sharing applications. We explore the role of real-time feedback in the context of Buddy Tracker, a mobile location-sharing application. Our work here focuses on ways in which real-time feedback affects people's behaviour in order to identify the main criteria for acceptance of this technology.

Based on the data from a three week field trial of Buddy Tracker we found that when using a system that provided real-time feedback, people were more accountable for their actions and reduced the number of unreasonable location requests. This work confirms our previous observations and also provides empirical evidence for the privacy protection potential of a socially translucent approach.

The following sections describe the study conducted, detailing our method and findings with a discussion of our results. Joint results of previous studies and the study described in this chapter are presented in section 5.5 as high level design criteria for designing real-time feedback applications in a manner that ensures social acceptance of the technology.

5.1. Study Objectives

The main objective of this study was to evaluate our system in the field trial in order to:

i. explore the effectiveness of our approach at supporting privacy management; and

ii. examine the impact of socially translucent system on social norms enforcement.

In addition to the two key objectives above we also continued the investigation of users' attitudes towards real-time feedback and studied the social issues that might affect acceptance of the technology. We also aimed at understanding people's feedback adoption criteria and eliciting requirements for effective and unobtrusive feedback technology.

5.2. Method

The field study consisted of three phases of one week each. In the first two phases, the participants had no privacy controls to protect their location and were free to use others' location information as they wished. Participants were part of an open society in which each users' location was visible to each member of the group. Data owners however had no knowledge about who was requesting their location. In the second week, participants were 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 beginning of the third week, we gave participants privacy controls, including an interface for setting coarse and fine grained location-sharing preferences (granularity control) as well as aggregated historical feedback and real-time feedback. In the third week each location request was visible to the data owner. At the end of the study, participants individually took part in debriefing interviews, which lasted between one and two hours. Interviews were audio-recorded and transcribed for further analysis. A diagram presenting our approach is presented in Figure 5-1.

Figure 5-1. Diagram presenting the methodology for the field-trial evaluation of real-time feedback.

5.2.1. Real-Time Feedback Implementation

We performed a field trial of Buddy Tracker to enable us to examine the usage of real-time feedback in a realistic scenario. Real-time feedback was delivered as a text message (i.e. a SMS message) sent to the tracked person, immediately after they had been looked up. The message took the form *"[X] has looked up your location*", where *[X]* was substituted with the relevant user's name. In comparison to the mobile interface elements described previously (Section 3.4.1), this form of feedback is closest to the dialog box element, incorporating elements of audio and vibro-tactile feedback depending on the user's device configuration for SMS notifications.

The rationale for using SMS as a method for delivering real-time feedback was twofold. Firstly, it was dictated by the low level of context-awareness in the initial implementation of Buddy Tracker. Lack of support for appropriate timing and unobtrusiveness could cause potential harm to our participants therefore we could not test different feedback representations at this stage.

Secondly, we knew that real-time feedback is an invasive technology, which can be become another annoying privacy feature that is quickly dismissed by users. Therefore we did not want to risk putting our participants into uncomfortable situations by presenting inappropriate feedback. Since text messaging is a widely used communication tool and each mobile phone user has his or her own strategy for handling disruptions caused by incoming text messages, we found this to be the best technology for delivering simple real-time privacy awareness at this early stage of our field studies.

5.3. Participants and Devices

We advertised the study through various mailing lists and by word of mouth asking for volunteers in a close social, family or work group, where all members of the group used an iPhone. Participants were told that they would use the Buddy Tracker prototype and allow us to monitor their activities, specifically any exchanges and interactions taking place between them and co-participants over a period of three weeks. We explained that we would send short experience sampling requests after each use of the system in order to collect data about motivation for any location tracking events. We also explained that we had instrumented the interface to collect information about any tracking events. Participants were offered £65 gift certificates for completing the 3-week study including pre- and post-study interviews, each lasting 90-120 minutes.

We recruited two groups of participants all of whom were experienced iPhone users in order to reduce Hawthorne and training effects (Adair 1984). The first group consisted of 7 people centered on one family (age range 17 to 52) with three young adult children and the partners of the two older children. The second group consisted of 5 people and was centered on a second family (age range 20 to 48) with two young adult children and a long-standing, close family friend. Each participant only had access to the real-time location data for all the other members of their own group.

In Chapter 3 we described the basic technical design of our Buddy Tracker prototype. After evaluating a number of Smartphone platforms we chose to implement our first prototype on the Apple iPhone, as it was the only device where we could get constant (every 10 minutes) automatic monitoring at a high level of accuracy (GPS/WiFi/Phone Cell) without depleting the battery before the end of one day (note: this study began in early 2010).

5.4. Findings

Over a period of 3 weeks 12 participants used the Buddy Tracker application 746 times (an average of three times/day/participant). We noticed only 81 views of the Buddy Map (showing all members of the group on a single map). Our participants preferred to check location of their friends individually using their profile. We found that user profiles (showing a text description of the user's location) were checked 668 times and of these the participants drilled deeper 305 times to look closer at the precise location of a buddy on a map, which could be accessed from the profile view (Figure 3-7). Participants did not indicate much interest in past movements of their friends; we recorded only 4 list views of past locations by a single member in the second group and no others.

5.4.1. Managing Privacy

Our participants did not express an interest in using privacy controls provided by Buddy Tracker with the exception of a few cases when they were specifically asked to do so during phase three of the study. We observed only one case, when our participant used a visibility setting without being asked to do that. As explained previously (see section 3.5.4.1), Buddy Tracker provides an interface allowing the data owner to hide himself by specifying a time period of invisibility, the user can choose between one, two or three hours. The user was automatically reminded about his location becoming visible 15 minutes before that happens. We asked the above participant about that event during the debriefing session:

Researcher: "*you made yourself invisible for 2 hours and you went back and hid yourself for longer*".

Participant: "*I went for drinks with one of my best friends (...) We hadn't seen each other so we met up and it's always like a very close personal thing, silly girly gossip whispering you know all this stuff and I quite liked knowing that it was really private from everybody. Everyone knew I was having some drinks because I tell everyone and she tells everybody, but while we were chatting it was just us and I quite liked that because that's how we open up to each other.*" Researcher: "*so the fact that you were able to hide yourself on that occasion made you feel more private than you would have been if somebody could have seen you on a map.*" Participant: "*Exactly! (...) You are conscious that other people, out of love, out of interest, or positive things but they are kind of aware. Which is fine there is nothing inherently wrong about it but sometimes you do just want to close the curtains.*"

The above highlights an important aspect of Altman's privacy regulation, which regards privacy as a dynamic process of regulating access to ourselves by others to fulfil temporal needs and the actual role. A lesson for privacy-aware systems designers is that privacy-sensitive systems should be equipped with coarse-grained privacy control, which has been previously highlighted by Lederer (Lederer et al. 2004).

We asked other participants about using privacy interfaces in the post-study interviews. Participants said that they did not change their privacy setting for a number of reasons:

- Social familiarity and closed-group setting: Some users did not feel the need to change privacy preferences because co-participants were members of their family or close friends and they had nothing to hide from them. Moreover, participants knew it was an experiment and their data were only accessible by specific group of people.
- Risk of misunderstanding: Some of our participants also said that changing privacy preferences would not be a good idea because other people would make inferences about the intent of not sharing everything within the social network, which might cause unpleasant situations and affect their relationships. One participant said that "*If I had used privacy settings my mum would be upset*". From their perspective, turning on

privacy settings in an advanced stage of the study was like changing rules during a game.

- Lack of familiarity with interface: Another reason given for not setting privacy preferences was that people did not have access to the interface for doing this (Figure 3-8, Figure 3-9) until phase three, and did not have sufficient opportunity to explore its functionality.

Of these, the main reason for not setting location-sharing privacy preferences was the first category, i.e. the experimental nature of the study coupled with the close relationship between the participants.

5.4.2. Social Implications of Feedback and Privacy Protection

The post-study interviews revealed that data owners, that is, those about whom location data was requested, were mostly neutral about feedback. Knowledge about who had accessed their location made them neither more or less willing to share their location information. Three participants said that they would not like to use real-time feedback in a real location-sharing application. The main reason given was that it starts to make the feedback recipient think about the motivation for the data requester, which can lead to false inferences, therefore people would like to avoid these situations by not knowing.

The perspective of the data requester is different, however. During interviews we found that that real-time feedback can have an impact on the data requester's identity and how their social networks perceive them. Participants also suggested that the information delivered in real time could shift one's position within the social network due to (wrong) inferences made by the data owner about the data requester.

We asked our participants if the visibility provided by real-time feedback affected their use of technology or comfort level of using it. They reported that feedback had a strong impact on how they used Buddy Tracker after it was introduced in the third phase. When another participant was asked if she would have repeated a tracking action she did in Phase 2, when there was no

feedback, once the feedback feature was activated she said "*I wouldn't have done it if I knew the person knows*". This demonstrates how real-time feedback introduces a "*Should I do it?*" debate in the user's mind, inhibiting tracking actions when there is no justification for them: "(…) *Obviously that would affect whether you tracked or not. Because if I were now tracking what the hell were you doing checking up on me unless I have an explanation for it*". Only one person (a mother from the smaller group) explicitly said that real-time feedback has no impact on how she used Buddy Tracker. However, she felt it was her instinct as a mother to check on members of her family frequently to protect them and if they received feedback about it then it would only reinforce that she cares about them. The mother in the larger group also reported that her use of the technology was to protect her family rather than being voyeuristic.

In order to look at how real-time feedback affected the usage of Buddy Tracker we also looked at the frequency of occurrence of the following two events: (1) checking buddies' location on a map and (2) viewing buddy's profile. We observed that the total number of each type of events in phase three was smaller than in the first phase (Figure 5-2). Although the larger number of events in phase one might be due to the "play" effect, data collected during interviews confirm that smaller usage of Buddy Tracker in phase three is the consequence of participants deciding to refrain from making location requests which they would find hard to justify had they been held accountable by the other party.

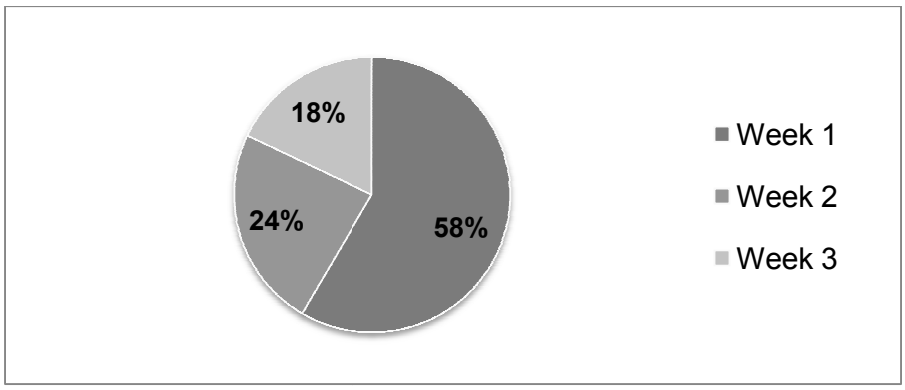


Figure 5-2. Pie chart showing frequency of tracking events made by Buddy Tracker users during each phase of the study as a percentage of all events.

Participants reported that the feedback did not stop them using the application but it made them think that they should have a good reason for using it: people are more accountable for their actions, which limits the number of unjustified tracking events.

5.4.3. Feedback Adoption

Although real-time feedback can be successful both in raising social awareness and preserving privacy, it has several disadvantages that were highlighted during interviews.

From a social perspective the biggest issue with real-time feedback is that people make inferences that can result in wrong judgments and also might affect social relationships. When deciding whether to locate someone, a requester has to deal with issues pertaining to motivation and responsibility, which a data owner does not have to do. When making a location request, certain conditions need to be met in order to (internally) justify the action. The purpose of that "*Should I do it?*" debate is of course not to think about the possible harm or other people's privacy, but to protect the person's own position within the group.

We found that the *internal debate* takes places also in data owner's head. One of our participants told us that feedback made her ask questions such as "*Why did X look at my location? What does he want?*". It shows that feedback might overwhelm some users with information, which results in inferences that can affect relationships.

5.5. High Level Design Criteria for Real-Time Feedback

Our studies have shown that real-time feedback is a desired option, which has a positive impact on users' privacy. At the same time technology needs to meet number of social criteria in order to be accepted. The invasive nature of real-time feedback technology has been recognized as the main barrier for this technology to be unobtrusively embedded. To help designers of mobile location-sharing applications get better insight into the how real-time feedback should be incorporated into the technology, we present the results of our studies as a set of high level design guidelines. We used Bellotti and Sellen's (1993) criteria for evaluating ubiquitous

services as a framework for presenting our results and highlighting the future direction of our research.

The design criteria presented below encompass findings from the field trial presented in this chapter and in-lab studies presented in Chapter 4.

Trustworthiness: *Systems must be technically reliable and instil confidence in users. In order to satisfy this criterion, they must be understandable by their users. The consequences of actions must be confined to situations which can be apprehended in the context in which they take place and thus appropriately controlled.* While Buddy Tracker supports both coarse and fine grained privacy controls, setting privacy rules is not mandatory and users can also make their profiles fully open which makes their data available to all users of the system. Visibility and awareness supported by real-time feedback are crucial to achieve accountability, as the factor supporting privacy of location information. Junglas and Spitzmuller highlight that trust in technology can result from the consumer's perception of being in control (Junglas and Spitzmuller 2006) therefore users that decide to use real-time feedback must feel that their privacy is protected and they are in control of their data. In other words, they are aware of who has access to their location information and they have an option to disconnect others by creating appropriate privacy rules.

Our studies have also shown that real-time feedback has to be supported by aggregated feedback information, which enables people to check who accessed their location even if they missed a real-time notification.

Appropriate timing: *Feedback should be provided at a time when control is most likely to be required and effective.* Buddy Tracker automatically notifies users about each location request made on them, which sometimes can annoy users and lead to the uncomfortable situations. Our studies revealed that users' willingness to receive a notification depends on the context, which incorporates several factors, such as time, location, mobile activity, phone's position, real-world activity, company and importance of the information. We found that mobile activity, which we

take as the current task being performed on the mobile device (e.g., phone call, writing SMS, browsing web), is an important factor in determining preferences for feedback representation.

Perceptibility/Unobtrusiveness: *Feedback should be noticeable. Feedback should not distract or annoy. It should also be selective and relevant and should not overload the recipient with information.* It is well known that too much privacy or security feedback numbs the user into ignoring it or switching it off. Buddy Tracker provides feedback representations in different dimensions, which conveys timely and meaningful information in both noticeable and more discrete form, depending on the context. Designers should use all available contextual information to provide feedback in a most visible and unobtrusive form.

Our studies have also shown that people would like to be reminded if there was no acknowledgment from the user to the feedback. A good example of this practice is a snooze function in an alarm clock; or the SMS delivery service in an Apple iPhone, which repeats the notification about a new text message a few minutes after delivery time if user has not read the message.

Minimal intrusiveness: *Feedback should not involve information that might compromise the privacy of others.* The underlying concept of real-time feedback is to support awareness by providing a simple message "*X looked up your location*". Therefore it is important not to provide too much detail about a requester, because it might affect his privacy. Real-time feedback in Buddy Tracker never discloses private information about the data requester, except name or pseudonym used in the system. It also depends on the feedback sensory representation used in a particular situation. Our studies revealed users' concerns related to using fully descriptive natural language auditory feedback in public places.

Fail-safety: *In cases where users omit to take explicit action to protect their privacy, the system should minimize information capture, construction and access.* An automatic hide/blur function for protecting one's privacy was suggested during the focus group study. Based on an unusual usage pattern identification, the system could automatically hide or blur one's location, which

can improve users' comfort for using location-sharing applications. In the basic scenario, automatic hide works as a user agent which helps negotiate location requests based on the information about relation, data flow and user's previous actions.For example, if user A is notified X times that another user B is looking up his location and if no explicit action is performed to prevent, ignore or continue that, the system could automatically change A->B privacy settings until A says differently. Automatic hide also contributes towards the low effort criterion, as it can help users justify their privacy preferences automatically.

Flexibility: *What counts as private varies according to context and interpersonal relationships. Thus mechanisms of control over user and system behaviours may need to be tailorable to some extent by the individuals concerned.* Buddy Tracker allows users to define whether and when they want to be notified in real time about particular events. Users have the option to switch real-time feedback ON or OFF (Figure 3-11). Real-time feedback should work according to the current mode of the mobile device, which minimizes the risk of disrupting users in their daily tasks and provides easy switch ON or OFF option for less discrete representations.

In the next version of Buddy Tracker (presented in Chapter 6) users could enable and select types of feedback. The system also provides an additional feature called *quiet hours*, which allows the user to specify when the system should not send any real-time feedback notification at all.

Low effort: *Design solutions must be lightweight to use, requiring as few actions and as little effort on the part of the user as possible.* In most cases real-time feedback does not require any effort from users. The underlying concept behind the feedback is to support awareness and understanding by providing timely information, although, some representations require user interaction (e.g. dialog box needs to be closed by the user). We found that feedback representations that require an action from the user are considered to be more annoying.

Another important element that helps meet this criterion is support for machine learning, which allows the notification system to adapt to users' preferences by learning from user's behaviour. The learning engine was introduced in the next version of the Buddy Tracker (see Chapter 6).

Meaningfulness/Learnability: *Feedback and control must incorporate meaningful representations of information captured and meaningful actions to control it, not just raw data and unfamiliar actions. They should be sensitive to the context of data capture and also to the contexts in which information is presented and control exercised. Proposed designs should not require a complex model of how the system works. They should exploit or be sensitive to natural, existing psychological and social mechanisms that allow people to perceive and control how they present themselves and their availability for potential interactions.* When designing for social awareness it is important to deliver meaningful information in an understandable manner. The real-time feedback interfaces presented in section 3.4 make use of known mobile interaction metaphors, such as sound, vibration or different types of visual elements, including programmable hardware features to enrich the user experience. In the most basic form, real-time feedback just conveys a standard message on the screen, such as "*X is checking your location*". Other interfaces, such as assigning a specific tone to this event function the same as the familiar assignment of a unique ringtone to a contact.

Low cost: *Naturally, we wish to keep costs of design solutions down.* Designing for real-time feedback is not an expensive task, as the message is simple. Our implementation uses well-known mobile interaction metaphors and GUI elements. However, the disadvantage is that some of the interfaces we developed only work on specific platforms. For example, the notification bar works on Google's Android powered devices and are absent on Symbian and Apple devices (at time of writing).

5.6. Discussion

Although this is a small study with a limited demographic coverage, these initial results suggest that real-time feedback is a good mechanism for supporting one's location privacy. Our

observations show that real-time feedback in the form of SMS messages can be used to incorporate social translucence into a location service, where the privacy of others is respected by providing visibility, awareness and accountability.

The introduction of real time feedback in the final week of the study had a definite effect on the participants' use of the system; it did not stop them but it did limit usage to the situations where they felt they had an obligation from the data owner to check his location. In other words, real-time feedback helped us introduce social norms into the digital system usage practice.

Our study indicates that one's privacy can be protected with little to no effort by making things visible one to another. We showed that visibility, which has been represented in the form of real-time notifications, resulted in better awareness of the extent to which the system works. We provided both quantitative and qualitative data to show that socially translucent architecture (presented in the section 3.5.3) successfully enforces accountability and limits the number of unmotivated and unreasonable location requests, which in consequence helps preserve one's privacy.

We have not observed any correlation between the knowledge of being tracked and changes in locations sharing rules. We believe this was due to the close relationship of our chosen participants. One of the lessons from our field evaluation is that restricting participants to a family-related group limited the scope of the data we collected.

This study has shown that real-time feedback does not only affects users' behaviour and activities within the system, but can also impact relationships in the real world. Participants did not stop using Buddy Tracker after real-time feedback was introduced, but its invasiveness and obtrusiveness has been reported as an important issue. The study proved a positive impact of real-time feedback on data owners' privacy, although we were not able to show that feedback has an impact on data owners' perception of control. We suspect this is due to the close relationship of participants we chose.

We proposed real-time feedback as a means for providing visibility, awareness and accountability in Buddy Tracker, a mobile location-sharing service. We argued that real-time feedback helps protect one's privacy by incorporating accountability, which reduces the number of 'unjustifiable' location requests. From our lab based evaluation, interviews and three weeks field investigation of Buddy Tracker we provided both quantitative and qualitative data to support the above hypothesis.

Although our participants did not change their privacy settings we suggest that this may be an artefact of the participant group types: both were very close extended families. Further studies involving peer groups and work relationships as well as more distant families are necessary before any further conclusions can be made about the utility of privacy settings.

Our study revealed a number of interesting phenomena about protecting privacy within the spectrum of a location-sharing service. We found a positive impact of social awareness on location tracking activities and privacy protection. However, our groups were limited, both in terms of diversity and social relations and in terms of number so further studies are clearly needed.

Although our work suggests that real-time feedback is a positive feature in terms of supporting one's privacy, there is clearly much more work to be done. We have designed several sensory representations of real-time feedback, which provide a diverse range of warnings for a given context. However we could not test them all because at the time of conducting our field trial, Buddy Tracker did not support appropriate timing, which has been recognized as a crucial element for the acceptance of this technology. A similar finding was described in the previous chapter presenting results of focus group discussion and user interviews.

Therefore it is important for us to explore how to convey meaningful information in the most appropriate way for a given context. To this end, we decided to conduct further work aimed at understanding users' preferences for real-time feedback (described in section 6.4) and extending the functionality of the Buddy Tracker by:

i. implementing a context-collector – a new module for the Buddy Tracker that would allow the system to sense the environment and collect information about user's current situation; and

ii. developing a machine learning module that would allow us to build an intelligent tool for conveying the meaningful feedback information in the most appropriate way for the given context.

We present our attempts at incorporating context-awareness and machine learning for a better user experience in section 6.5.

5.7. Chapter Summary

In this chapter we presented the field-trial of early version of the Buddy Tracker equipped with a real-time feedback feature. Our field trial showed that people were more accountable for their actions if they knew that the data owner would be notified of their request. Providing feedback to those whose location was being checked resulted in better awareness of the location requests made by others. This resulted in location requests being made only when the requester has good reason to do so.

This study provides empirical evidence on the effectiveness of a socially translucent architecture for social norms enforcement in digital systems. This study also helped us identify design choices for socially acceptable real-time feedback system.

Despite the positive results of this study, there is much work to be done at improving our system in order to meet those criteria. The key problem reported in the studies we conducted so far is lack of *intelligence* – our system cannot adapt to deliver the most appropriate real-time feedback representation for a given context. In the next chapter we investigate the effectiveness of context-awareness and machine learning in ensuring social acceptance of real-time feedback. We start with the presentation of results of the survey we used to collect data about users' real-time feedback preferences in different scenarios, which we used to inform the design and

development of a Real-Time Feedback Manager, an extension for Buddy Tracker supporting context awareness and machine learning for better user experience.

Chapter 6. Context-Aware Real-Time Feedback

> "*A computer would deserve to be called intelligent if it could deceive a human into believing that it was human.*"
>
> Alan Turing

In Chapter 5 we concluded that future work on real-time feedback technology should focus on (1) understanding users' preferences for real-time feedback and (2) extending its functionality by implementing context-awareness and a learning mechanism that will enable the interface to adapt to the users' situation. Here, we discuss how the above problems have been addressed in the second version of Buddy Tracker.

We start by describing the architecture and technical details of the extended Buddy Tracker application that addresses shortcomings identified in our previous studies. We focus in particular on three new features: a context collector, a learning engine and a real-time feedback manager. These three elements are the key towards minimizing the intrusiveness of our technology. Recall that intrusiveness and lack of intelligence have been recognized as the biggest criticism to the real-time feedback technology reported by participants in our previous studies (see Chapter 4 and Chapter 5).

Next, we present an online survey (section 6.4), in which we collected users' feedback preferences based on their responses to potential scenarios. We detail the survey design process and discuss how results of the survey informed the field trial of the real-time feedback manager – a context aware real-time feedback technology.

Furthermore we report on our experience from the development process and also discuss findings of our field study with 15 participants (section 6.5). The findings show that context-awareness and machine learning can minimize the intrusiveness of the real-time feedback technology, therefore making this function socially acceptable and allowing users to benefit

from the increased level of awareness that real-time feedback affords. We conclude with recommendations on how a better understanding of the user and application-specific context can improve the user experience and social acceptance of the system.

6.1. Redesign of the Buddy Tracker

In this section we present a new version of Buddy Tracker, a mobile phone application that allows users to share their location amongst a group of people. Here, when we talk about Buddy Tracker we refer to the extended Buddy Tracker application addressing shortcomings identified in our previous studies.

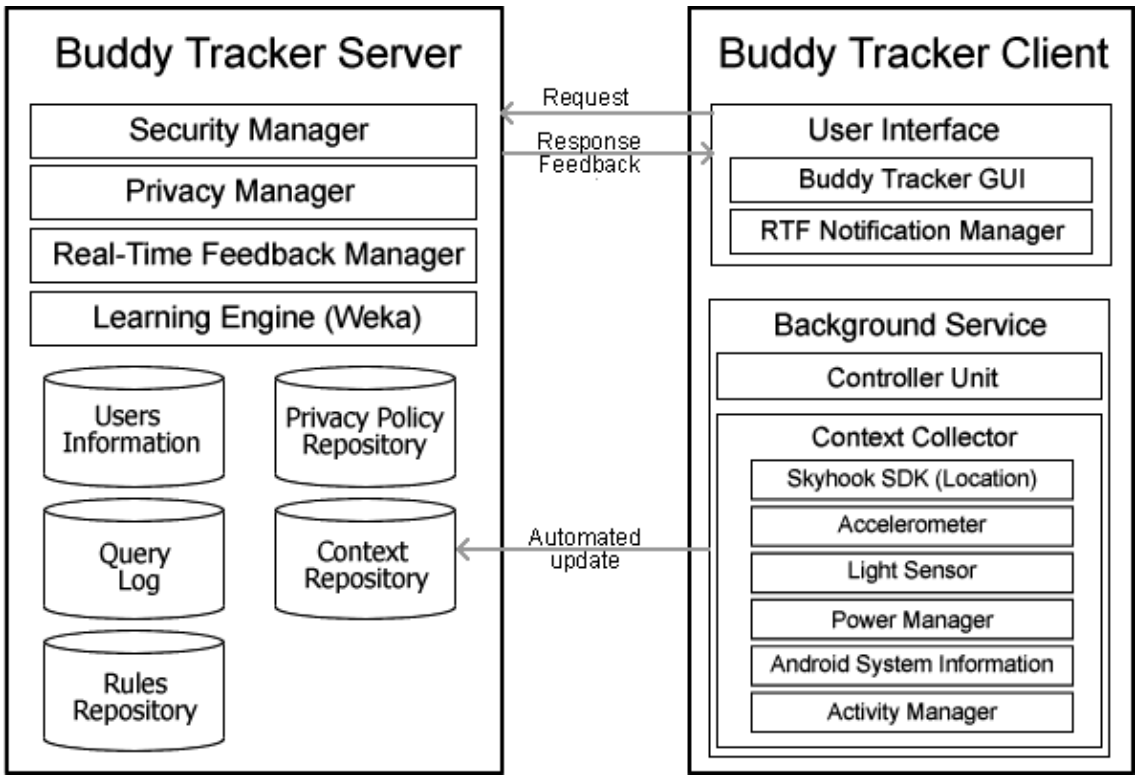


Figure 6-1. An extended architecture of the Buddy Tracker application.

The application comprises two main components, a client application developed in Java for Android devices and a server application, which has been implemented as a set of PHP classes working on top of the MySQL database. HTTP is used for communication between the client

and the server. Encryption mechanisms are used to prevent eavesdropping of the sensitive contextual information transmitted from the client device. The architecture of the new Buddy Tracker system is illustrated in Figure 6-1.

6.1.1. Buddy Tracker Server

The server implements four modules: Security Manager, Privacy Manager, Real-Time Feedback Manager and the Learning Engine (described in section 6.3); and uses five main data repositories (User Information, Privacy Policy Repository, Query Log, Context Repository and Rules Repository). The User Information repository contains information about users, such as their name, login and password. The Context Repository stores the users' location information and other contextual data (see section 6.2).

Users' privacy preferences are stored in a Privacy Policy Repository and the Query Log contains information about location requests. This repository is used by Buddy Tracker's aggregated feedback module, enabling users to view who accessed their location in the past. The remaining element, the Rules Repository, contains information about users' preferences for real-time feedback. Note, that initial rules for users' real-time feedback preferences have been derived from the data collected in the survey (see section 6.4).

The functionality of Buddy Tracker's server modules can be illustrated using an example scenario in which a user looks up the location of another. The first module that takes part in that request is the Security Manager, which is responsible for each user's authentication. After a successful check of a user's details in the Users Information repository, the location query is forwarded to the Privacy Manager which analyzes the data owner's privacy policy. The system sends a response to the user based on the requester's details and the data owner's privacy policy.

Information about the location query (data requester, data owner, location, granularity level of disclosed location) is then forwarded to the Real-Time Feedback Manager that communicates with the Controller Unit on data owner's device in order to collect data owner's current context information collected via Context Collector.

Next, the Real-Time Manager checks the data owner's preferences for real-time feedback (stored in the Rules Repository) and cross-references that with the user's context; and then returns the most appropriate feedback representation to the Controller Unit on the client device. The controller Unit communicates with the GUI and displays the real-time feedback notification to the user.

Simultaneously, the Real-Time Feedback Manager saves the location request information in a Query Log for future reference, in case the data owner wants to use an aggregated feedback to see who looked up his location. In the situation when the Real-Time Feedback Manager can not find a personalized rule for the data owner, the system uses initial rules stored in the Rules Repository in order to minimize the intrusiveness of the notification. The process of deriving initial rules for delivering the most appropriate real-time feedback in the given context is described in section 6.4.4.

The Learning Engine is used to derive new, personalized rules based on the user's feedback. By personalized rule we mean a rule that has been created based on the recipient's feedback in reaction to the real-time feedback notification. The method for collecting user's feedback is discussed in the methodology section (see section 6.5.2).

6.1.2. Buddy Tracker Client for Android

The Buddy Tracker client application is implemented as an Android application. The client application consists of two elements: the user interface, which allows users to control the disclosure of their location, change privacy preferences and check their buddies; and the background service, which automatically updates the user's current context and checks for new location lookups. The background service consist of two elements, a Controller Unit responsible for communication with the server; and Context Collector, responsible for sensing the user's environment. Buddy Tracker for Android also supports the interfaces for real-time feedback presented in the section 3.4.1.

6.1.2.1. Home Screen and Main Functionality

The Buddy Tracker for Android application is presented in Figure 6-2. The primary interface of Buddy Tracker shows five tabs:

1. Home – main screen, allowing the user to control the frequency of location updates and switch on/off the background service.
2. Buddies - shows the list of all friends with a link to the map at the bottom of the list, which shows all the user's friends on a single map. Clicking on a friend's name opens their profile, with more detailed information about current location as a text description with a link. In this section the user can also adjust their privacy preferences (i.e. hide/blur their location for chosen person, or hide their location for a specified amount of time). See Figure 6-2 A.
3. Settings – allows the user to adjust their quiet hours (time, when the system should not deliver notifications, e.g. the user can tell the system that they do not wish to receive any notifications between 10PM and 7AM) and enable preferred representations of the real-time feedback. See Figure 6-2 B and C.
4. Feedback - aggregated feedback mechanism, which allows users to see who has viewed their profile, location or who accessed their location history. Users could also access aggregated feedback information directly from the buddy profile.
5. Forms – displays a list of recent ESM questionnaires awaiting user's feedback. ESM questionnaires are described in detail in section 6.5.2.

Figure 6-2. Buddy Tracker for Android. Picture A presents a main screen; B and C present a Settings module that allows the user to adjust quiet hours and enable/disable preffered feedback interfaces.

6.1.2.2. Support for Real-Time Feedback

The new version of the Buddy Tracker application, Buddy Tracker for Android, supports numerous sensory dimensions of real-time feedback. From the list of real-time feedback interfaces presented in section 3.4.1 we do not provide support for flashlight, a flashing screen notification. We decided to drop this functionality due to the low acceptance for this type of interface as observed in our exploratory studies.

6.1.2.3. Background Service and Context Collector

The background service is implemented as an invisible part of the Buddy tracker client. It consists of two main modules, the Context Collector responsible for contextual sensing and updating the user's current context on the server; and the Controller Unit, whose main function is to communicate with the Real-Time Feedback Manager and checking for new location lookups.

The Controller Unit is implemented as Android service class, and its functionality can be managed from the main user interface. For example, the user can switch the service ON or OFF

when and as needed: the user can also set up the frequency for checking for new location lookups.

6.2. Context in the Real-Time Feedback Manager

Results from our previous studies (see Chapter 4 and Chapter 5) on the efficacy of real-time feedback suggest that the most important requirement for the social acceptance of real-time feedback is the system's ability to convey meaningful information in the most appropriate way for the given situation. This requires the mobile application to be able to sense the environment, *contextual sensing,* and adapt the user interface to the given situation, *contextual adaptation* (Dey and Abowd 1999).

According to Dey and Abowd, situation is described by context, which is defined as "*any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves*" (Dey and Abowd 1999).

In order to use the user's context effectively, we started our work on context-aware real-time feedback with exploratory studies aimed at understanding what 'mobile context' means for our application, and how we can utilize that. Based on the findings of our initial studies and on the analysis of several reports providing information about usage practices of mobile devices, we combined that knowledge with the capabilities of current mobile platforms in sensing the environment. The outcome of our analysis has informed the list of contextual information types supported in Buddy Tracker, which is presented in Table 3.

Buddy Tracker uses several available sensors, such as the GPS, accelerometer, light sensor, Android system logs, information about currently running applications and other methods to collect the most accurate information about the user's context. Calendar entries can be used to determine the user's current activity; and the Google Geo Service is used to translate GPS coordinates into more meaningful text descriptions. We use Skyhook's Core Engine SDK to collect information about the user's current position. Unfortunately, due to technical problems

and a negative effect on battery life, we could not implement noise level sensing in our field trials, although this feature was implemented in our lab-based standalone application prototype.

Table 3. Types, representations and descriptions of contextual information collected by Context-Manager component in the Buddy Tracker.

Type	Representation	Description
Identity	User information	Information about the user, i.e. age, gender
Time	Timestamp	Date and time of update
Location	Coordinates	Collected through GPS, WiFi or nearest cell-id
Location	Full Address	Collected through Google Geo Service API
Location	Category	Category of location, i.e. work, gym, shopping centre, library. We used categories from (Khalil and Connelly 2006)
Location	Personal tag	User defined description of the location, i.e. home, John's
Screen state	0,1	Says if the screen was on/off
Current task	Package name	Currently used application, i.e. com.android.camera suggests user was using a camera
Phone mode	Normal, In call or Ringtone	Describe the current state of the phone
Ringer mode	Silent, Vibrate or Normal	Current ringer setting
Battery level	0-100	Battery level shown as percentage
Battery charging	0,1	Tells if battery was plugged to the charger
Light level	Number	Current light level in lux
Light description	i.e. dark, bright inside	Current light level expressed in natural language
Phone in use	0,1	Says if the user was using the phone
Movement	x,y,z	Reading from the accelerometer
Phone position	Number	Current position of the phone, calculated based on the current accelerometer reading.
Screen visibility	Text	Textual representation describing probability of the screen's visibility: unknown, visible, maybe_visible or invisible
Screen brightness	0-255	Numeric representation of the screen brightness
Company	0,1	Tells if user is likely with others. Collected form users' calendar, i.e. meeting entry suggests not alone
Company relationship	Text	Label representing relation between the user and the company, we used categories from (Khalil and Connelly 2006)
Current activity	Text	Real world activity, collected from the calendar or inferred through the current location

Contextual information describing the user's current situation is used in the learning module, which is directly connected to the real-time feedback manager, and its role is to learn new rules based on the user's context.

6.3. Learning Engine and Rules Enforcement

At the heart of the Buddy Tracker architecture is the learning engine. The learning system is responsible for analyzing the user's context and creating a predictive model (rules) of their preferences for the real-time feedback. We initially developed our own learning algorithm, which required users to provide additional information about the relevant context. In other words, in addition to the questions presented in Figure 6-6, participants also had to tell the system what contextual factors had an impact on their decision and whether the feedback notification was or was not appropriate in the particular situation when they were notified. Preliminary tests showed that the algorithm was not usable because it required too much input from users. As a result people were less willing to answer questionnaires.

Therefore we decided to find a more affordable learning algorithm, which resulted in a more usable method of collecting users' feedback. After the examination of several algorithms available in Weka data mining software (Hall et al. 2009) on the dataset collected from the survey discussed in section 6.4 we decided to use the J48 implementation of the C4.5 algorithm (Quinlan 1993). The algorithm is capable of learning from incomplete contextual information, which minimizes the user's effort and increases the chance of collecting useful data. We also found that this algorithm has an intuitive way of representing the rules, which is useful in examining the most relevant contextual factors. By 'most relevant context' we mean elements of context that have the biggest impact on users' preferences. Other algorithms we considered performed poorly on a few preliminary tests and C4.5 was preferable because it is an established (and reliable) technique.

The learning engine consists of two main elements, the learner and the interpreter. The learner's job is to analyze users' feedback and cross reference it with contextual factors describing the

environment and create a user's model. A model is a decision tree that contains users' rules for real-time feedback preferences. The second element of the learning system, the Interpreter, is responsible for rules enforcement.

The interpreter can be seen as a function $f(C_1, C_2, \ldots, C_n)$, where each argument describes individual contextual factors as shown in Table 3 (i.e. C_1 = *location label,* C_2 = *ringer mode,* C_3 = *mobile activity* etc.). The complete function can be represented as $f(C_1, C_2, \ldots, C_n) = RTF$, where RTF, the output of this function, is the most appropriate real-time feedback representation for the given situation.

6.4. Study 1

Context-awareness has been identified as one of the shortcomings in the current implementation of Buddy Tracker. Therefore richer understanding of context was needed before we could proceed to the next step – development and evaluation of Real-Time Feedback Manager.

Here we present an online survey, in which we collected users' feedback preferences based on their responses to potential scenarios. We detail the survey design process and discuss how results of the survey informed the field trial of the Real-Time Feedback Manager – a context aware real-time feedback technology.

6.4.1. Study Objectives

Our previous studies showed that real-time feedback is an intrusive technology, and a wrong notification could have a negative effect on users' experience. Therefore we decided to support context-awareness and adaptation mechanisms in the Buddy Tracker. Towards this end we started our work by asking the question below:

What is the most appropriate feedback representation for the given context?

The main goal of this study was to:

i. capture people's preferences for the real-time feedback notifications if they were using our Buddy Tracker technology; we aimed to collect a range of data about users' preferences for real-time feedback across different situations;

ii. derive initial rules, which would minimize the negative impact on users' experience in the field trial (described in section 6.5);

By deriving initial rules for real-time feedback preferences we also wanted to minimize the number of participants that could potentially withdraw from the study due to the system delivering inappropriate feedback in early use.

6.4.2. Method

We conducted a scenario-based online survey to collect information about people's preferences for real-time feedback notifications. We were aware that using surveys to analyze users' experience isolated from their natural setting might introduce biases due to the discrepancy between peoples' beliefs and intentions, and their actual behaviour (Jensen et al. 2005). Therefore, we used videos to allow users to indirectly experience the interface as realistically as possible. In this section we present the design, method and recruitment process.

6.4.2.1. Scenario Design

Based on the data we collected during interviews with users of location sharing technologies, focus group participants and information about people's mobile practices, we created 24 different scenarios. Each scenario was especially designed to cover different types of contextual information, such as location, real-world activity, mobile task or presence of other people. A full list of all contextual variables supported by our scenarios is presented in the Table 4.

For example, a scenario looking at users' feedback preferences in context would read: "*Imagine, you are seated in a restaurant and, while waiting for your meal to arrive, check your bank statement via mobile browser when Jenny checks your location.*" In this scenario, the context comprises the user's location, phone's position, mobile activity and real-world activity. Results presenting users' preferences for this scenario are shown in Figure 6-3. In addition to the textual

description, we also showed the participants an image illustrating the situation. A list of all scenarios is available in the appendices (A.2.).

Table 4. Contextual variables used to design scenarios for the survey.

Contextual variable	Description
Pv	Phone's visibility, yes or no
C	Company, tell if user is with others, yes or no
Pin	Phone in use, says if the user was using the phone, yes or no
R	Relationship with the data requester, i.e. wife, boss
I	Importance of the requester, information, situation, i.e.
L	Location of the user, i.e. work
A	Activity, a real-world activity, i.e. in the meeting
MA	Mobile activity, a task performed on the mobile device, i.e. writing SMS

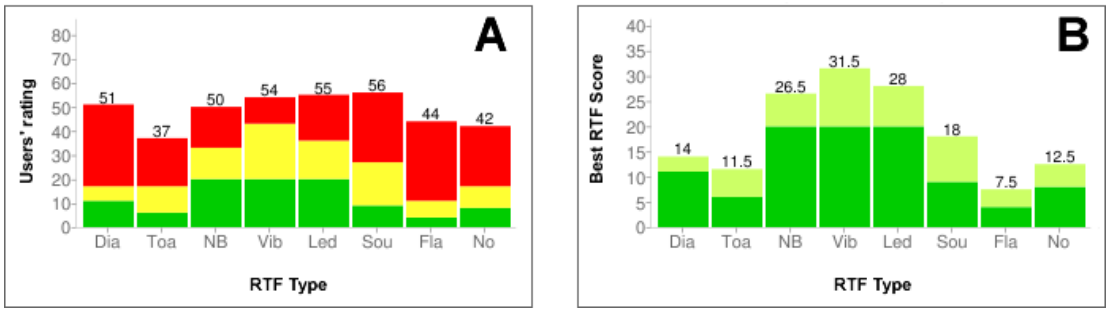


Figure 6-3. Survey results for scenario four ('*Imagine, you and your friends are engrossed playing your favourite game on your mobile. When, Alison checks your location.*'). Chart A shows all users' answers/ratings for this scenario. Users' preferences for particular interface are represented using three colours (green – best option, yellow – acceptable, red – unacceptable option). Chart B presents a selection of the best real-time feedback (RTF) representation for this scenario. Using the formula Best = answers (best) + answers(acceptable)/2 we found that notification bar (Vib) is the most appropriate interface for this scenario.

6.4.2.2. Survey Design

Each participant was asked to express his or her preference for each of 10 scenarios, randomly assigned to them amongst the 24 available. Users had to assign at least one feedback representation to one of the three options: *best choice*, *acceptable* or *please no*, representing the most inappropriate feedback representation. Users could not assign one feedback type to more than one option, i.e. sound cannot be the *best* and *acceptable* choice at the same time. This approach helped us identify the most unacceptable feedback representations, which were ignored in case of small differences in certainty of positive answers.

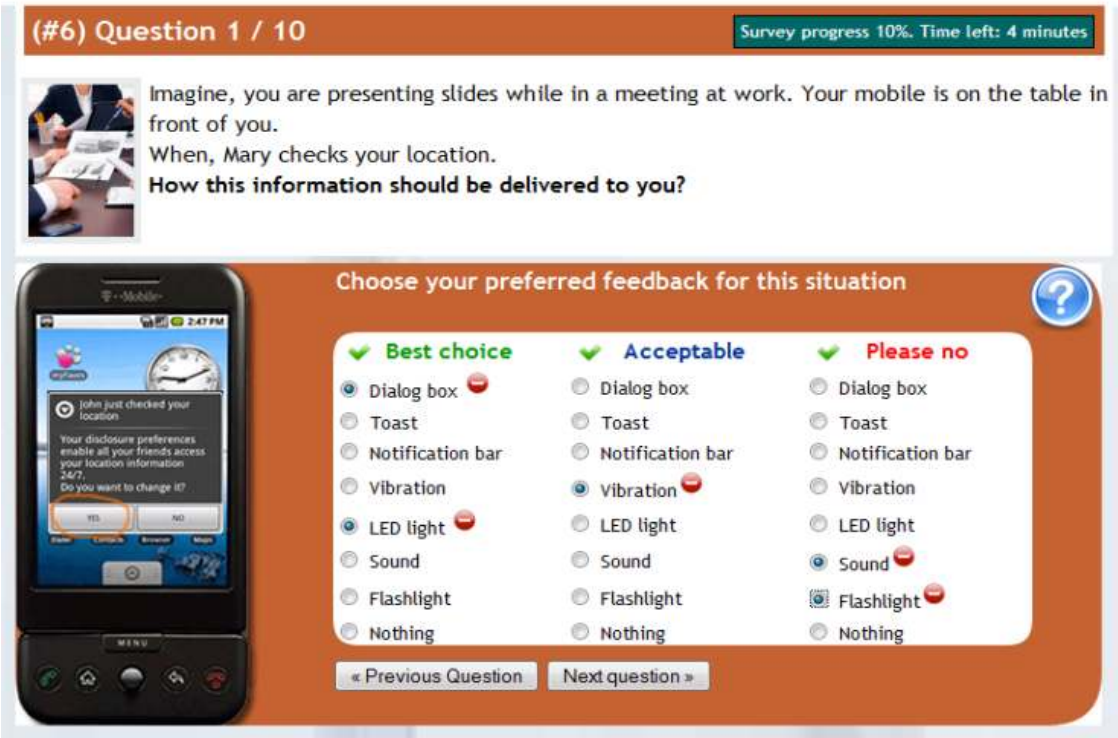


Figure 6-4. Screenshot of the survey presenting the question view. In this view the user is presented with the example scenario supported by the visual representation. Underneath, the user could see a mobile device, in which he can preview how the notification looks like in the real world. The last section allows the user to assign the notification of his choice to one of the three options.

Since mobile interfaces for the real-time feedback proposed in section 3.4.1 were developed for the Android platform, we were aware that many people might not be familiar with Android at the time of the study (early 2010 when Android was not a very popular platform yet). Because

we did not want to limit our participants only to Android users, we used short videos to present how each interface works on the mobile device. Before the user could proceed to the questions, he was asked to read information about each interface and watch a short video presenting its functionality. We also added a video preview option in the answers section so users could see the interface working while answering the question, just by clicking on its name on the list. A screenshot of the survey is presented in Figure 6-4.

6.4.3. Participants

We launched our online survey in February 2010 and advertised our research through word of mouth, social networking sites (especially Facebook and Twitter) and location-sharing applications such as foursquare and Brightkite. We raffled a £45 gift voucher as an incentive to take part in the study.

A total of 3136 people started the survey. We discarded the data of all respondents that completed the survey in less than 4 minutes or did not provide answers to 10 scenarios. Due to the number of questions and instructions it was impossible to complete the study in less than 4 minutes, unless the respondent was already familiar with the interfaces and did not need any training. The following findings are from the 216 surveys that remained which give 2160 users' preferences for the real-time feedback in different situations.

The gender ratio of our respondents was 3-1 male to female. The age demographic showed that 46% (101) of all respondents were in their twenties, 29% (63) were aged between 31 and 40, 21% (45) over 41, and 3% (7) under 20 years old. Only one user was aged over 60. Over 60% of all participants were active users of location sharing applications, mainly foursquare, Brightkite, Gowalla and Google Latitude. Interestingly, some of the respondents mentioned Twitter as location-sharing service. Detailed demographics are presented in the Figure 6-5.

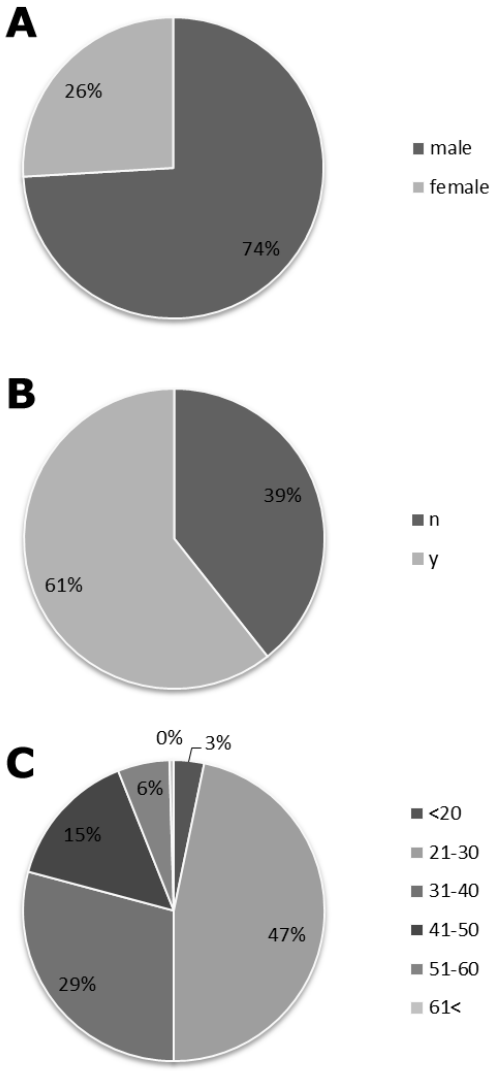


Figure 6-5. Survey demographics. Chart A presents gender information; chart B shows previous experience with location sharing services (y – user uses location sharing services, n – user has never used a location sharing services); and chart C shows age demographics.

6.4.4. Results

The main goal of this work was to derive initial rules, which would minimize the negative impact on users' experience in the field trial described in section 6.5. We also wanted to minimize the number of participants that could potentially withdraw from the study due to the system delivering inappropriate early feedback. We mapped each scenario into the context model (set of contextual variables describing the situation that is supported by our system,

presented in Contextual variables used to design scenarios for the survey.). We then used statistical models to generalize users' preferences (data collected through the survey) and assign the most appropriate representation for real-time feedback to the context model. We encoded generalized preferences as rules in the form of a decision table, which was used in the field evaluation of the technology. A rule is represented as a list of contextual variables *C(value)* and users' feedback preferences $RTF_{OPTION}(I)$, where *I* represents an interface, or group of interfaces. Note that the user could assign one interface or more to the specific scenario. An example rule template is presented as follows:

$$RULE_n = C_1(x),\ C_2(y),\ C_3(z),\ \ldots,\ C_n(n),\ RTF_{BEST}(I_a),\ RTF_{ACCEPTABLE}(I_b),\ RTF_{UNACCTEPTABLE}(I_c)$$

An example rule from the decision table representing users' preferences for scenario number four looks as follows:

$$RULE_3 = Pv(y),\ C(y),\ Pin(y),\ R(friends),\ L(outside),\ A(\text{'standing'}),\ MA(\text{'playing a game'}),\ RTF_{BEST}(VIB),\ RTF_{ACCEPTABLE}(NB),\ RTF_{UNACCTEPTABLE}(DIA)$$

Sometimes people assigned a similar number of 'best' answers to different interfaces, therefore we need to find a way of finding the best one. Since we asked users to assign more than one representation to a given option (best, acceptable and unacceptable) we decided to find the best feedback representation for the given context using the following formula: Best feedback representation = number of 'best' answers + 0.5 * number of 'acceptable' answers. The weight of 'acceptable' answers (0.5) was halved relative to the best answer in order to reduce its relative influence. It allowed us to find the best representation for the given situation and maintain unobtrusiveness of the notification.

Since evidence from the literature shows that users' preferences expressed in surveys might vary from the actual behaviour (Acquisti and Grossklags 2005) we do not report findings from the survey as ideal rules for the real-time feedback delivery. Therefore the role of rules derived

in this study is to shorten the training period and minimize a negative impact of intrusive notifications on user experience in the initial phase of the next field trial of context-aware real-time feedback.

Thus the main goal of this data was to collect initial users' preferences to use as default real-time feedback delivery rules. We also used this data to find the most appropriate learning algorithm for the field trial. Based on the data collected we examined several learning algorithms in order to find the most suitable method for adapting types of the notification to the context. We ran a 10-fold cross validation of our dataset using five different algorithms: Id3, J48, LAD, NBT and REP. The 10-fold cross validation involves randomly splitting the training dataset into 10 subsets (folds) of approximately equal size, preserving proportions of the original dataset. Then the algorithm is trained using nine (out of ten) folds and an error rate is calculated by testing on the remaining one. The process is repeated 10 times for each of the 10 folds. The cross-validation estimate of accuracy is returned as an average of correct classifications from each test (Kohavi 1995).

This analysis helped us identify the J48 implementation of C4.5 algorithm (Quinlan 1993) as the most suitable learning method for our dataset. This algorithm was further incorporated into the Buddy Tracker system.

6.5. Study 2

Once context-awareness and machine learning were implemented into Buddy Tracker and initial rules describing users' preferences for real-time feedback in a specific context were derived from the survey described in the previous section, we were ready to test our technology in the real-world. We conducted a field trial aimed at evaluating the effectiveness of context-awareness and machine learning at improving the usability of the real-time feedback.

6.5.1. Study Objectives

Our main objective here was to see if the latest enhancements made to the Buddy Tracker have an impact on users' experience and acceptance of the technology. We were also interested in

assessing whether associating contextual factors with users' preferences can minimize the intrusiveness while maximizing the effectiveness of real-time notifications. Intrusiveness was the biggest criticism to this technology reported by participants of our previous studies (see Chapter 4).

6.5.2. Method

The study spanned a total of 3 weeks and was split into two phases. During the first phase we collected data about individuals' preferences in order to create a training dataset for the learning engine. This phase lasted two weeks. In the first phase we used rules derived from the survey described in the previous section.

In the second phase, lasting one week, we introduced real-time feedback notifications that were based on output from the learning engine. This was the only difference between the two phases.

During both phases users received a real-time feedback notification every time someone looked-up their location; 5 minutes later they received a text message with a unique URL to the experience sampling questionnaire (see Figure 6-6). We decided to use SMS as a delivery method for ESM questionnaires because our previous experience showed that mobile phone users have developed their own strategies for handling interruptions caused by incoming messages (Jedrzejczyk et al. 2010a). It has been recognized as an appropriate way of notifying users, people could also easily ignore that if they could not provide feedback at the time. Since both real-time feedback and incoming SMS notification were sent through the same channel, we decided to send ESM questionnaires 5 minutes after the notification event in order to make sure that people do respond to the notification event rather to the ESM notification, which could cause a bias to our results. Five minutes were short enough, so the user could recall the real-time feedback notification and his reaction; at the same time it was long enough to minimize the confusion caused by the notification of incoming SMS message.

6.5.2.1. Experience Sampling Method

The experience sampling method (ESM) belongs to the wider group of diary methods (Bolger, Davis, and Rafaeli 2003) used to capture user experiences in a natural setting. Initially, the method was used in psychology, now is widely used in HCI and privacy research (Anthony, Henderson, and Kotz 2007; Mancini et al. 2009; Consolvo et al. 2005).

Since our research requires user input in order to learn from the behaviour we found this method the most appropriate for collecting data about users' reactions to the real-time feedback technology. We implemented a mobile version of ESM that allowed us to automatically send ESM questionnaires when the event occurs and automatically feed users' feedback into the learning engine. It allowed us to implement incremental learning in the second phase. By incremental learning we mean that the user's predictive model of real-time feedback preferences was re-created automatically after the user submitted the questionnaire. Mobile questionnaires were also less problematic for our participants, as we used the same device to collect users' feedback and run the Buddy Tracker application. They did not have to carry a diary or any other recording device.

Collecting data through ESM requires commitment on the part of the participants, as they need to spend a significant amount of time to fill in the questionnaires. Therefore our questionnaire does not require any typing; the users only chose predefined options by taping on the answer. In the final version of the questionnaire users were asked to (1) score the accuracy of location where the system logged them at the time of sending the notification; (2) say if they noticed the notification; and (3) tell us if the notification used was appropriate for the given situation.

Similarly to the survey presented in the previous section, users had three options to score the notifications: YES (best choice), OK (acceptable) and NO (unacceptable notification). Users were asked to suggest a more appropriate notification for the given situation when they answered OK or NO. A drop down list of available types of feedback appeared, from which

users could choose a better option. Information from questionnaires was used by the learning engine to improve the accuracy of later notifications.

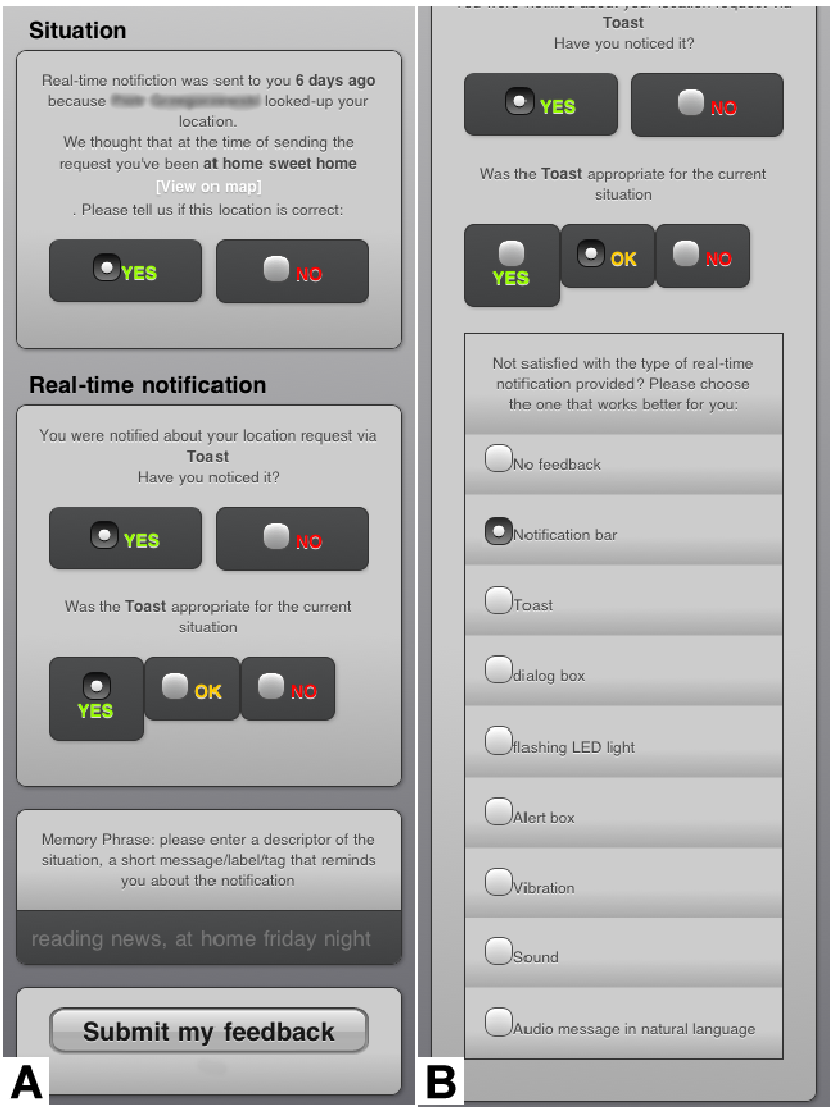


Figure 6-6. (A) Feedback form used to collect the data form users. Form consisted of two main section: situation and real-time notification. Users could also specify a memory-phrase, a unique description that could remind him about the situation (Mancini et al. 2009). (B) Expanded view, presents additional drop down list of feedback types, which enabled users to instruct the system what would be more appropriate feedback representation in the given context.

6.5.2.2. Extending Experience Sampling with a Memory Phrase

Since ESM was used to collect information about users' preferences for the technology, we could not expect that participants remember everything about their experience when they

received the notification. The ESM questionnaire allowed us to answer *what* interface worked or not in the given scenario, but we also we seek a way for improving our chance of understanding the *why* question. To this end we implemented an optional feature in the questionnaire, called *memory phrase*, a textual description to help participants recollect the specific situation in detail during post study interviews.

The Memory Phrase was first described by Mancini et al. in the study of mobile Facebook users privacy concerns (Mancini et al. 2009). This method has been proved efficient at triggering users' memory about past events. An example memory phrase entered by the user is presented in the Figure 6-6 A: "*reading news, at home Friday night*". The personal nature of the memory phrase makes it a powerful memory trigger. Users could assign their own descriptor to the situation, which is capable of reminding the user about the event but most importantly the memory phrase is "*capable of triggering a connection to the experience*" (Mancini et al. 2009).

6.5.2.3. Post Study Interviews

At the end of the field trial, participants individually took part in post-study debriefing sessions. Interviews aimed to explore the participants' decision making process, i.e. why a particular type of notification was deemed to be preferable over another; or why participants expressed different preferences even when their context appeared to be the same (from the system's point of view). The materials used during debriefing sessions included:

i. users' answers to experience sampling questionnaires, including memory phrase;
ii. system logs containing activities users' had undertaken during the study; and
iii. results of the initial analysis performed on users' data, such as situations when people noticed a notification but scored it negatively, or situations when people answered differently in the same context.

6.5.3. Participants and Devices

We recruited 15 participants (3 females and 12 males) from a variety of backgrounds and included a truck driver, a dental surgery assistant, a PhD student, a logistics officer, a sales

manager, a graphic designer, curriculum managers, software developers, a CEO of a big company, a flight lieutenant from the Royal Air Force and an unemployed person. We did not want to limit our participants to one specific group due to the similarities in the life pattern, which might have an impact on our results. Therefore we aimed to recruit a diverse group of people living according to different patterns and working in different places and with different people. For example, real-time feedback preferences might vary between the 9AM to 5PM office worker and a truck driver.

Participants could invite their friends to take part in the study as *requesting users*. These used our web or iPhone app to check on their friends' location, but did not provide us any data about the real-time feedback, as their location was not being tracked or requested. Therefore we do not consider requesting users participants, as they were only requesting locations of their friends in order to increase the number of realistic real-time notifications presented to participants actively sharing their location. Participants and their *requesting users* were split into seven groups. Most of the participants were based in the UK, one participant was based in Cyprus, one in Poland and one visited Vietnam during the study.

6.5.3.1. Setup

Prior to the study participants were asked to complete the Westin Harris privacy survey (Taylor 2003). We also asked our participants to specify a set of meaningful locations, i.e. home or office, using the location manager module developed for the purpose of this study (see Figure 6-7). Each user could create their own database of locations, assign them to one of the existing categories, which we borrowed from (Khalil and Connelly 2006); or specify their own label for place.

Users could also create areas by specifying a radius between 50 yards and 2 miles. This information was used to correlate users' preferences with places and improve the learning process. Participants were instructed about additional controls provided by the system, such as quiet hours, that allowed them to create time periods when they did not want to be disturbed by

the system. Users could also specify what types of notifications could be used (see Figure 6-2 B and Figure 6-2 C), we encouraged our participants to enable all feedback interfaces and let the system learn from their behaviour. We also asked our participants to check if their mobile device met the requirements of the system, such as checking if TTS (Text To Speech) functionality was installed on their phone.

Four participants did not have their own Android device but they accepted devices from us, and used them as their main phones for the period of this study.

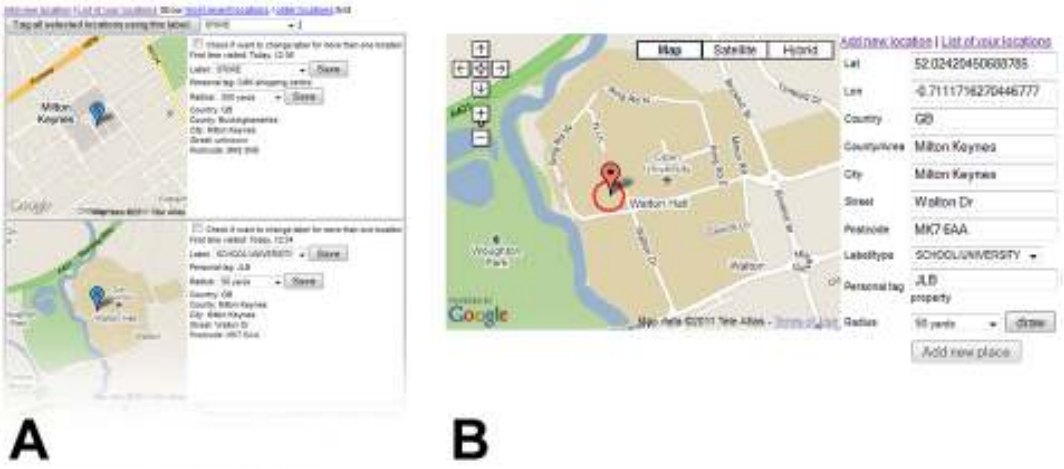


Figure 6-7. Location manager module. Prior to the study users were asked to create a list of the most visited locations, i.e. work place, gym, shopping center or home. A presents a list of already defined locations; B presents the form used by participants to define a new place.

Participants were informed about the purpose of the study and information collected. We also made them aware of the negative implications of participating, such as reduced battery life. Extended batteries were offered for those participants who were not satisfied with the battery life on their phone. We also explained that we had instrumented the interface to collect information about any tracking events. Participants were offered a £40 (approx. $65) gift certificate for completing the 3-week study including post-study interviews, each lasting 30-90 minutes. Our research protocol was approved by our institution's Human Research Ethics Committee.

6.5.4. Findings

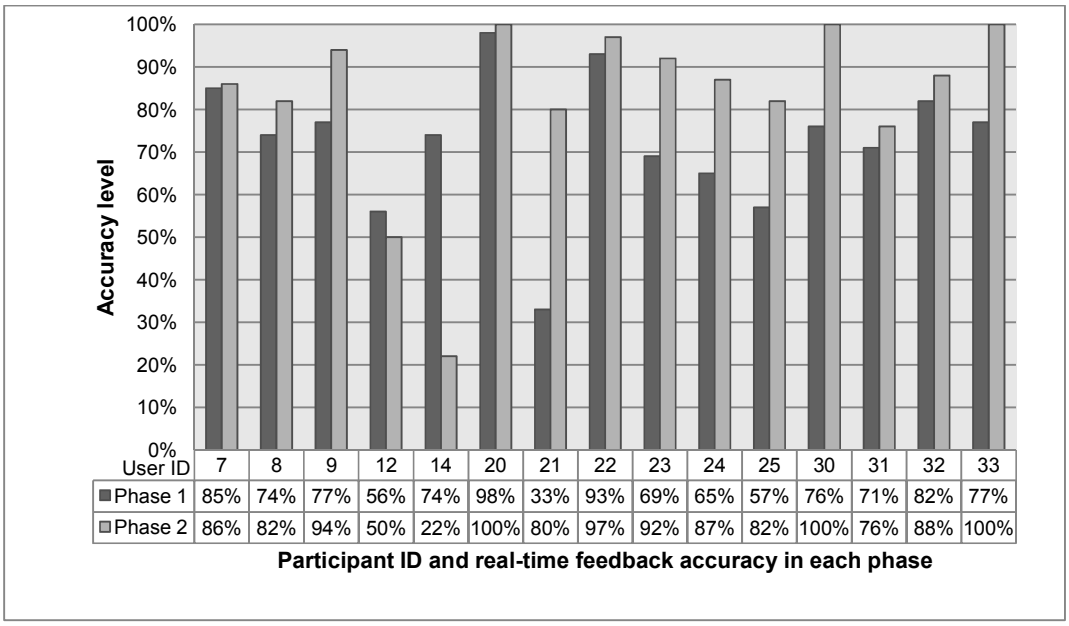
Over the period of 3 weeks the system sent 3937 experience sampling questionnaires (same as the number of real-time feedback notifications), of which 2192 were answered successfully. Participants started but did not complete 114 questionnaires and 809 were ignored by participants. The overall participation rate, calculated as the percentage of successfully completed questionnaires, was 56%. Participants answered an average of 146.6 questionnaires (median=137). The most active participant completed 257 (user 7) questionnaires and the least active only 19 (user 32).

In this section we describe the main findings of our study. We use both quantitative and qualitative data collected during the study to report our findings. We begin by evaluating the efficiency of the context-awareness and learning engine at providing an unobtrusive and effective notification mechanism. Then we examine the effect of selected contextual information on the system's performance and users' acceptance of real-time feedback technology. We also discuss social issues related to real-time feedback, such as how the users' job affected the accuracy of notifications and discuss issues related to mobile privacy. We also look at how the group's privacy can be violated by our technology and how people overcame those problems in their life.

6.5.4.1. Acceptance of the Context-Aware Feedback

After examining the users' answers we noticed that 13 participants experienced an increase in the system's accuracy in the second phase of the study. By accuracy we mean the appropriateness of the notification used for the given situation. Only two users' reported lower accuracy in the second phase. User 12 and user 14 experienced 5% and 51% drop in the accuracy of notifications respectively (see Figure 6-8). We found that the system could not adapt to user 12 as he kept changing his rules due to his unpredictable circumstances and social context (he was a sales person travelling across the country). We describe the impact of lifestyle on the system's performance later in the dissertation. Additionally, the low accuracy of user 14 is the consequence of unexpected problems he experienced in the last phase; he could only

participate for one day during the final week. For this reason we have omitted user 14 when calculating the average accuracy of the system.



User ID	7	8	9	12	14	20	21	22	23	24	25	30	31	32	33
Phase 1	85%	74%	77%	56%	74%	98%	33%	93%	69%	65%	57%	76%	71%	82%	77%
Phase 2	86%	82%	94%	50%	22%	100%	80%	97%	92%	87%	82%	100%	76%	88%	100%

Figure 6-8. Accuracy of notifications during two phases of the study. Chart shows a percentage of positive feedback given by each user during 2 phases of the study.

The average accuracy of feedback delivery was 72.45% in the first phase, and 86.75% in the second phase. An average increase in the system's performance was 14%, the maximum increase was 46%. Surprisingly the user with the higher increase (user 21) did not notice a significant change in the system's performance.

6.5.4.2. The Impact of Learning on User Experience

Only a few users reported that they actually noticed an improvement in the system's accuracy. Some users were able to precisely point out the moment when the system started to provide more accurate feedback notifications. We found that better accuracy contributed to greater reliability on the part of the system and trust on the part of the user.

During post-study interviews, users reported that they felt more confident and comfortable using the system in the second phase. We found that awareness of the notification was a contributing

factor towards the acceptance of this technology. In other words, the more notifications participants noticed, the more positive their feedback was. Figure 6-9 illustrates the correlation between the awareness rate and acceptance rate.

We observed 49 cases when people noticed a notification but scored it negatively, 42 in the first phase and 7 in the second phase. Of these, 37 were caused by more intrusive notifications (natural language, sound and vibration). Of these 33 were in the first phase and 4 in the second phase. This shows that the learning system helped us minimize the intrusiveness of this technology and increase the acceptance of real-time feedback notifications. We observed an 83% drop in the number of intrusive notifications presented to users in phase 2. During post-study interviews participants reported that most of these negative answers were the consequence of unpleasant situations caused by the system, for example, if natural language notification was used during a meeting or while having dinner with friends.

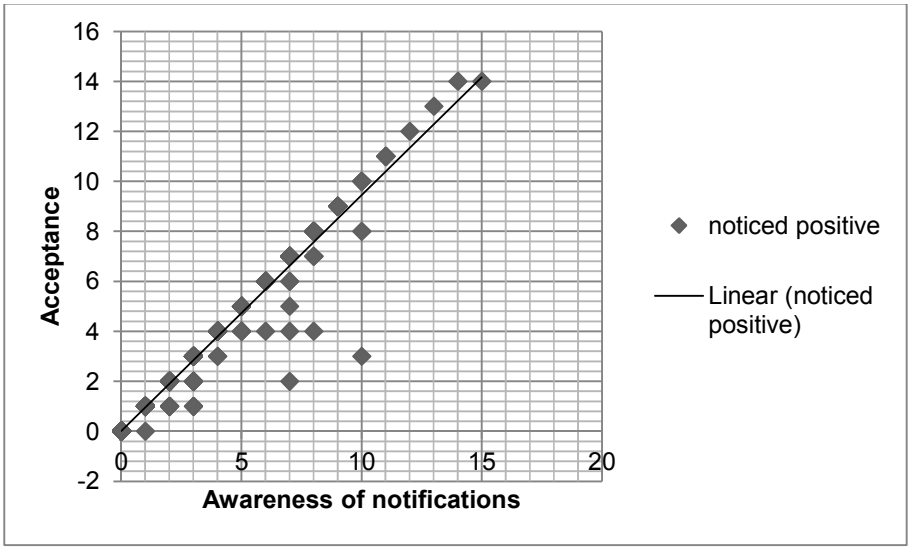


Figure 6-9. Correlation between the number of noticed notifications (awareness of notifications); and positive feedback (diamond markers). This chart suggests that acceptance of technology is correlated with awareness of notifications (correlation rate = 0.9788).

The awareness rate was increased by 7.29% in the second phase (46.98%). By awareness rate we mean the percentage of noticed notifications. This means that the learning system helped us

to not only increase the unobtrusiveness but also increase the efficiency of information delivery, which had a positive impact on usability and users' acceptance of the technology. The increased awareness contributed towards greater trustworthiness and reliability of the system.

Since the figures presented above are results of the machine learning module, it is important to recall that users had an option to manually change types of notifications used by the system. Users' changes in their preferences were also used to determine what feedback representation was the most acceptable in the context. We observed that especially at the beginning of the study participants were playing with the system. They were switching on and off selected feedback representations to test if they can control the notification mechanism. Half of our participants decided to keep selected feedback representations off for a longer period, i.e. three users switched off natural language completely for the most time of the study, user 8 did not like the security alert (dialog box presenting aggregated information about location requests made on him, see Figure 3-2 A). Very often users' decisions were related to their personal preferences, i.e. participants that switched off natural language feedback reported that they did not like the voice generated by the technology. We noticed that one participant kept his phone in the silent mode most of the time, which also had an impact on the notification system – it minimized the set of available notifications by disabling auditory feedback. We also observed situations, when users changed their settings for a limited amount of time (i.e. one switched the vibration off for 5 hours).

By implementing machine learning and context-awareness in Buddy Tracker we aimed to develop an intelligent notification mechanism for real-time feedback. Results of the field trial show that this approach helped us achieve higher accuracy and lower intrusiveness, which was the main shortcoming of real-time feedback technology reported in previous studies (see Chapter 4 and Chapter 5). One could argue that manual settings might bias our results and make the effectiveness of our system elusive because the user could manually switch off the most invasive notifications (i.e. sound). However, it is important to mention that users' scores were made based on a several criteria such as intrusiveness, perceptibility, meaningfulness or

effectiveness. The goal of using the learning system was not only to minimize the intrusiveness but also increase user's awareness of notifications, which could not be achieved otherwise. Manual control is also required due to the flexibility of the system, which allows the user to control the system thus contribute towards the greater trust.

6.5.4.3. Effect of Location on Acceptance and Awareness

Figure 6-10 shows the distribution of users' locations at the time when they received real-time feedback notifications. Most of the time participants received notifications while they were at home, at work or in an unknown place. The chart suggests that there were only a few situations when participants were notified about look-up events while at a store, pub or in the library. However, many of these locations are covered in the other/unknown group.

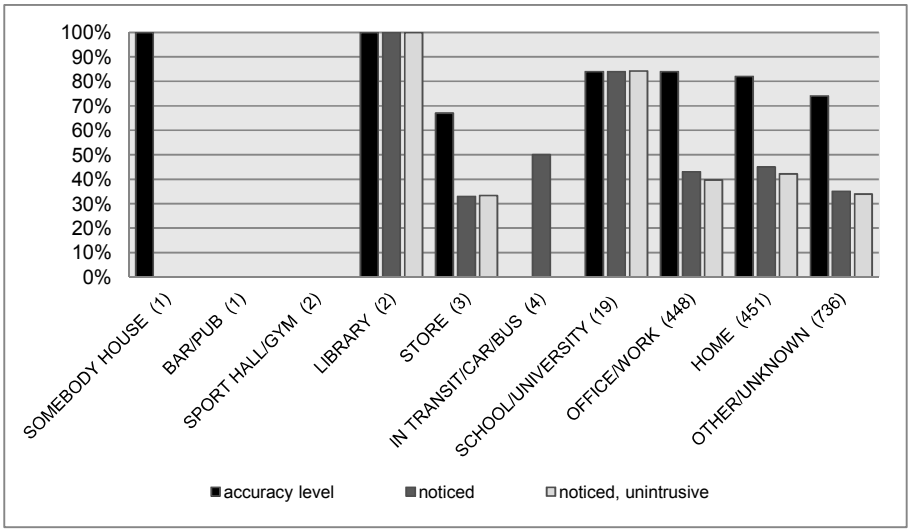


Figure 6-10. System performance vs. location. This chart presents the accuracy of notifications at different locations (black bar), percentage of noticed notifications (dark grey bar) and level of unobtrusiveness (light grey bar). The number of situations when users received a real-time feedback at the location is shown in parentheses.

Prior to the study, participants found it difficult to specify all the places they were likely to visit during the study, therefore we cannot perform a detailed analysis of users' preferences for the real-time feedback in relation to the contextual factor location. Instead, to explore the effect of

location on users' preferences, we use the two most frequent known locations, namely home and work.

The usage rate (number of situations when users actively used their phone at the time a notification was received) was higher at home, which suggests why toast (TOA) and notification bar (NB) visualizations were preferred at home. We observed that for 47% of notifications delivered while users were at home, the participants were using their phone at the time. The usage rate at work was 32%. The most commonly used feedback representations at work were LED and vibration (VIB). Surprisingly, we did not observe a big difference in the acceptance rate of natural language notifications (NL) between the two locations (see Figure 6-11). Another interesting observation is that 95% of accepted NL notifications at work were reported by office workers with more than 10 people in the office. However, only three positive NL notifications, when at work, were reported by the participant who was a truck driver.

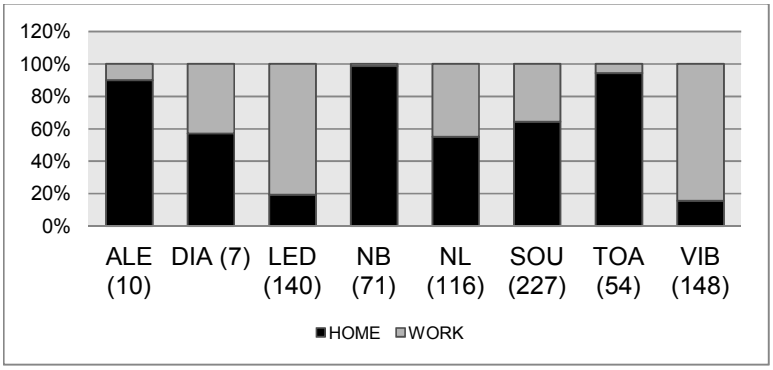


Figure 6-11. Users' preferences for real-time notifications at home and work using different methods (abbreviated). This chart shows the percentage of positively scored notifications for two most frequent known locations with the total number of situations for each method shown in parentheses.

Another interesting observation is that people are likely to receive a more intrusive notification for its entertainment value. For example, we observed a situation in which the user was at the restaurant with his girlfriend. The system used a natural language to notify him about the location lookup made on him. While, the restaurant is a specific type of place, in which certain

social norms govern our behaviour, he actually scored this notification as an appropriate way of delivering real-time feedback. Results from our survey (see Figure 6-12) suggest that in the restaurant the system should not use sound to provide a feedback, however a real-life experience shows that people sometimes compromise the intrusiveness of technology for a little bit of fun and entertainment.

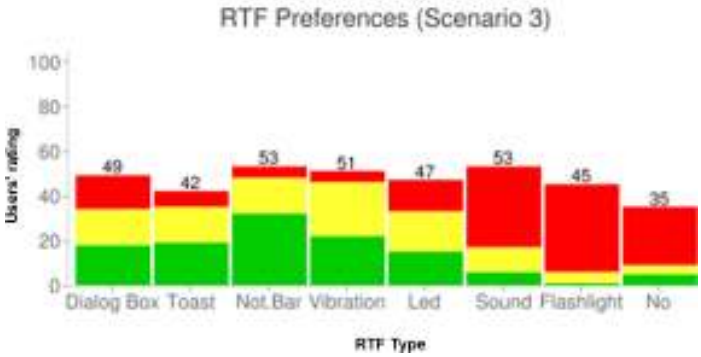


Figure 6-12. Users preferences for scenario number three as reported in the survey (see section 6.4). This chart shows that sound is not an appropriate for the situation (User at the restaurant, browsing the Internet on his mobile while waiting for a meal), however experience from the field trial suggests that people are likely to accept more intrusive notifications for their entertainment value.

6.5.4.4. Effect of Mobile Activity on Acceptance

We noted that our participants used a range of 24 different applications, at the time at which a real-time feedback notification was received. Mostly these were social and communication applications. We examined the decision tree models generated for each user by the learning algorithm and found that current mobile activity was the common node for 10 users.

Our analysis shows that mobile activity is an important element of context, which can be used to determine the most appropriate type of notification while the phone is in use. This is especially important for the system designers, as it can minimize the contextual information that must be collected through battery-consuming sensors.

One interesting observation was that even less intrusive notifications, such as toast (see Figure 6-13), are perceived as annoying while watching videos, browsing the Internet or typing. We

observed that even people with a pragmatic approach to the technology did not like to be disturbed when performing one of the above tasks.

Figure 6-13. Toast notification, a small, semitransparent floating window appearing on the screen and disappearing after 2 seconds. Pictures presents toast displayed to the user while typing a number. (a) Less usable and more intrusive, toast in the first phase placed in the middle of the screen; (b) more usable, toast in the second phase displayed in the bottom of the screen, a picture of requester was presented in the second phase.

In the second phase we changed the position of the toast notification, and aligned it to the bottom of the screen to see if the main factor was really the current task, or if we could solve this problem by changing the position of the notification (see Figure 6-13 B). In the second phase we also displayed a picture of the requester to minimize the cognitive effort of assimilating the information. We observed that in the second phase that bottom alignment had a positive effect on user experience while browsing the Internet; no negative feedback for toast notifications were reported in the second phase.

Users were not presented with toast notifications while watching videos in the second phase. However data collected during interviews confirms that alignment of the notification and the new design has a positive effect on user experience, but there are situations in which the system

should respect people's privacy and not display any visual notification that covers the working area of the screen (i.e. while people type text or watch videos).

6.5.4.5. Lifestyle and Personality vs. System's Performance

Our study suggests that real-time feedback technology is not for everyone. Some people are just not interested in who viewed their location. Others do not seem to like to know this information in real time (however, this attitude might change based on who's checking and how important it is). Finally, others report more practical reasons for their low level of acceptance, such as battery consumption.

We looked at the acceptance rate in relation to users' occupation and other life patterns. We found that it is more difficult to provide both an unobtrusive and effective notification system for mobile occupations (for example in cases such as those of the truck driver or sales person). We observed that a proximity sensor showing the distance between the owner and the mobile device would solve many performance problems in the case of highly mobile users. For example: mobile participants (a truck driver and a sales person) very often missed notifications provided using audible natural language. When asked about particular situations during the interview session, they reported that at the time of the feedback delivery they had left phone in the car, which made the usefulness of sound notification elusive.

We also found that system acceptance depends on two main factors: intrusiveness of the method of delivery and effectiveness (awareness of notifications). Although effectiveness is a positive factor contributing to the acceptance of real-time feedback technology, nevertheless it is not important for everyone. We found that effectiveness is more important for people with a pragmatic approach towards technology while intrusiveness is more important for people with a more opportunistic attitude. There is a stronger need for historical feedback in the second group than there is in the first group.

6.5.4.6. Attitudes towards location sharing technologies

Amongst the 15 participants taking part in our study only 4 had prior experience with location sharing and tracking technologies (we do not count GPS/SatNav as location tracking as it does not involve a third party access to one's location). When asked about their attitude towards the Buddy Tracker technology in the debriefing interviews, participants reported different reasons for sharing, or not, their location and for tracking others.

The most common reasons for using the Buddy Tracker was to support coordination; ensure a loved one's safety, e.g., tracking children, monitoring a partner's long journey; or just curiosity. Additionally, some users reported using Buddy Tracker and the real-time feedback technology as a game playing activity: for example, one of the participants reported that *"when someone looks me up, I look him up in return*".

Some people used the system to check where they have been or track their running activities. One of our participants mentioned that very often he shares his tracks with other people having interest in sport. He called that *conversational sharing*, during which he discusses his achievements using location data.

Despite the socially-oriented aspects of using location sharing technologies, we found that interest in location sharing might have a non-social background. We noticed that one of our participants used the technology because he likes maps. A real-time map view allowed him to monitor how his buddies travelled between their work and home destinations. People also used Buddy Tracker to coordinate their life, i.e. check if the person is "contactable" (for example, one of our participants was in Vietnam during the study, and sometimes had problems with connectivity) or to express feelings (for example, a female participant tracked her partner via Buddy Tracker to coordinate her cooking with her partner's journey home in order impress him with a hot dinner upon his arrival).

The most common reasons for not using location sharing technologies are lack of interest in someone else's life, ethical issues related to tracking and what appeared to be the less socially-

orientated personality of some participants. People also described several technical problems that had an impact on their acceptance of this technology, such as battery life and accuracy of location, both of which make the system less useful. Those who reported negative aspects of location sharing were mainly people with a utilitarian and pragmatic approach to location sharing.

6.5.4.7. Real-Time Feedback and Mobile Privacy

We designed the real-time feedback technology as the tool for supporting awareness, which can help people understand the actual data flow and help them make more informed privacy decisions. What we mean by personal privacy in this context is the processes by which individuals selectively disclose personal information (Hong 2005). However there is much more to privacy than management and rules setting, and this study sheds new light on aspects of privacy specific to mobility and mobile technology. We revealed several mobility issues that have an impact on our personal privacy and sense of solitude.

Mobile phones are not communication-only devices anymore; our participants described their devices as "*a computer that happens to be a phone*" or an "*information device*". Some of them used their phone only for communication, but most of our participants used their phones for many different purposes, such as entertainment, listening to music, personal organization, networking, checking emails, news reading or physical and virtual navigation. Most of our participants were in the close proximity of their phones 24 hours a day. Only 4 participants reported that they keep their phone in a bag, in the kitchen or in the living room overnight. Understanding the context in which people use their devices, seems to be very important when analyzing the privacy impact of real-time feedback technologies, and any notification mechanisms in general.

Buddy Tracker used several representations for real-time feedback to minimize the negative effect of notifications such as intrusiveness. However there were situations where even less

intrusive notifications, such as toast, had a negative impact on a users' experience and their sense of privacy.

During the debriefing session we asked one of the participants (female, 28) why she refused the toast notification while she was watching a video on YouTube (prior to that episode she rated this type of notification positively 43 times). She reported that at that moment she was relaxing with her 2 year old son and they were watching television on her phone. The notification was not only annoying but also caused a bit of anger and also affected her sense of privacy as she did not want anything or anyone to disturb her. She tried to dismiss it immediately but she had no control over it, and had to wait 2 seconds before the notification disappeared automatically. When asked about this experience, the user reported that "*there are times when a phone should not disturb and should not act as an information device*".

A similar incident took place with another user (a 28 year-old male student), while he was preparing for his supervision meeting on the next day. He was notified about a location look-up event via audio message in natural language. He remembered this situation as one of the most annoying during the whole study as at that moment he was in a bad mood and needed to withdraw from his surroundings.

The intrusion to one's privacy caused by any notifications, by real-time location feedback, incoming SMS buzz or a ringtone, can have a negative effect and could cause frustration or even embarrassment, all of which have an impact on willingness to accept a technology. On one hand, technology can be useful and desired, on the other hand, it can disturb and affect one's *right be let alone*.

A key observation here is that, when we talk about mobile privacy, we should distinguish between the control layer, supporting the privacy of information generated or shared through the mobile service, and the communication layer, between the service and the user. The latter, responsible for information presentation, can have an impact on different aspects of privacy, for example, intimacy and solitude as the incidents with our participants indicate.

Mobile privacy is not always about protecting information, but it also refers to a mobile service user's state of mind, which determines when and how to interact with the environment. It is also important that in these instances privacy was being violated even if the phone was not being used. In other words, privacy-sensitive applications need to take into consideration the entire context of the user, including his mood. However, given the technological limitations of current mobile platforms, this can only be approximated at this time.

6.5.4.8. Real-Time Feedback and External Image

The post-study interviews revealed that data owners, those that receive a notification when somebody looks-up their location, were concerned about their external image while using the technology. For example, inappropriate notifications presented during a meeting may be regarded as a sign of disrespect to other people and the device owner could be perceived as rude. Therefore the criteria for successful notification include the user's imagined view of how others around them will react. In other words, this means that people choose notifications that would be good for them but also acceptable to people nearby.

Participants reported a number of unpleasant situations when an inappropriate notification was used, for example, when natural language was used during a meeting, it irritated others and embarrassed the user. Disturbing other people was a common example of the technology's intrusiveness. However, 5 people, those with more utilitarian view on location sharing and real-time feedback technology, reported that they would accept more intrusive notifications for improved awareness.

Our study shows that people make judgments about others based on how they use technology. One user reported that "*someone, whose phone is talking all the time does not make a good impression and seems to be unreliable person*", which suggests that delivering notifications too frequently might have an impact on the user's external image.

We asked participants to use all available types of notifications and let the phone learn from their behaviour what the most appropriate notification was in any given context. However, to

provide additional control over real-time feedback and minimize the intrusiveness, Buddy Tracker allowed participants to limit the types of notifications which could be used (interface presented in Figure 6-2 B). We observed that when some participants switched off the most intrusive notifications (vibration, sound and natural language), they did it to protect their reputation by not allowing the technology to do things that are not acceptable in the given environment, e.g., the work place. Many users kept their phone in silent mode, which automatically disabled the audible feedback in the Buddy Tracker.

6.5.5. Discussion

In this section we have presented our work on context-aware real-time feedback, a novel application for supporting awareness in privacy-sensitive mobile applications. Our main objective was to design and develop an unobtrusive notification mechanism empowering users by providing them with information about their location data flow. The real-time feedback supports them in the ongoing process of privacy management and thus helps them to enjoy the social participation afforded by ubiquitous technology with awareness and proactivity. We used rich contextual information and machine learning techniques to adapt the system to each individual in order to improve the acceptance of the technology and minimize the intrusiveness of notifications. The findings of our study show that our approach can significantly minimize the intrusiveness, which has a positive impact on user experience.

Our findings also suggest that designing unobtrusive notifications for ubiquitous technology is a very challenging task due to several factors, such as technological limitations (e.g., battery problems, accelerometer not working while phone in sleep mode, lack of proximity sensor), personal attitudes, occupation type and mental state (e.g., concentration, mood).

We decided to use off the shelf mobile devices in order to increase the realism of the study. Although modern devices are capable of sensing rich information about the users' environment, battery consumption of sensors make it difficult to develop a long-lasting and reliable system. Due to this problem we could not use all available sensors to provide richer contextual clues to

the learning system, e.g., the microphone could not be used to measure the noise level.Our participants reported technical limitations and high battery consumption to be the most negative factors towards the acceptance of the technology. This indicates that current technology is not yet able to provide usable context-awareness.

To the best of our knowledge, our study was the first to explore the use of context-aware notification mechanisms supporting awareness in the field of mobile computing. Our findings indicate that contextual factors are critical in determining a user's reaction to different forms of feedback and that the ability of a device to learn about and adapt to a user's context, afforded by machine learning, can determine the acceptance of real-time feedback technology. Although the study was small and most of our participants were male, our findings provide new insights about the actual impact of real-time feedback technology on mobile privacy and mobile privacy management.

However, our findings also suggest that there is much more to privacy in ubiquitous computing than control and management of data flow. We observed an interesting phenomenon about mobile privacy within the spectrum of human computer interaction. Specifically, that users' acceptance of the technology depends not only on the intrusiveness and effectiveness of notifications from a pragmatic or social perspective, but also on what we might call the users' emotional context, which might include for example their level of concentration, or their need for intimacy or solitude, at notification time. These factors have a significant impact on how users perceive technology, and whether and how they want to be alerted.

The application presented in this chapter uses a client-server architecture, which is not ideal due to potential security problems (i.e. a third party could potentially monitor the traffic to collect data transmitted between the client and the server). Technological improvements in Buddy Tracker's architecture are needed and should include using a client's device for data capture, data storage and learning process in order to minimize privacy and security problems related to

data transfer. One of the next items in our research agenda is to use on-device learning approaches, similar to Wang and Ahmad (Wang and Ahmad 2010).

Despite the positive findings of our study, we need to investigate further how to incorporate machine learning into this type of system in a usable manner. As reported here, we managed to improve the accuracy of notifications and significantly minimize the intrusiveness of the technology. However, similar to work by Sadeh (Sadeh et al. 2009), our methodology required users' feedback to learn new rules, which might be cumbersome.

Although we were able to use an algorithm that is capable of learning rules from a limited data set (hence minimizing user effort), incorporating the learning process into real systems still poses a significant challenge. While people may be willing to give feedback to the system while taking part in an experiment for which they receive compensation, they may not be willing to do the same in an un-controlled setting. Therefore the next step in this research is to explore any links between users' personalities, occupations, and life style in general, and privacy attitudes in order to determine whether an adaptive model for user acceptance of real-time feedback technology can be derived. Concomitantly, new input methods may be required, which will allow us to design more affordable ways of defining learning rules.

6.6. Chapter Summary

In this chapter we presented an online survey, in which we collected users' feedback preferences based on their responses to potential scenarios. We described details of the survey design process and discussed how results of the survey were used in the field trial of context aware real-time feedback technology. Data collected from the survey were also useful in identifying the most suitable learning method for our dataset: the J48 implementation of C4.5 algorithm.

While the survey was a first step towards understanding users' preferences for the real-time feedback, we have further conducted a study investigating the potential of using contextual cues and machine learning to increase the usability of real-time feedback technology. Based on both

quantitative and qualitative data, collected during a 3-week field trial and following debriefing interviews, we reported several novel findings. We showed that machine learning and context-awareness can increase the contextual appropriateness of notifications, which contributes towards greater trust in the system and higher level of comfort, thereby increasing the overall user experience. While we observed a significant drop in the intrusiveness of the system in the second phase, we did not observe a significant increase in the effectiveness of notifications.

We also observed a number of social implications related to real-time feedback technology, such as impact on mobile privacy and social image. Our findings indicate that mobile activity has an impact on users' preferences, and information about users' mobile activity is useful in determining an appropriate notification type for a given context. Although machine learning techniques are efficient at improving user experience, new methods for collecting users' feedback are needed to make the learning process more transparent and more usable in mobile applications.

Chapter 7. Privacy-Shake – Introducing Control

> "*A computer shall not waste your time or require you to do more work than is strictly necessary.*"
>
> Jef Raskin

As stated at the outset, this thesis is concerned with methods for improving feedback and control relating to privacy management in mobile applications. The previous chapters have focused on the former and therefore this chapter tackles the challenge of providing simple coarse grained privacy controls in location-sharing services. Studies described in Chapter 4 and our early work on privacy issues in location-sharing mobile applications described in (Jedrzejczyk et al. 2009) have shown that users of location-sharing systems require an easy way for controlling basic privacy preferences.

Although our work on coarse-grained privacy management interfaces was influenced by our studies, this problem has been noted in earlier work (Lederer et al. 2004). Lederer described "*lacking coarse-grained control*" as one of the five problems in interaction design for privacy-aware systems. Some solutions involving location privacy policies have been suggested for managing location privacy (e.g., (Myles, Friday, and Davies 2003)). However, prior research shows that end-users have difficulties in expressing and setting their privacy preferences (Cranor and Garfinkel 2005; Sadeh et al. 2009).

Setting privacy rules is also a time-consuming process, which many people are unwilling to do until their privacy is violated. Moreover, most known privacy management solutions are based on graphical user interface, and treat privacy management as a main task, while privacy is a very contextual concept. Visual interfaces absorb a user's attention and require the user to grapple with the application while their main goal is to interact with the physical (Robinson, Eslambolchilar, and Jones 2009).

To address this problem, we present "Privacy-Shake", a novel interface for managing coarse grained privacy settings. We describe a prototype that enables users of Buddy Tracker, our location sharing application, to change their privacy preferences by shaking their phone. Users can enable or disable location sharing and change the level of granularity of disclosed location by shaking and sweeping their phone.

In this chapter we present and motivate our work on Privacy-Shake and report on a lab-based evaluation of the interface with 16 participants.

7.1. Motivational Scenario

The example scenario below illustrates a privacy control problem. The scenario is illustrated by the storyboard presented in Figure 7-1.

Bob, our character is walking around the town. It is his wife's birthday, and he wants to buy her a bracelet (Both Bob and his wife use Buddy Tracker to locate each other). He came across his wife's favourite jewellery shop and decided to go in. While shopping he realized she could look up his location via Buddy Tracker and spoil the surprise. Therefore, Bob shakes his phone vertically and then he moves his phone forward, then smiles and continues shopping.

In the above scenario, Bob's action is driven by the temporal need – buying a gift for his wife. While he is normally keen to share his location with wife, in that particular situation he wants to blur his location as it can reveal his activity and spoil the surprise. He is immersed in the physical world and is focused on shopping activities and using visual interface in this context requires Bob to divide his attention between the physical and virtual world. Using a haptic interface allowed him to perform the task quicker, without even looking at the screen.

We see this as a strong motivation to design tools that help users control their privacy settings as a consequence of their daily tasks. The underlying requirement of our coarse-grained privacy management tool is to provide an efficient, heads-up interface for managing location privacy that does not overwhelm configuration over action.

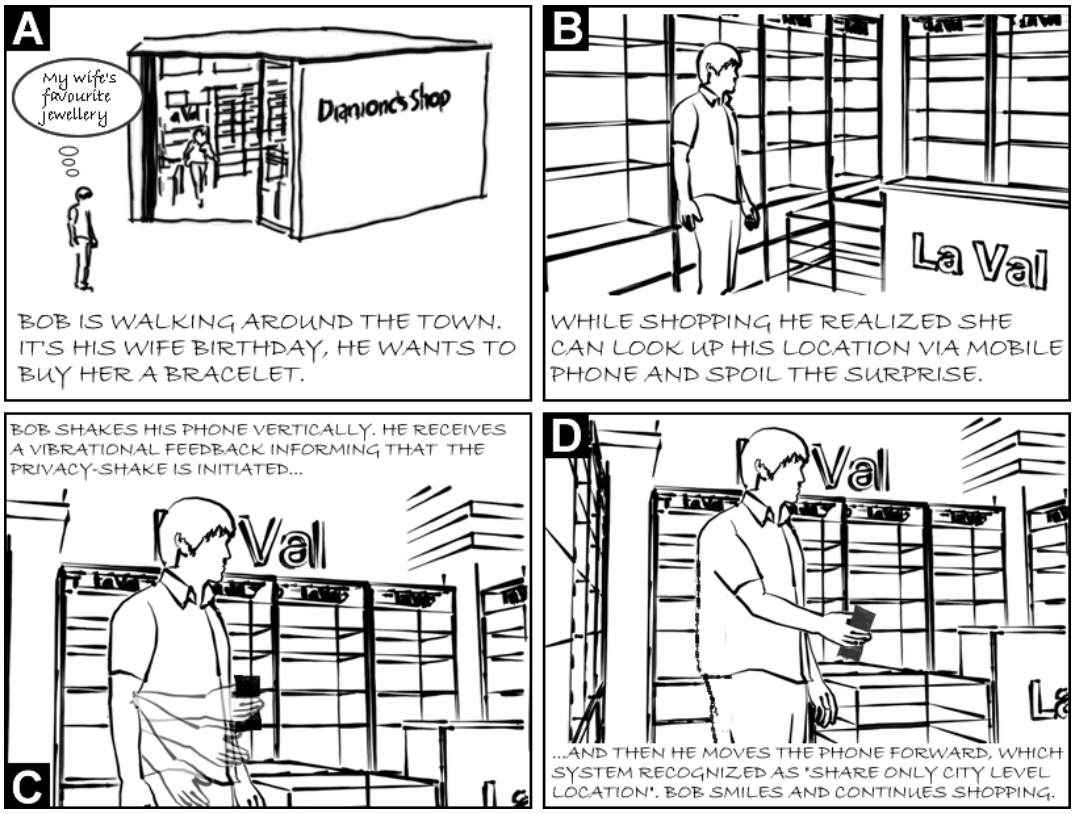


Figure 7-1. An example problem illustrating a need for quick and efficient coarse-grained privacy management interface. (A) Bob, our character is walking around the town. It is his wife's birthday, and he wants to buy her a bracelet (Both Bob and his wife use Buddy Tracker to locate each other). He came across his wife's favourite jewellery shop and decided to come in. (B) While shopping he realized she can look up his location via the Buddy Tracker and spoil the surprise. (C) Then, Bob shakes his phone vertically and next (D) he moves his phone forward while watching bracelets in store. Bob smiles and continues shopping.

7.2. Privacy-Shake Interface

In this section we present Privacy-Shake, a haptic interface for managing coarse-grained privacy preferences in mobile, location-sharing applications. The underlying requirement for our interface is to provide heads-up, non-screen based interaction that allows its users to change their privacy settings quickly in reaction to the situation. Here we describe a technical details of our interface and discuss the design choices for haptic interaction.

7.2.1. Technical Details and Functionality

Lederer suggested that coarse-grained interfaces for location-sharing technologies "*could incorporate both a precision dial (ordinal) and a hide button (binary), so users can either adjust the precision at which their context is disclosed or decidedly halt disclosure*". In our interface we decided to support both ordinal and binary controls for location sharing.

The current prototype supports the following settings: visibility (user can enable/disable location sharing) and granularity (changing the level of granularity of disclosed location from exact location to city level location).

The current prototype of Privacy-Shake is developed in Java and works on Android powered mobile devices. It uses the built in accelerometer to monitor the current position of the device. Our application works in a background in order to save time needed for switching the phone on. While it can significantly decrease the time required for changing privacy settings, the shortcoming of this solution is that the user might change his privacy settings inadvertently. We solved this problem by implementing an *initiation movement*. Initiation movement is a dynamic vertical shake that initiates the Privacy-Shake interface and increases sensitivity of the interface.

7.2.2. Haptic Interaction – Defining a Gesture Language for Expressing Privacy Preferences

Due to the dynamic nature of the mobile device, every action has to be initiated by the initiation movement, a dynamic, vertical shake. This is required to protect the user against any inadvertent changes made to his privacy policy and distinguish the user's action from the noise generated by user's daily movements, e.g. walking, jogging, using a lift. As the system recognizes the movement, vibrational feedback is provided to confirm that the system is ready.

Once the system is initiated, a user can change privacy settings by performing one of the following actions:

- vertical movement enables location sharing (Figure 7-2 A) – we decided to assign a vertical shake to this action as vertical head movement metaphor represents "yes" in the Western countries, by shaking phone vertically the user says "Y*es, I want to share my location with others*";
- horizontal movement (left and right) disables location sharing (Figure 7-2 B), in this movement we used another head gesture metaphor, which in Western countries means "no", in our system horizontal movement means "*No, I do not want to share my location*" ;
- by moving the phone forward, a user can change the granularity of disclosed location to the city level (Figure 7-2 B), this movement uses a distance metaphor, people tend to move their hand forward when pointing a distant objects;
- the user instructs the system to share exact location by moving the phone towards his body (Figure 7-2 A).

Successful action is confirmed by short vibration (the length depends on the action) and optional auditory message (e.g. natural language message "*Anyone can see you*") when the user enables location sharing.

Figure 7-2. Privacy-Shake in action. Arrows present the direction of movement that triggers a privacy-management setting. (A) user enables location sharing by vertical shake; (B) user disables location sharing by sweeping the phone, left-right-left, or right-left-right; (C) user changes the accuracy of disclosed location to city level by increasing the distance between his body and the device; (D) user instructs the system to share his exact location by moving the phone towards his body.

7.3. In-lab Evaluation of Privacy-Shake

We conducted a lab-based trial of the Privacy-Shake interface to evaluate its usability and examine both the potential and vulnerabilities of the current prototype. We were also interested studying people's initial reactions to this novel technology.

7.3.1. Study Objectives

The objective of this study was to examine the potential of haptic interfaces for supporting coarse-grained privacy settings in a mobile, location-sharing application. In particular we were interested in:

i. studying the effectiveness of haptic interfaces in privacy management tasks. Users were asked to conduct a privacy management task on both haptic and graphical user interfaces.
ii. evaluating the performance of Privacy-Shake vs. GUI: the time of performing a task was measured and compared;
iii. exploring users' reactions to the Privacy-Shake concept as a means for controlling coarse-grained privacy settings: users were asked to score the interface against user experience goals;
iv. discovering vulnerabilities of our interface; and
v. validating a gesture-language for privacy management.

7.3.2. Method

Participants were recruited by word of mouth. Each took part in the study individually and each session lasted between 40 and 60 minutes. At the beginning of each session we introduced the Privacy-Shake concept, the purpose of the study and each participant signed a consent form as approved the university's Human Research Ethics Committee. Users were given a short demo of the system and were given a chance to play with the interface prior to performing four privacy management tasks using Privacy-Shake and the Buddy Tracker.

In the next phase of the study, each participant was asked to complete the following privacy management tasks:

Task 1. Enable location sharing using Privacy-Shake.

Task 2. Disable location sharing using Privacy-Shake.

Task 3. Change the granularity of disclosed location to (a) exact location (building level), (b) city level (both using Privacy-Shake).

Task 4. Disable location sharing using the graphical user interface provided in the Buddy Tracker application (users used interface for coarse-grained privacy management presented in the Figure 3-8).

The following measures were recorded:

- time to performing each task – from the time when user started the initiation movement to the vibration confirming the action,
- number of successfully completed tasks,
- time of disabling location sharing using the GUI.

Each participant had three attempts to perform each task.

At the end of each session we asked participants to complete a questionnaire to rate Privacy-Shake against selected usability and user experience goals (Sharp, Rogers, and Preece 2007). We asked our participants about their experience from using the interface and their opinion about the functionality (i.e. how is it to learn how to use Privacy Shake? or how easy is to remember how to use Privacy-Shake?).

7.3.3. Participants and Devices

We recruited 16 participants aged from 23 to 45 for the study, 8 women and 8 men. Most of them had prior experience with motion-capture interaction, mainly from playing the Nintendo

Wii[20]. Eleven participants were graduate students, 4 were recruited from the university's staff and the remaining user was recruited outside the university.

Privacy-Shake was installed on the Android Dream device, also known as G1, which was used in the study. Participants were asked to perform tasks 1-3 on this device. The fourth task, changing visibility in the Buddy Tracker using graphical user interface was conducted on the iPhone.

7.3.4. Findings

We split findings into two sections: usability and user experience, and performance.

Usability and User Experience

Most of our participants reported that using Privacy-Shake is enjoyable experience that brings a little bit of fun into the privacy management tasks. Twelve participants reported that learning how to use the Privacy-Shake was easy (2 users reported that it was difficult), 12 of them said that it is also easy to remember how to use it, as the interaction is simple and intuitive. Participants reported that *yes* and *no* metaphors for binary settings and *proximity* and *distance* metaphors for granularity were simple to learn and remember.

However, four users said that they would not like to use it due to the awkwardness of the interface and potential harm it may cause, e.g. accidentally pushing people in a crowded bus. A similar observation was described by Rico and Brewster (Rico and Brewster 2010).

Four participants reported that using Privacy-Shake was annoying and six of them said that it caused frustration, which is related to the problems their experienced with the interface. Users' ratings for Privacy-Shake are presented in the Figure 7-3 below.

[20] "Wii – Official Website at Nintendo", http://www.nintendo.com/wii [Accessed: April 23, 2012]

Using Privacy-Shake is...	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Enjoyable	0	2	2	7	5
Engaging	0	1	4	6	5
Pleasurable	0	2	5	5	4
Exciting	1	1	6	3	5
Fun	0	2	1	5	8
Boring	9	3	2	0	2
Frustrating	2	3	5	6	0
Annoying	2	5	5	3	1

Figure 7-3. User Experience rating for Privacy-Shake reported by participants.

Performance

Results of performing privacy management tasks using Privacy-Shake and a graphical interface are presented in Figure 7-4. Only five users managed to successfully complete each privacy management task using Privacy-Shake. Three users could not disable their location sharing and nine users had problems changing the granularity of disclosed location. The biggest difficulty users experienced was with task 3b, only three users successfully completed the task three times. More than a half of all attempts to perform this task were unsuccessful (58%). Only task T1 was successfully completed by all users, thirteen participants disabled location sharing using Privacy-Shake and ten of them successfully changed the granularity of disclosed location to city level.

Two users successfully completed 11 of 12 attempts, which was the best result during the study (both female). 58% of all attempts were successful. We observed that females performed slightly better at using Privacy-Shake with 64% efficiency versus 53% for males.

At the time of conducting the study, Privacy-Shake was in early development, and the technology provided a very limited set of gestures. Moreover the accelerometer's sensitivity was set up based on the preferences of researcher developing the interface (author of this thesis, 180 cm tall). We observed that participants with a similar height (around 180 cm) performed better. For example users that performed the best were 170 and 180 cm tall. We also noticed that people's shaking patterns varied, and their performance was affected by the way they held

the phone. This suggests a need for individual calibration, a functionality that allows the user to adjust the interface according to personal preferences.

Although the actual efficiency is not ideal, the comparison between the mean time of performing tasks T2 (6 seconds) and T4 (18 seconds) shows that haptic interface can be successfully used to perform some basic privacy management tasks faster than the traditional GUI.

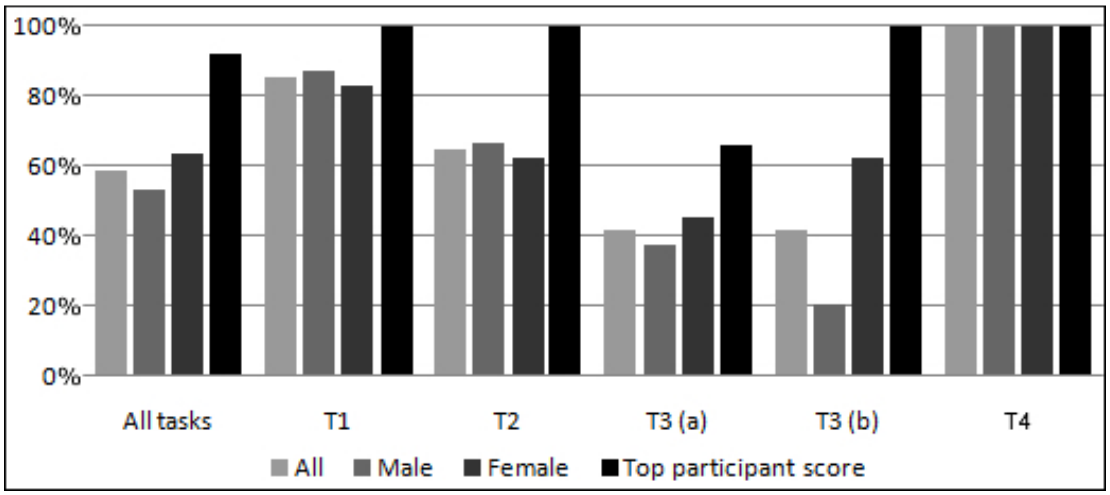


Figure 7-4. Bar chart presents the percentage of successfully completed tasks (efficiency) during the study.

7.3.5. Discussion and Future Work

We presented the concept and initial results of the evaluation of Privacy-Shake, a novel interface for 'heads-up' privacy management. The chosen demographic was not broad, but the study helped us identify both social and technical issues related to the interface. One of the main issues we found were lack of individual calibration and support for more discreet movements, which highlights the future research agenda for our work on Privacy-Shake. Though the actual efficiency is not ideal, the comparison between the mean time of performing tasks T2 (6 seconds) and T4 (18 seconds) shows that haptic interface can be successfully used to perform some basic privacy management tasks faster than the traditional GUI.

The Privacy-Shake concept received generally positive feedback, which encourages us to continue the work on improving the interface and enhancing the user experience. Further work is also needed to extend the functionality of Privacy-Shake by implementing new gestures for managing group settings or expressing more fine-grained preferences.

The study also suggested that some people are not ready for gesture based systems, as some participants reported *awkwardness* of the interface. While some researchers have recently started discussions about the problems of acceptance for gestural interfaces (Montero et al. 2010; Rico and Brewster 2010), new studies aimed at understanding social acceptance of gesture-based interfaces in the presence of other people are needed. This might include a field trial, in which people are asked to perform different types of gestures in public places. Participants' willingness to perform a task in the wild was already studied in (Rico and Brewster 2010), but observing reactions of the other people in the environment would provide new insights into the efficacy and social acceptance of gestural interfaces.

7.4. Chapter Summary

In this chapter we described Privacy-Shake, a gestural interface for managing coarse grained privacy settings in location-sharing mobile applications. We built a prototype that enables users of Buddy Tracker, an example location sharing application, to change their privacy preferences by using gestures. Users can enable or disable location sharing and change the level of granularity of disclosed location by shaking and sweeping their phone.

Our in-lab evaluation of Privacy Shake suggests that the current implementation needs improvement; the mean successful task completion rate was of 58%. However, in the study we identified the main vulnerabilities of the interface and users' practices that will help us improve the interface and make it more efficient.

Since most participants reported a positive attitude towards using the Privacy-Shake, feedback received from participants suggests further research should be aimed at exploring the reactions of others in the environment to users of the interface.

Chapter 8. Summary and Future Work

> "*Privacy is addressed best by giving users methods, mechanisms and interfaces to understand and then shape the system in all three environments.*"
>
> David H. Nguyen and Elizabeth D. Mynatt

8.1. Conclusions

The key problem addressed in this thesis is that current privacy-awareness solutions for socio-technical systems provide insufficient support for natural, face-to-face behaviour, which results in lack of enforcement for social norms. In consequence end-users can not draw upon their real-world (non-digital) experience to structure interactions with others in digital systems. Although ubicomp encompasses social, technical and physical environments, there is no coherence between the face-to-face behaviour and actions in the digital systems.

Drawing from Altman (1975; 1977), Erickson and Kellog (2000); and Bellotti and Sellen (1993) we designed, built and evaluated a privacy awareness system that helps end-users make more informed privacy decisions in ubicomp systems. We proposed real-time feedback as a means for providing *visibility*, *awareness* and *accountability* in Buddy Tracker, a mobile location-sharing service. We argued that real-time feedback helps protect one's privacy by incorporating social norms, which reduces the number of 'unjustifiable' location requests. From our lab-based evaluation, interviews and field investigations of Buddy Tracker we provided both quantitative and qualitative data to support the above hypothesis. Moreover, we designed and built a privacy-awareness system capable of adapting to the user's context, which improves the user experience and has a positive impact on the acceptance of this technology.

Secondly, we said that privacy is a practical problem and managing privacy is a cumbersome task that many people are unwilling to do. Moreover, all known privacy management solutions are based on a graphical user interface, and treat privacy management as a main task, while

privacy is a very contextual concept. Visual interfaces absorb user's attention and require the user to grapple with the application while their main goal is to interact with the physical (Robinson, Eslambolchilar, and Jones 2009).

To address this problem, we described the "Privacy-Shake", a novel interface for managing coarse grained privacy settings in location-sharing applications. We built a prototype that enables users of Buddy Tracker, to enable or disable sharing and change the level of granularity of disclosed information by shaking and sweeping their phone.

8.2. Summary of Contributions

At the outset we listed number contributions of the work presented in this thesis to the field of privacy in Ubiquitous Computing. Here we re-iterate these and highlight the evidence, which confirms the contributions.

1. **Buddy Tracker**: In Chapter 3 we presented a privacy-aware location-sharing application based on the Altman's privacy regulation theory and social translucence supporting *visibility*, *awareness* and *accountability* aiming at incorporating social rules in spatially dispersed systems.
2. **A design and evaluation of a real-time feedback as a means of incorporating social translucence in a location-sharing scenario**: Chapter 3 of this thesis presents a classification of feedback and provides guidance on how it can be implemented in mobile applications. This thesis provides empirical evidence that real-time feedback is an effective tool for supporting users' privacy (Chapter 4 and Chapter 5). Informed by focus group discussion, interviews and field trials of the real-time feedback technology we have shown that it has the potential to minimize the privacy-management burden and support privacy perception. We have also shown that the cumulative effect of the real-time feedback has an impact on data requesters' behaviour - it enforces accountability in their actions. This finding suggests an important function of socially translucent systems.

3. **Examination of the role of context-awareness in improving real-time feedback**: Chapter 6 illustrates a context-aware extension, which has been built into the real-time feedback to improve the user experience and social acceptance of the technology. Informed by the results of the field trial presented in this chapter we showed that our implementation is successful at minimizing the intrusiveness of the technology and increasing the visibility of notifications. In the spirit of Nguyen and Mynatt (2002), we have designed an invisible notification system for Ubiquitous Computing that helps people not only understand the system but also incorporates social norms that help people respect others' values. By invisible we mean a state of technological unobtrusiveness achieved by incorporating multi-sensory dimensions of real-time feedback representations, context-awareness and machine learning.
4. **A novel interface for ad-hoc privacy management, namely Privacy-Shake**: In Chapter 7 we proposed a concept of the haptic interface for managing coarse grained privacy. A prototype has been build and evaluated against usability, support for privacy tasks and social acceptance.

This thesis also provides several smaller contributions such as:

5. **Clear proposition of what mobile context is and how it can be used to design for**: Initial studies described in Chapter 4 and Chapter 5 helped us specify contextual factors determining users' acceptance of the real-time technology. Understanding the nature of mobile context was a crucial element towards the usable real-time feedback technology, which has been presented in the Chapter 6.
6. **A working prototype of a context-aware, socially translucent system that meets Bellotti and Sellen's criteria**: During our design process we have gone through three full user-centred design cycles, during which we incrementally achieved greater usability, positive user experience and low intrusiveness of the real-time feedback technology. In the process of building the Buddy Tracker application we have designed and developed several software components, which allowed us to build a usable and

socially-acceptable system. Throughout the thesis, we have demonstrated the features of our application that meet the criteria of privacy-awareness systems defined in the seminal work of Bellotti and Sellen (1993), i.e. unobtrusiveness, appropriate-timing or perceptibility.

7. **Support for researchers conducting field studies on privacy in location sharing technologies**: The software used in this research (server application, Buddy Tracker application and the real-time feedback manager for Android) is freely available from www.buddytracker.open.ac.uk. Our software offers a rich solution for researchers and students conducting user studies aimed at exploring privacy-related problems in the context of mobile, location-sharing applications. It provides several modules that support common researcher tasks, such as participants' records management, basic logs analysis, checking non-active users or support for communication. Our system is equipped with a fully instrumented interface that logs data about every users' action, which can be further used in quantitative analysis or can be used to guide the interview process. We incorporated the experience sampling method (ESM) for studying users' experience in the field. ESM has been extended by a powerful memory triggering tool developed by our research team - memory phrase. Our studies have shown that this method is very useful for work involving post-study interviews, as it is "*capable of triggering a connection to the experience*" (Mancini et al. 2009).

8.3. Future Work

Despite these contributions and usefulness of our approach at providing interfaces for feedback and control, there remain some challenges and unexplored research questions that require further work. In this section we discuss future work aimed at exploring these challenges. Due to the twofold interest of the work presented in this thesis, we discuss the future research agenda in the context of feedback and control.

8.3.1. Feedback

Here, we summarize future directions aimed at improving feedback technology and exploring the potential of our feedback technology in designing novel ubicomp services.

Nudging People Towards Privacy

Our research has started the discussion about novel ways of achieving privacy: by designing systems that nudge people towards privacy-respecting behaviour. We showed that social norms can be enforced by incorporating feedback in the digital systems. More studies are needed to explore what other design features can help people make better privacy choices. We observed that our work on real-time feedback stimulated other researchers (Balebako et al. 2011) to explore the potential of nudging in achieving privacy.

Usability of Learning Algorithms

Although in our studies we were able to use a machine learning algorithm that is capable of learning rules from a limited data set (hence minimizing user effort), incorporating the learning process into real systems still poses a significant challenge. It is because user's feedback is required for those algorithms to work effectively. Therefore we need to investigate further how to incorporate machine learning into this type of systems in a usable manner. As reported in Chapter 6, we managed to improve the accuracy of notifications and significantly minimize the intrusiveness of the technology. However similarly to work by Sadeh (Sadeh et al. 2009), our methodology required users' feedback to learn new rules, which might be cumbersome. While people may be willing to give feedback to the system while taking part in an experiment for which they receive compensation, they may not be willing to do the same in an un-controlled setting.

Therefore the next step in this research is to explore any links between users' personalities, occupations, and life style in general, and privacy attitudes in order to determine whether an adaptive model for user acceptance of real-time feedback technology can be derived.

Concomitantly, new input methods may be required, which will allow us to design more affordable ways of defining learning rules.

Performance of the Real-Time Feedback

In our research we decided to use off the shelf mobile devices in order to increase the realism of the studies. Although modern devices are capable of sensing rich information about the users' environment, battery consumption of sensors make it difficult to develop a long-lasting and reliable system. Due to this problem we could not use all available sensors to provide richer contextual clues to the learning system, e.g., microphone could not be used to measure the noise level. Recall, that participants of the field trial presented in the section 6.5 reported technical limitations and high battery consumption to be the most negative factors towards the acceptance of the technology. This indicates that that current technology is not yet able to provide *usable context-awareness*, which might have an impact on the development of context-aware mobile applications. We solved this problem by offering our participants an extended battery, which is not feasible in the real world. Therefore developers and engineers should maximize their effort at developing new ways of cheap access to sensory information. Optimization guidelines are also needed for context-aware applications developers that will help them optimize code in order to offer a long standing user experience.

Improvements in the Buddy Tracker Architecture

Technological improvements of Buddy Tracker's architecture are needed and should include using a client's device for data capture, data storage and learning process in order to minimize privacy and security problems related to data transfer. We envision that the future real-time feedback technology uses on-device learning approaches, similar to Wang and Ahmad (2010). It will minimize security problems and save battery life, which has been highlighted as one of the practical problems of our technology.

A Need for Interactive Visualizations for Feedback

Similarly to the three privacy attitudes reported in (Taylor 2003), we observed two attitudes towards our technology (pragmatic and opportunistic) and their correlation between two main factors determining social acceptance of the real-time feedback. We found that effectiveness is more important for people with a pragmatic approach towards technology while intrusiveness is more important for people with a more opportunistic attitude. Moreover we observed that there is a stronger need for historical feedback in the second group than there is in the first group. Therefore more work is needed at improving the awareness of users with opportunistic approach towards technology. We see that this gap could be addressed by designing easy to use visualizations easily available on the mobile device. While the initial design for aggregated feedback for touch screen devices has been presented in the section 3.4.2, more work is needed at implementing and evaluating a working prototype.

Novel Notification Services

Since the main goal of real-time feedback application presented in this thesis was to support privacy awareness by providing timely and meaningful information about the actual information flow in the ubicomp systems, we see a number of business opportunities incorporating our technology. The real-time feedback system presented in this thesis could be used in many applications that require an automated notification services. An unobtrusive notification service can lead to the development of novel messaging systems that can improve our life by providing timely information while we grasp with the physical. We believe that our technology provides a tangible proof that Weiser's vision of *calm computing* can be achieved in the near future.

8.3.2. Control

We presented the concept and initial results of the evaluation of Privacy-Shake, a novel interface for 'heads-up' privacy management. The chosen demographic was not broad, but the study helped us identify both social and technical issues related to the interface.

Improved Accuracy and Personal Calibration

Two main technological issues of the Privacy-Shake are lack of individual calibration and support for more discreet movements. Our study revealed differences in people's movements and gestures, which had an impact on the performance of our interface. It was suggested that users should be able to calibrate the interface for their movement style, which should help improve the effectiveness of the interface. Secondly, users reported that movements should be more discrete, since users understood the need for the dynamic initiation movement, it was suggested that the interface should be more sensitive and allow for tiny movements.

Extending the Gestures Language

Privacy-Shake supports only four settings and some users suggested we should incorporate more gestures to enhance its functionality. Future improvements of the interface could focus on designing novel gestures for group settings or expressing more fine-grained preferences.

Privacy-Shake in Request-Based Location-Sharing Applications

Since Privacy-Shake system was evaluated in the context of the Buddy Tracker we did not explore the effectiveness of the Privacy-Shake interface in a request-based setting, where each location disclosure requires the data owner to accept or reject the query. User could reply to the request using gesture and system then could learn new policies based on data owner's decisions, which would be used in the future. Consider the example scenario:

> Scenario: Bob and Alice are users of Buddy Tracker application equipped with Privacy-Shake. One day Alice requests Bob's location. Bob held the phone in his pocket at the time of request. The system informed Bob that Alice is requesting his location by using a natural language feedback. Bob moved the phone vertically, he repeated the movement and then he moved the phone forward. The system recognized this gesture as: always share this location at exact level with Alice. This scenario is presented in the Figure 8-1 below.

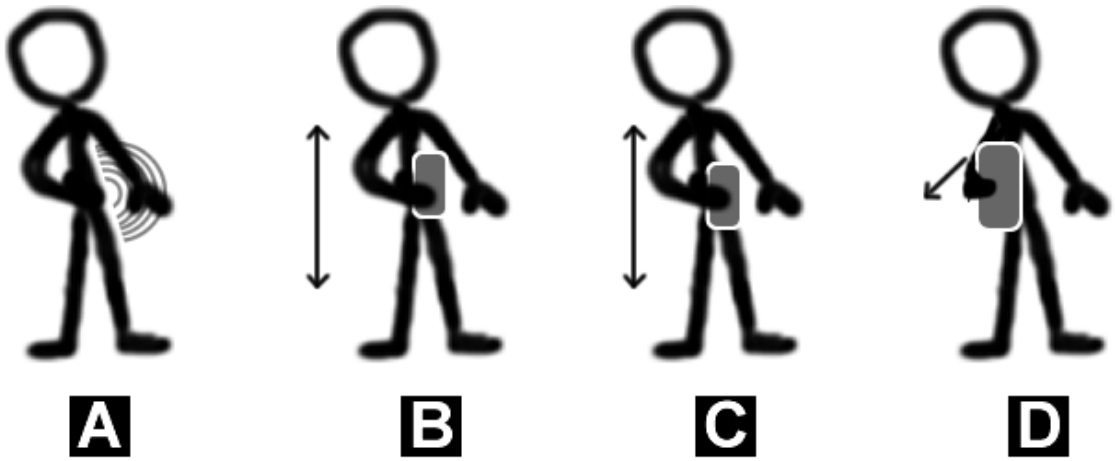


Figure 8-1. Privacy-Shake and real-time feedback technology in request-based location-sharing system. (A) Bob receives a real-time feedback notification about new location request from Alice. His phone vibrates and plays a message "Alice wants to see where you are". (B) Bob shakes phone vertically. It means that he wants to share his location. (C) Bob shakes his phone vertically again, it means that he wants to share exact location. (D) bob moves his phone towards, which allows him to save this preference for the future.

By using a combination of three simple gestures, the user could not only reply to the location request but also manage his privacy policy for the future. User's movement could be transformed into a privacy rule specifying privacy decision, granularity of disclosed location and temporality of the rule. Since the system incorporates real-time feedback technology, immediate reaction from the user (user took phone out of the pocket after the notification) suggests the correlation between user's intention and feedback, which could eliminate the initiation movement and allow for high sensitivity for discrete movements.

Obviously utility of gestural interfaces at specifying more complex privacy rules requires further research, which should look at usability, acceptance of gestures but also cognitive load on user's memory. Since the underlying idea of Privacy-Shake was to use it for specifying simple and situation-dependent privacy rules, complexity of gestures might overwhelm users, thus making this scenario unusable.

Acceptance of Gestural Interfaces

Our research on Privacy-Shake showed that some people are not ready for gesture based systems, participants reported *awkwardness* of the Privacy-shake interface. While some researchers have recently started the discussion about the problem of acceptance for gestural interfaces (Montero et al. 2010; Rico and Brewster 2010), new studies aimed at understanding social acceptance of gesture-based interfaces in the presence of other people are needed. It might include a field trial, in which people will be asked to perform different types of gestures in the public place. Participants' willingness to perform a task in the wild was already studied in (Rico and Brewster 2010), but observing reactions of the environment would provide new insights into the efficacy and social acceptance of gestural interfaces.

8.4. Concluding Remarks

Participation in modern, socially-focused digital systems involves a large degree of privacy management. That is controlling who may access what information under what circumstances. Effective privacy management requires that mobile systems' users be aware of the actual information flow. Moreover, privacy preferences vary across the context and it is hard to define privacy policies that reflect the dynamic nature of our lives. To address these problems we presented tools for feedback and control: real-time feedback and Privacy-Shake.

Since there is no strong consensus in the HCI community as to how privacy-awareness interfaces should be built. We believe that the work on real-time feedback presented in this thesis goes some way towards addressing the problem of awareness interfaces, which has been recognized as one of the key challenges for the future work on privacy in HCI (Iachello and Hong 2007). Moreover, the ideas presented in this thesis provide a new starting point for the privacy-aware systems designers. Our work shows that privacy can be achieved by incorporating social norms in socio-technical systems.

By designing the Privacy-Shake we demonstrated that privacy management tasks do not have to be boring, and can provide a pleasurable and fun experience. Although the Privacy-Shake is still

in its infancy, we believe that by presenting this concept we have opened a new design space for privacy controls.

References

"*One must be a wise reader to quote wisely and well.*"

Amos Alcott

Ackerman, Mark S., and Lorrie F. Cranor. 1999. "Privacy Critics: UI Components to Safeguard Users' Privacy." In *Proceedings of CHI '99*, 258–259. ACM New York, NY, USA.

Acquisti, Alessandro, and Jens Grossklags. 2005. "Privacy and Rationality in Individual Decision Making." *Security & Privacy, IEEE* 3 (1): 26–33.

Adair, John G. 1984. "The Hawthorne Effect: A Reconsideration of the Methodological Artifact." *Journal of Applied Psychology* 69 (2): 334–345.

Adam, Karim. 2009. "Balancing Privacy Needs with Location Sharing in Mobile Computing." PhD thesis, Milton Keynes, UK: The Open University.

Adams, Anne. 2000. "Multimedia Information Changes the Whole Privacy Ballgame." In *Proceedings of CFP '00. The Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions*, 25–32. Toronto, Ontario, Canada: ACM.

Ahmed, Murad. 2009. "Village Mob Thwarts Google Street View Car - Times Online." http://technology.timesonline.co.uk/tol/news/tech_and_web/article6022902.ece.

Altman, Irvin. 1975. *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole.

———. 1980. *Culture and Environment*. Wadswrorth, Inc., Belmont, CA.

Altman, Irwin. 1977. "Privacy Regulation: Culturally Universal or Culturally Specific." *Journal of Social Issues* 33 (3): 66–84.

Anthony, Denise, Tristan Henderson, and David Kotz. 2007. "Privacy in Location-Aware Computing Environments." *IEEE Pervasive Computing* 6 (4): 64–72. doi:http://doi.ieeecomputersociety.org/10.1109/MPRV.2007.83.

Archea, John. 1977. "The Place of Architectural Factors in Behavioral Theories of Privacy." *Journal of Social Issues* 33 (3): 116–137.

Ashley, Paul, Satoshi Hada, Gunter Karjoth, Calvin Powers, and Matthias Schunter. 2003. *Enterprise Privacy Authorization Language (epal)*. Zurich, Switzerland: IBM Research.

Balebako, Rebecca, Pedro G. Leon, Hazim Almuhimedi, Patrick G. Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie F. Cranor, and Norman Sadeh. 2011. "Nudging Users Towards Privacy on Mobile Devices." In *Workshop on Persuasion, Influence, Nudge and Coercion Through Mobile Devices (PINC at CHI '11)*. Vancouver, BC, Canada.

Barbaro, Michael, and Tom Zeller. 2006. "A Face Is Exposed for AOL Searcher No. 4417749 - NYTimes.com." http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482.

Barkhuus, Louise, and Anind Dey. 2003. "Is Context-aware Computing Taking Control Away from the User? Three Levels of Interactivity Examined." In *Proceeding of UbiComp 2003*, 149–156. Seattle, WA, USA: Springer.

BBC News. 2007. "Data Lost by Revenue and Customs." http://news.bbc.co.uk/1/hi/uk/7103911.stm.

Bellotti, Victoria, and Abigail Sellen. 1993. "Design for Privacy in Ubiquitous Computing Environments." In *Proceedings of ECSCW '93*, 77–92. Milan, Italy: Kluwer Academic Publishers.

Beresford, Alastair R., and Frank Stajano. 2003. "Location Privacy in Pervasive Computing." *IEEE Pervasive Computing* 2 (1): 46–55.

Beyer, Hugh, and Karen Holtzblatt. 1998. *Contextual Design: Defining Customer-centered Systems*. San Diego, CA, USA: Morgan Kaufmann.

Bolger, Niall, Angelina Davis, and Eshkol Rafaeli. 2003. "Diary Methods: Capturing Life as It Is Lived." *Annual Review of Psychology*: 54:579–616.

Brar, Ajay, and Judy Kay. 2004. *Privacy and Security in Ubiquitous Personalized Applications*. Technical Report. Sydney, Australia: School of Information Technologies, University of Sydney. http://catalogue.nla.gov.au/Record/3534174.

Brodie, Carolyn A., Clare-Marie Karat, and John Karat. 2006. "An Empirical Study of Natural Language Parsing of Privacy Policy Rules Using the SPARCLE Policy Workbench." In *Proceedings of the Second Symposium on Usable Privacy and Security*, 8–19. Pittsburgh, Pennsylvania: ACM.

Campbell, Andrew, and Marcus Alexander. 1997. "What's Wrong with Strategy." *Harvard Business Review* 75 (6): 42–51.

Cavoukian, A. 2009. *Privacy by Design... Take the Challenge*. Canada: Information and Privacy Commissioner of Ontario.

Consolvo, Sunny, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. "Location Disclosure to Social Relations: Why, When & What People Want to Share." In , 81–90. Portland, Oregon, USA.

Cranor, L. F, and S. Garfinkel. 2005. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc.

Cranor, Lorrie F., Praveen Guduru, and Manjula Arjula. 2006. "User Interfaces for Privacy Agents." *ACM Transactions Computer-Human Interaction* 13 (2): 135–178.

Cranor, Lorrie F., Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. 2002. "The Platform for Privacy Preferences 1.0 (P3P1. 0) Specification." *W3C Recommendation* 16. http://www.immagic.com/eLibrary/TECH/W3C/P3P_10.pdf.

Dey, Anind K., and Gregory D. Abowd. 1999. "Towards a Better Understanding of Context and Context-Awareness." In *Proceedings on HUC '99*, 304–307. Karlsruhe, Germany: Springer-Verlag.

Dourish, Paul, and Ken Anderson. 2006. "Collective Information Practice: Emploring Privacy and Security as Social and Cultural Phenomena." *Human-Computer Interaction* 21 (3): 319–342.

Dourish, Paul, and Victoria Bellotti. 1992. "Awareness and Coordination in Shared Workspaces." In *Proceedings of CSCW '92*, 107–114. Toronto, Canada: ACM.

Duckham, Matt, and Lars Kulik. 2006. "Location Privacy and Location-aware Computing." In *Dynamic & Mobile GIS: Investigating Change in Space and Time*, 3:35–51.

Erickson, Tom, and Wendy A. Kellogg. 2000. "Social Translucence: An Approach to Designing Systems That Support Social Processes." *ACM Transactions on Computer-Human Interaction (TOCHI)* 7 (1): 59–83.

Fahrmair, Michael, Wassiou Sitou, and Bernd Spanfelner. 2005. "Security and Privacy Rights Management for Mobile and Ubiquitous Computing." In *Workshop on UbiComp Privacy*. Citeseer.

Fallman, Daniel. 2003. "Design-oriented Human-computer Interaction." In *Proceedings of CHI '03*, 225–232. Lauderdale, Florida, USA: ACM.

Gaver, William W. 1991. "Sound Support for Collaboration." In *Proceedings of the Second Conference on European Conference on Computer-Supported Cooperative Work*, 293–308. Amsterdam, The Netherlands: Springer.

Goffman, Erving. 1978. *The Presentation of Self in Everyday Life*. Harmondsworth.

Van Grove, Jennifer. "Are We All Asking to Be Robbed?" http://mashable.com/2010/02/17/pleaserobme/.

Gunter, Carl A., Michael J. May, and Stuart G. Stubblebine. 2005. "A Formal Privacy System and Its Application to Location Based Services." In *Workshop on Privacy Enhancing Technologies*, 256–282. Toronto, Canada: Springer.

Hall, Mark, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H. Witten. 2009. "The WEKA Data Mining Software: An Update." *ACM SIGKDD Explorations Newsletter* 11 (1): 10–18.

Harper, Richard, Tom Rodden, Yvonne Rogers, and Abigail Sellen. 2008. *Being Human: Human-computer Interaction in the Year 2020*. Microsoft Research.

Harris, Paul. 2010. "'Bling Ring' on Trial for Hollywood Celebrity Burglaries." http://www.guardian.co.uk/lifeandstyle/2010/jan/17/bling-ring-los-angeles-hollywood.

Heft, Harry. 2001. *Ecological Psychology in Context: James Gibson, Roger Barker, and the Legacy of William James's Radical Empiricism*. Lawrence Erlbaum.

Hengartner, Urs. 2007. "Hiding Location Information from Location-Based Services." In , 268–272. Mannheim, Germany: IEEE.

Holland, Simon, David S. Morse, and Henrik Gedenryd. 2002. "AudioGPS: Spatial Audio Navigation with a Minimal Attention Interface." *Personal and Ubiquitous Computing* 6 (4): 253–259.

Hong, Dan, Mingxuan Yuan, and Vincent Y. Shen. 2005. "Dynamic Privacy Management: a Plug-in Service for the Middleware in Pervasive Computing." In *Proceedings of the 7th International Conference on Human Computer Interaction with Mobile Devices and Services (Mobile HCI '05)*, 1–8. Salzburg, Austria: ACM.

Hong, Jason I. 2005. "An Architecture for Privacy-Sensitive Ubiquitous Computing". Unplublished PhD Thesis, University of California at Berkeley, Computer Science Division.

Hong, Jason I., Gaetano Boriello, James A. Landay, David W. McDonald, Bill N. Schilit, and Doug J. Tygar. 2003. "Privacy and Security in the Location-enhanced World Wide Web." In *Proceedings of the Workshop on Privacy at Ubicomp 2003*. Seattle, WA, USA: Citeseer.

Hong, Jason I., and James A. Landay. 2004. "An Architecture for Privacy-sensitive Ubiquitous Computing." In *Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services*, 177–189. Boston, MA, USA: ACM.

Hsieh, Gary, Karen P. Tang, Wai Yong Low, and Jason I. Hong. 2007. "Field Deployment of IMBuddy: a Study of Privacy Control and Feedback Mechanisms for Contextual IM." In *Proceedings of UbiComp '07*, 91–108. Innsbruck, Austria: Springer-Verlag.

Iachello, Giovanni, and Gregory D. Abowd. 2005. "Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing." In *Proceedings of CHI '05*, 91–100. Portland, Oregon, USA: ACM.

———. 2008. "From Privacy Methods to a Privacy Toolbox: Evaluation Shows That Heuristics Are Complementary." *ACM Trans. Comput.-Hum. Interact.* 15 (2): 1–30.

Iachello, Giovanni, and Jason Hong. 2007. *End-User Privacy in Human-Computer Interaction*. Now Publishers Inc.

Iachello, Giovanni, Ian Smith, Sunny Consolvo, Mike Chen, and Gregory D. Abowd. 2005. "Developing Privacy Guidelines for Social Location Disclosure Applications and Services." In *Proceedings of SOUPS '05*, 65–76. Pittsburgh, Pennsylvania: ACM.

Jedrzejczyk, Lukasz, Blaine A. Price, Arosha K. Bandara, and Bashar A. Nuseibeh. 2009. *I Know What You Did Last Summer: Risks of Location Data Leakage in Mobile and Social Computing*. Technical Report no 2009/11, Milton Keynes, UK: The Open University.

———. 2010a. "Privacy-shake: a Haptic Interface for Managing Privacy Settings in Mobile Location Sharing Applications." In *Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services (Mobile HCI '10)*, 411–412. Lisbon, Portugal: ACM.

———. 2010b. "On the Impact of Real-time Feedback on Users' Behaviour in Mobile Location-sharing Applications." In *Proceedings of SOUPS '10*. Redmond, WA, USA: ACM.

Jensen, Carlos, Colin Potts, and Christian Jensen. 2005. "Privacy Practices of Internet Users: Self-reports Versus Observed Behavior." *International Journal of Human-Computer Studies* 63 (1-2): 203–227.

Jensen, Carlos, Joe Tullio, Colin Potts, and Elizabeth D. Mynatt. 2005. *Strap: A Structured Analysis Framework for Privacy*. GVU Technical Report. Georgia Institute of Technology.

Jiang, Xiaodang, Jason I. Hong, and James A. Landay. 2002. "Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing." In *Proceedings of UbiComp '02*, 176–193. Göteborg, Sweden: Springer.

Junglas, Iris, and Christiane Spitzmuller. 2006. "Personality Traits and Privacy Perceptions: An Empirical Study in the Context of Location-Based Services." In *Proceedings of the International Conference on Mobile Business (ICMB'06)*, 36. Copenhagen, Denmark: IEEE Computer Society.

Kaplan, Stephen, and Rachel Kaplan. 1982. *Cognition and Environment: Functioning in an Uncertain World*. Praeger. http://books.google.com/books?id=jtlOAAAAMAAJ.

Karat, Clare M., John Karat, Carolyn Brodie, and Jinjuan Feng. 2006. "Evaluating Interfaces for Privacy Policy Rule Authoring." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*, 83–92. Montreal, Quebec, Canada: ACM.

Kay, Matthew, and Michael Terry. 2010. "Textured Agreements: Re-envisioning Electronic Consent." In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, 1–13. Redmond, Washington: ACM.

Kelley, Patrick G., Lucian Cesca, Joanna Bresee, and Lorrie F. Cranor. 2010. "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach." In *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI '10)*, 1573–1582. ACM.

Khalil, Ashraf, and Kay Connelly. 2006. "Context-aware Telephony: Privacy Preferences and Sharing Patterns." In *Proceedings of CSCW '06*, 469–478. Banff, Alberta, Canada: ACM.

Kohavi, Ron. 1995. "A Study of Cross-validation and Bootstrap for Accuracy Estimation and Model Selection." In *International Joint Conference on Artificial Intelligence (IJCAI '95)*, 14:1137–1143. Montreal, Quebec, Canada: Morgan Kaufmann, Los Altos, CA.

Krueger, Richard A., and Mary A. Casey. 2009. *Focus Groups: A Practical Guide for Applied Research*. 3rd ed. Sage Publication.

Krumm, John. 2007. "Inference Attacks on Location Tracks." *Pervasive Computing* 4480/2007: 127–143. doi:10.1007/978-3-540-72037-9_8.

Kupritz, Virginia. W. 2000. "Privacy Management at Work: A Conceptual Model." *Journal of Architectural and Planning Research* 17 (1): 47–63.

Langheinrich, Marc. 2002. "A Privacy Awareness System for Ubiquitous Computing Environments." In *Proceedings of UbiComp '02*, 237–245. Goeteborg, Sweden: Springer-Verlag.

———. 2005. “Personal Privacy in Ubiquitous Computing. Tools and System Support.” PhD Thesis, Zürich, Switzerland: Swiss Federal Institute of Technology (ETH Zürich).

Lederer, Scott. 2003. “Designing Disclosure: Interactive Personal Privacy at the Dawn of Ubiquitous Computing”. Master’s Thesis, Berkeley, California, United States: Computer Science Division, University of California.

Lederer, Scott, Anind K. Dey, and Jennifer Mankoff. 2002. “Everyday Privacy in Ubiquitous Computing Environments.” In .

Lederer, Scott, Jason I. Hong, Anind K. Dey, and James A. Landay. 2004. “Personal Privacy Through Understanding and Action: Five Pitfalls for Designers.” *The Journal of Personal and Ubiquitous Computing* 8 (6): 440–454.

Mancini, Clara, Yvonne Rogers, Arosha K. Bandara, Tony Coe, Lukasz Jedrzejczyk, Adam N. Joinson, Blaine A. Price, Keerthi Thomas, and Bashar A. Nuseibeh. 2010. “Contravision: Exploring Users’ Reactions to Futuristic Technology.” In *Proceedings of the 28th International Conference on Human Factors in Computing Systems CHI’010*, 153–162. Atlanta, GA, USA: ACM.

Mancini, Clara, Yvonne Rogers, Keerthi Thomas, Adam N. Joinson, Blaine A. Price, Arosha K. Bandara, Lukasz Jedrzejczyk, and Bashar A. Nuseibeh. 2011. “In the Best Families: Tracking and Relationships.” In *Proceedings of the 29th International Conference on Human Factors in Computing Systems CHI’11*. Vancouver, BC, Canada: ACM.

Mancini, Clara, Keerthi Thomas, Yvonne Rogers, Blaine A. Price, Lukasz Jedrzejczyk, Arosha K. Bandara, Adam N. Joinson, and Bashar A. Nuseibeh. 2009. “From Spaces to Places: Emerging Contexts in Mobile Privacy.” In *Proceedings of UbiComp ’09*, 1–10. ACM.

Margulis, Stephen T. 2003. “On the Status and Contribution of Westin’s and Altman’s Theories of Privacy.” *Journal of Social Issues* 59 (2): 411–429.

Marmasse, Natalia. 2004. “Providing Lightweight Telepresence in Mobile Communication to Enhance Collaborative Living”. PhD Thesis, Massachusetts, USA: Massachusetts Institute of Technology.

Montero, Calkin S., Jason# Alexander, Mark T. Marshall, and Sriram Subramanian. 2010. “Would You Do That?: Understanding Social Acceptance of Gestural Interfaces.” In *Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services (Mobile HCI ’10)*, 275–278. Lisbon, Portugal: ACM.

Moor, James H. 1997. “Towards a Theory of Privacy in the Information Age.” *SIGCAS Comput. Soc.* 27 (3): 27–32.

Myles, Ginger, Adrian Friday, and Nigel Davies. 2003. “Preserving Privacy in Environments with Location-Based Applications.” *IEEE Pervasive Computing* 2 (1): 56–64.

Neustaedter, Carman, and Saul Greenberg. 2003. “The Design of a Context-aware Home Media Space for Balancing Privacy and Awareness.” In *Proceedings of UbiComp ’03*, 297–314. Seattle, WA, USA: Springer.

Nguyen, David H., and Elizabeth D. Mynatt. 2001. "Privacy Mirrors: Making Ubicomp Visible." In *Human Factors in Computing Systems: CHI 2001 (Workshop on Building the User Experience in Ubiquitous Computing)*.

———. 2002. *Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems*. GVU Technical Report. Georgia, GA, USA: Georgia Institute of Technology. http://hdl.handle.net/1853/3268.

Ni, Qun, Dan Lin, Elisa Bertino, and Jorge Lobo. 2007. "Conditional Privacy-aware Role Based Access Control." In *ESORICS '07: Proceedings of the 12th European Symposium On Research In Computer Security*, 72–89. Springer.

Nissenbaum, Helen. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79 (1).

Openbook. "Openbook - Connect and Share Whether You Want to or Not." http://youropenbook.org/.

Palen, Leysia, and Paul Dourish. 2003. "Unpacking 'Privacy' for a Networked World." In *Proceedings of CHI '03*, 129–136. Ft. Lauderdale, Florida, USA: ACM.

Patrick, Andrew S., and Steve Kenny. 2003. "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-computer Interactions." In *Workshop on Privacy Enhancing Technologies*, 107–124. Dresden, Germany: Springer.

Pedersen, Darhl M. 1999. "Model for Types of Privacy by Privacy Functions." *Journal of Environmental Psychology* 19 (4): 397–405.

Petronio, Sandra. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press, Albany.

Pettersson, John, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein, and Henry Krasemann. 2005. "Making PRIME Usable." In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, 53–64. Pittsburgh, PA, USA: ACM.

Pfitzmann, Andreas, and Marit Köhntopp. 2001. "Anonymity, Unobservability, and Pseudeonymity - a Proposal for Terminology." In *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*, 1–9. Berkeley, California, United States: Springer-Verlag New York, Inc.

Please Rob Me. "Please Rob Me." http://pleaserobme.com/.

Privacy Rights Clearinghouse. "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy | Privacy Rights Clearinghouse." http://www.privacyrights.org/ar/fairinfo.htm.

Quinlan, John R. 1993. *C4. 5: Programs for Machine Learning*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

Raento, Mika, and Antti Oulasvirta. 2005. "Privacy Management for Social Awareness Applications." In *Proceedings of CAPS '05 Workshop*. Helsinki, Finland: Helsinki University Press.

Raskin, Jef. 2000. *The Humane Interface: New Directions for Designing Interactive Systems*. Addison-Wesley.

Reeder, Rob W., Lujo Bauer, Lorrie F. Cranor, Michael K. Reiter, Kelli Bacon, Keisha How, and Heather Strong. 2008. "Expandable Grids for Visualizing and Authoring Computer Security Policies." In *Proceeding of the Twenty-sixth Annual SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*, 1473–1482. Florence, Italy: ACM.

Reeder, Rob W., Patrick G. Kelley, Aleecia M. McDonald, and Lorrie F. Cranor. 2008. "A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization." In *ACM Workshop on Privacy in the Electronic Society (WPES '08)*, 45–54. Alexandria, Virginia, USA: ACM.

Rico, Julie, and Stephen Brewster. 2010. "Usable Gestures for Mobile Interfaces: Evaluating Social Acceptability." In *Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI '10)*, 887–896. Atlanta, GA, USA: ACM.

Robert, Lemos. "Rental-car Firm Exceeding the Privacy Limit? - CNET News." http://news.cnet.com/2100-1040-268747.html.

Robinson, Simon, Parisa Eslambolchilar, and Matt Jones. 2009. "Sweep-Shake: Finding Digital Resources in Physical Environments." In *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services (Mobile HCI '09)*, 12. Bonn, Germany: ACM.

Rodden, Tom, Adrian Friday, Henk Muller, and Alan Dix. 2002. *A Lightweight Approach to Managing Privacy in Location-based Services*. Technical Report. Lancaster, UK: Lancaster University. http://eprints.lancs.ac.uk/12967/.

Rogers, Yvonne. 2011. "Interaction Design Gone Wild: Striving for Wild Theory." *Interactions* 18 (4): 58–62.

Rotenberg, Marc, and Cedric Laurant. 2004. "Privacy and Human Rights 2004." thttp://www.privacyinternational.org/article.shtml?cmd[347]=x-347-542782.

Sadeh, Norman, Jason I. Hong, Lorrie F. Cranor, Ian Fette, Patrick G. Kelley, Madhu Prabaker, and Jinghai Rao. 2009. "Understanding and Capturing People's Privacy Policies in a People Finder Application." *The Journal of Personal and Ubiquitous Computing* 13 (6): 401–412.

Sellen, Abigail, Rachel Eardley, Shahram Izadi, and Richard Harper. 2006. "The Whereabouts Clock: Early Testing of a Situated Awareness Device." In *CHI'06 Extended Abstracts on Human Factors in Computing Systems*, 1307–1312. Montreal, Quebec, Canada: ACM.

Sharp, Helen, Yvonne Rogers, and Jenny Preece. 2007. *Interaction Design: Beyond Human-computer Interaction*. 2nd ed. John Wiley & Sons.

Shneiderman, Ben. 1996. "The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations." In *IEEE Symposium on Visual Languages*, 336. Boulder, Colorado, USA: IEEE.

Taylor, Humphrey. 2003. "Most People Are 'Privacy Pragmatists' Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits." *The Harris Poll* 17: 19.

Toch, E., J. Cranshaw, P. Hankes-Drielsma, J. Springfield, P. G Kelley, L. Cranor, J. Hong, and N. Sadeh. 2010. "Locaccino: a Privacy-centric Location Sharing

Application." In *Proceedings of the 12th ACM International Conference Adjunct Papers on Ubiquitous Computing*, 381–382. ACM.

Toch, Eran, Justin Cranshaw, Paul H. Drielsma, Janice Y. Tsai, Patrick G. Kelley, James Springfield, Lorrie F. Cranor, Jason I. Hong, and Norman Sadeh. 2010. "Empirical Models of Privacy in Location Sharing." In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (UbiComp '10)*, 129–138. ACM.

Tsai, Janice, Patrick Kelley, Lorrie Cranor, and Norman Sadeh. 2009. "Location-sharing Technologies: Privacy Risks and Controls." In *In Research Conference on Communication, Information and Internet Policy*. Arlington, VA, USA.

Tsai, Janice Y., Patrick G. Kelley, Paul H. Drielsma, Lorrie F. Cranor, Jason I. Hong, and Norman Sadeh. 2009. "Who's Viewed You?: The Impact of Feedback in a Mobile Location-sharing Application." In *Proceedings of CHI '09*, 2003–2012. ACM.

Vildjiounqite, Elena, Tapani Rantakokko, Petteri Alahuhta, Pasi Ahonen, David Wright, and Michael Friedwald. 2008. *Privacy Threats in Emerging Ubicomp Applications: Analysis and Safeguarding. In Kouadri Mostefaoui, S., Maamar, Z. and Giaglis, G. M. Eds. Advances in Ubiquitous Computing: Future Paradigms and Directions.* IGI Global publication.

Wall, Steven, and Stephen Brewster. 2006. "Feeling What You Hear: Tactile Feedback for Navigation of Audio Graphs." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*, 1123–1132. Montreal, Quebec, Canada: ACM.

Wallop, Harry. "Burglars Using Twitter and Facebook to 'Case the Joint' - Telegraph." http://www.telegraph.co.uk/technology/facebook/7900704/Burglars-using-Twitter-and-Facebook-to-case-the-joint.html.

Wang, Alf I., and Qadeer K. Ahmad. 2010. "CAMF - Context-Aware Machine Learning Framework for Android." In *Proceedings of SEA '10*. Marina Del Rey, CA, USA: ACTA Press.

Warren, Samuel D., and Louis D. Brandeis. 1890. *The Right to Privacy. Harward Law Review*. Boston.

Weiser, Mark. 1991. "The Computer for the 21 Century." *Scientific American* 256 (3): 94–104.

Weiser, Mark, Rich Gold, and John S. Brown. 2010. "The Origins of Ubiquitous Computing Research at PARC in the Late 1980s." *IBM Systems Journal* 38 (4): 693–696.

Westin, Alan. 1967. *Privacy and Freedom*. Vol. 97. New York: Atheneum.

Zetter, Kim. "CardSystems' Data Left Unsecured." http://www.wired.com/science/discoveries/news/2005/06/67980.

Appendices

A.1. Scenarios for In-lab Evaluation of the Real-Time Feedback.

SCENARIO 1: ALICE IN THE MEETING 1.

Alice and Bob are users of Nearby Friends application. Alice and Bob are friends. Bob checks on Alice's location when she is on the meeting, LED light on her phone started flashing when she was presenting her slides.

a) She glanced on her phone and after the meeting Alice checked how many times Bob looked at her location recently and she decided not to share her exact location with Bob.

b) Alice did not notice the flashing light.

SCENARIO 2: ALICE IN THE MEETING 2.

Alice and Bob are users of Nearby Friends application. Alice and Bob are friends. Bob checks on Alice's location when she is on the meeting, her phone started playing a sound "Bob is checking your location" when she was presenting her slides.

a) After the meeting Alice checked how many times Bob looked at her location recently and she decided not to share her exact location with Bob.

b) She felt embarrassed and switched the Real-Time notifications OFF immediately.

c) Alice was just explaining an important element of her work and she had a very bad time due to difficult questions from the audience. She felt very embarrassed and has thrown the phone to the bin. (Very extreme one)

SCENARIO 3: SHARING LOCATION WITH STRANGERS.

Alice, Bob and Ed are users of Nearby Friends application. Alice and Bob are friends, Alice does not know Ed, but Ed knows Bob. One day, Ed looks at Bob's connections; he found

Alice's profile interesting and decided to check her location. Her location sharing settings allow friends of friends to look at her location. At the time Ed looked at her, Alice's phone vibrated.

a) She looked at her phone and changed her disclosure settings immediately. Her location is no longer accessible to strangers.

b) She felt threatened because she didn't know that the person she does not know is able to access her location.

SCENARIO 4: PRIVACY SHOCK.

Alice and Bob are users of the Nearby Friends application. Alice and Bob are friends, they also work together. Nearby Friends just launched a new service called "Privacy Shock" which informs data owners if someone is looking at their profiles very often.

a) After two weeks the system automatically displayed a warning saying "*Alice: Bob has checked your location 50 times in last week. Do you want to change your disclosure preferences for Bob? [YES] [NO] [Trust Bob] [View more]*". Alice clicks on YES button

b) Alice went for holiday, all her friends knew she's on holiday and many of them were very curious where she is at the moment. After one week of location checks made by Alice's friends she started receiving series of alerts saying that her friends are checking her location. Which she found very annoying as she didn't feel it's bad that her friends are curious where she is.

c) Alice knew that the "Privacy Shock" function is reciprocal; therefore she stopped using the service as often as before. Alice knew that every time she was looking at someone's location at the time she shouldn't that person might be informed about that. (Alice is presenting the service to Mark and they both are curious where Bob was at the moment, as they both know he was on date with a new girlfriend. However they don't do it because it was late and Alice reminded herself that if she does so Bob will know that and might feel it to be an invasive action.)

SCENARIO 5: NEARBY FRIENDS.

Ed and Bob are users of the Nearby Friends application. Bob is in the shopping mall. Suddenly his phone vibrates and plays a sound "Bob is 50 yards from you".

a) He started looking around and found Bob checking out a window display in nearby shop. He phoned him and said "Hi Bob, look back". Bob started looking around and noticed Ed. They haven't see each other for a long time, therefore they decided to go for a coffee.

b) He started looking around and found Bob checking out a window display in nearby shop. He hides himself behind the wall and makes himself invisible in the application.

SCENARIO 6: DO NOT DISTURB, I'M BROWSING THE INTERNET NOW.

Alice is browsing the Internet on her mobile phone. At the same time John thought about Alice and was wondering where is she now. He logged in to the Buddy Tracker application to check Alice's location.

a) Small notification has been displayed on Alice's screen that John checked her location.

b) Dialog box appeared on Alice's screen. She could not read the article.

A.2. Scenarios Used in the Survey

Table 5. Table presents 24 scenarios used in the real-time feedback survey (described in the chapter 6). Single person saw 10 scenarios.

#				R	I	Description
1	y	y	y	company: strangers		Imagine, you are on a bus, surrounded by a dozen strangers, composing an SMS. When, Bob checks your location. Location: bus,public transport Activity: standing in a crowd Mobile activity: writing SMS
2	y	y	y	company: strangers		Imagine, you are on the phone to your partner / house mate, asking if there is anything they specifically need as you are at the supermarket. When, John checks your location. Location: supermarket,shop Activity: shopping Mobile activity: phone conversation

3	y	y	y	company: strangers		Imagine, you are seated in a restaurant and while waiting for your meal to arrive, check your bank statement via mobile browser. When, Jenny checks your location. Location: restaurant Activity: waiting for a meal,sitting Mobile activity: browsing Internet
4	y	y	y	company: friends, colleagues		Imagine, you and your friends are engrossed playing your favourite game on your mobile. When, Alison checks your location. Location: no details, it can be play ground, school Activity: standing Mobile activity: playing game
5	y	y	y	company: friends, family		Imagine, you are out for a walk in the park with family and friends, you stop to take a photo using your mobile. When, Alan checks your location. Location: park Activity: walking Mobile activity: taking picture
6	y	y	n	company: business relation, colleagues from work		Imagine, you are presenting slides while in a meeting at work. Your mobile is on the table in front of you. When, Mary checks your location. Location: work,meeting room Activity: in the meeting,presenting slides Mobile activity: n/a
7	y	y	n	company: family		Imagine, you are sat at home with close family enjoying a meal. Your phone is on the table. When, Susan checks your location. Location: home,parents home Activity: family dinner Mobile activity: n/a
8	y	y	n	company: friends, all people know the requester; requester: friend		Imagine, you are driving friends to the Cinema, 'handsfree' of course. When, Tom who everybody in the car knows, checks your location. Location: car Activity: driving a car Mobile activity: n/a
9	y	y	n	company: friends, all people know the requester; requester: friend		Imagine, you are having a drink with friend who also uses 'Buddy Tracker', your mobile is on the bar. When, a common friend Lyn checks your location. Location: bar, pub Activity: sitting in a pub, drink, chatting etc Mobile activity: n/a
10	y	y	n	requester: partner; company: workmate	high	Imagine, you are having a 'swift one, early doors' with a workmate, prior to going home. Your mobile is on the bar. When, your Partner checks your location. Location: bar, pub Activity: sitting in a pub, drink, chatting etc Mobile activity: n/a
11	y	n	y			Imagine, you are at home, composing an SMS. When, Bob checks your location. Location: home Activity: lie on the sofa Mobile activity: writing SMS
12	y	n	y			Imagine, you are at home but in the middle of a telephone call. When, Bob checks your location. Location: home Activity: lie on the sofa Mobile activity: phone conversation
13	y	n	y			Imagine, you are lounging on the couch, 'browsing' for somewhere to go. When, Bob checks your location. Location: home Activity: lie on the sofa

						Mobile activity: browsing Internet
14	y	n	y			Imagine, you are playing your favourite game on your mobile while relaxing at home. When, Bob checks your location. Location: home Activity: Mobile activity: playing game
15	y	n	y			Imagine, you are at home taking a picture of the cat to send to your Mum. When, Bob checks you location. Location: home Activity: Mobile activity: taking picture
16	y	n	n			Imagine, you are driving alone, 'handsfree' of course. When, Bob checks your location Location: car Activity: driving a car Mobile activity: n/a
17	y	n	n			Imagine, you are sitting in your private office, your mobile on the desk in front of you. When, Bob checks your location Location: office Activity: sitting at desk Mobile activity: n/a
18	y	n	n			Imagine, just in from work, waiting for the rest of the household to arrive. When Bob checks your location. Location: home Activity: sitting on a sofa, armchair, just waiting for others Mobile activity: n/a
19	n	y	y	company: strangers, do not know people around		Imagine, you are on the bus talking on the mobile with your friend Alice. When, Bob checks your location. Location: bus, public transport Activity: standing Mobile activity: phone conversation
20	n	y	n	company: business relation		Imagine, you are presenting slides while in a meeting at work. Your mobile is on the floor, in your bag / briefcase. When, Bob checks your location Location: office, meeting room Activity: business meeting, presenting slides Mobile activity: n/a
21	n	y	n	company: family, friends		Imagine, you are sat at home with close family enjoying a meal. When, Bob checks your location. Location: home Activity: family meal Mobile activity: n/a
22	n	n	y		important phone call	Imagine, you are alone in a quiet room, in the middle of a important telephone call. When, Bob checks your location. Location: quiet room Activity: sitting at desk Mobile activity: phone conversation
23	n	n	n			Imagine, you are in your car driving, mobile in your pocket. When, Bob checks your location. Location: car Activity: driving a car Mobile activity: n/a
24	n	n	n			Imagine, you have arrived home early and are preparing the evening meal for the family. When, Bob checks your location Location: home, kitchen Activity: cooking Mobile activity: n/a