Tumult and turmoil: privacy in an ambient world

Linda Little[1] & Pam Briggs[1]

PACT Lab, School of Psychology & Sports Science,
Northumbria University, Newcastle, UK, NE1 8ST
l.little@unn.ac.uk

Abstract. Ambient Intelligence (AmI) and ubiquitous computing allow us to consider a future where computation is embedded into our daily social lives. This vision raises its own important questions. Our own interest in privacy predates this impending vision, but nonetheless holds a great deal of relevance there. As a result, we have recently conducted a wide reaching study of people's attitudes to potential AmI scenarios with a view to eliciting their privacy concerns. The approach and findings will be discussed.

1 Introduction

Ambient Intelligence (AmI) refers to the convergence of ubiquitous computing, ubiquitous communication, and interfaces that are both socially aware and capable of adapting to the needs and preferences of the user. AmI evokes, or perhaps presages, a near future in which humans will be surrounded by 'always-on', unobtrusive, interconnected intelligent objects, few of which will bear any resemblance to the computing devices of today.

The majority of current work on AmI is driven by technological considerations, despite claims that it is fundamentally a human-centred development that will essentially set people free from the desktop. One of the particular challenges of AmI is that the user will be involved in huge numbers of moment-to-moment exchanges of personal data without explicitly sanctioning each transaction. Nijholt et al [7] argue research tends to focus on the interaction with the device or environment, and not with other people or how the user is willing, able or wants to communicate with the environment or have the environment communicate with them. In other words, as the communication device disappears we will need a more explicit study of the appropriateness of different forms of communication in different context i.e. the issue of privacy becomes paramount. The seamless exchange of information has vast social implications, in particular the protection and management of personal information. The protection of personal information is not just related to information exchanged by devices; we also need to consider the environment and other people around at that particular time.

1.1 Privacy

Every major advance in information and communication technologies since the late 19th century has increased concern about individual privacy [10]. We already know that perceptions of privacy impact upon current technology use [4]. AmI brings new and increased risks, including fraud and identity theft, and therefore we see privacy control as essential in AmI.

In an ambient world information collection, processing and sharing are fundamental procedures needed for the systems to be fully aware of the user's needs and desires. AmI technologies will act on the user's behalf without their explicit knowledge and the interaction will be invisible. By its very nature this puts ambient technology and privacy in conflict. We need to understand this conflict and how privacy impacts upon AmI technology adoption and use.

Several programs exist to stop personal details being collected. Privacy preference protocols and systems such as P3P allow users to set preferences in accordance with their privacy needs. However, we must question whether this concept would truly work in an AmI society. Recent studies now acknowledge the complex nature of human-human interaction and the need for users to set multiple privacy preferences in an AmI world [e.g. 10]. Palen & Dourish [9] argue that as our lives are not predictable, and privacy management is a dynamic response to both the situation and circumstance, prior configuration and static rules will not work. Therefore, disclosure of information needs to be controlled dynamically. Olson et al [8] take an opposite view and suggest individuals can set preferences for sharing information as people tend to have clusters of similar others and therefore the task is not as complex or particularly difficult to undertake as it first may seem.

Academics, researchers and industry acknowledge that AmI technologies introduce a new privacy risk [e.g.10]. Consider the following question: Will users be able to set their own privacy preferences? The answer seems easy, but is it? Humans live, work and interact with a variety of people and in different environments. The multifaceted nature of human-human interaction requires each individual to set complex sets of privacy preferences dependent upon their situation and circumstance. These preferences would also have to remain stable across place, space, country and culture.
If AmI technologies are used globally, systems must be designed so that user privacy settings remain secure and unchanged across international boundaries. For example, Europe has a tighter data protection act compared to the USA [2]. Therefore someone travelling from Europe to the USA might find unknown others have access to his or her personal information when entering the country due to the slacker regulation and control of privacy policies related to AmI systems.

One area of growing concern that violates privacy is tracking. For example, Consolvo et al [1] found individuals are willing to disclose something about their location most of the time. However, the individual will only disclose information when: the information is useful to the person requesting it, the request is timely, is dependent upon the relationship he or she has with the requestor and why the requestor needs the

information. These findings highlight the need for control and choice over disclosure of personal information at any one point in time.

Levels of control and actual context of the interaction all have a major affect on use of AmI technology and the user. We need to understand how people will regulate, control and choose when to interact with such devices and who will have access to their personal information.

To fully understand privacy we need to consider: how humans interact with each other, how humans interact with technology, how technologies communicate with other technologies and know the technical constraints of each system.

The aim of this research is to investigate how people will control information exchange when using AmI devices by investigating trust and privacy permissions. This paper focuses on privacy related issues with regard to ambient technology.

2 Method

To understand and investigate the concept of AmI technology and subsequent use key stakeholders provided specific scenarios illustrating the ways in which privacy, trust and identity information might be exchanged in the future. The stakeholders included relevant user groups, researchers, developers, businesses and government departments with an interest in AmI development. Four scenarios were developed, related to health, e-voting, shopping and finance that included facts about the device, context of use, type of service or information the system would be used for. All scenarios were considered relevant and portrayed human interaction with technologies and information exchange in everyday settings. An example of the shopping scenario is given below:

Shopping Scenario*: Anita arrives at the local supermarket grabs a trolley and slips her PDA into the holding device. A message appears on screen and asks her to place her finger in the biometric verification device attached to the supermarket trolley. Anita places her finger in the scanner and a personalised message appears welcoming her to the shop. She has used the system before and knows her personalised shopping list will appear next on the PDA screen. Anita's home is networked and radio frequency identification tags are installed everywhere. Her fridge, waste bin and cupboards monitor and communicate seamlessly with her PDA creating a shopping list of items needed. The supermarket network is set so that alerts Anita of special offers and works alongside her calendar agent to remind her of any important dates. As she wanders around the supermarket the screen shows her which items she needs in that particular aisle and their exact location. The device automatically records the price and ingredients of every item she puts into trolley and deletes the information if any item is removed. When Anita is finished she presses a button on the PDA and the total cost of her shopping is calculated. Anita pays for the goods by placing her finger on the biometric device and her account is automatically debited, no need to unpack the trolley or wait in a queue. The trolley is then cleared to leave the super-*

market. Anita leaves the supermarket, walks to her car and places her shopping in the boot.

The elicited scenarios were scripted and the scenes were videotaped in context to develop Videotaped Activity Scenarios (VASc). The VASc method is an exciting new tool for generating richly detailed and tightly focused group discussion and has been shown to be very effective in the elicitation of social rules [5]. VASc are developed from either in-depth interviews or scenarios, these are then acted out in context and videotaped. The VASc method allows individuals to discuss their own experiences, express their beliefs and expectations. This generates descriptions that are rich in detail and focused on the topic of interest. For this research a media production company based in the UK was employed to recruit actors and videotape all scenarios. The production was overseen by both the producer and the research team to ensure correct interpretation. British Sign Language (BSL) and subtitles were also added to a master copy of the VASc's for use in groups where participants had various visual or auditory impairments.

2.1 Participants

The VASc's were shown to thirty-eight focus groups, the number of participants in each group ranged from four to twelve people (N=304). Participants were drawn from all sectors of society in the Newcastle upon Tyne area of the UK, including representative groups from the elderly, the disabled and from different ethnic sectors. Demographic characteristics of all participants were recorded related to: age, gender, disability (if any), level of educational achievement, ethnicity, and technical stance. A decision was made to allocate participants to groups based on: age, gender, level of education and technical stance as this was seen as the best way possible for participants to feel at ease and increase discussions. As this study was related to future technology it was considered important to classify participants as either technical or non-technical. This was used to investigate any differences that might occur due to existing knowledge of technological systems. Therefore participants were allocated to groups initially by technical classification i.e. technical/non-technical, followed by gender, then level of educational achievement (high = university education or above versus low = college education or below), and finally age (young, middle, old). In this paper findings are discussed from all participants and not by the different classifications used.

2.2 Procedure

On recruitment all participants received an information sheet that explained the study and the concept of AmI technologies. Participants were invited to attend Northumbria University, UK to take part in a group session. The groups were ran at various times and days over a three-month period. Participants were told they would be asked to watch four short videotaped scenarios showing people using AmI systems and con-

tribute to informal discussions on privacy and trust permissions for this type of technology.

At the beginning of each group session the moderator gave an explanation and description of AmI technologies. After the initial introduction the first videotaped scenario was shown. Immediately after this each group was asked if they thought there were any advantages and/or disadvantages they could envisage if they were using that system. The same procedure was used for the other three-videotaped scenarios. The scenarios were viewed by all groups in the same order: e-voting, shopping, health and finance. Once all the videos had been viewed an overall discussion took place related to any advantage/disadvantages, issues or problems participants considered relevant to information exchange in an ambient society. Participant's attitudes in general towards AmI systems were also noted.

3 Results

All group discussions were transcribed then read; a sentence-by-sentence analysis was employed. The data was then open coded using qualitative techniques and several categories were identified. The data was physically grouped into categories using sentences and phrases from the transcripts. Categories were then grouped into the different concepts, themes and ideas that emerged during the analysis.

Preliminary findings for all group discussions indicate several themes and concepts that provide greater insight into privacy issues regarding information exchange in an ambient society. One of these concepts 'informational privacy (a person's right to reveal or not reveal personal information to others)' will be discussed.

The concept of informational privacy was a major concern for all participants. Participant's highlighted complex patterns of personal information would be required to be able to control who receives what and when. Global companies and networks were seen as very problematic – facilitating the transmission of personal information across boundaries each with different rules and regulations.

'Databases can be offshore thereby there are sort of international waters and they are not under the jurisdiction of anyone or the laws of anyone country, you'd have to have global legislation.'

Participants acknowledged companies already hold information about you that you are unaware of and this should be made more transparent. Concerns were raised over the probability that stakeholders would collect personal information in an ad hoc manner without informing the person. Data gathering and data mining by stakeholders would create profiles about a person that would contain false information. Participants believed profiling would lead to untold consequence. For example, a person might be refused health insurance as their profile suggests he or she purchases unhealthy food.

'It's (information) where it can lead. That's the key to a lot of personal information about you, it's telling you where you live, they (3rd parties) can get details from there and there's companies buying and selling that information'.

'The device will say ' are you sure you want to eat so much red meat because we are going to elevate your insurance premium because of your unhealthy lifestyle'.

4 Discussion

The findings from this research support the view privacy is a multidimensional construct with underlying factors that dynamically change according to context. When interacting with technology privacy protection and disclosure of information is a two-way process.

To establish privacy the following questions need to be addressed when related to information exchange: Who is receiving it? Who has access? Is the receiver credible, and predictable? Where is the information being sent and received? Does the user have choice and control? How does the device know who to communicate with, e.g. through personalised agents? This raises interesting questions regarding permission setting within an AmI context – regarding the extent to which individuals should be allowed to make day to day decisions about who or what to trust on an ad hoc basis, or should employ agent technologies that represent their personal privacy preferences and communicate these to other agents [6].

Disclosure of information in any form or society is a two-way process. We need to consider the following guidelines when considering adoption and use of AmI systems:

a) Choice the option to reveal or hide information
b) Control: the ability to manage, organise and have power over all information exchanged and to notified of information held about you
c) Transparency: the need for stakeholder's to be open to information held about a person and for that person to have a right to access and change such information
d) Global rules and regulations: a global infrastructure of rules related to information exchange
e) Obscurity: the need for information exchange to be closed or made ambiguous dependent on the user's needs and desires at anyone moment in time
f) Privacy preference: the need for the user to set preferences that can be dynamic, temporary and secure.

These guidelines are basic and we need to consider the fact humans are inherently social beings and their actions are always directly or indirectly linked to other people. Practices such as the Fair Information Practice -FIP [e.g. 3] are needed to mediate privacy, empower the individual, increase the users control and create assurance.

These policies also reduce data-gathering, data-exchanging and data-mining and therefore important in an ambient society.

The method used in this research has proved very successful in trying to understand privacy in an ambient society. Further investigation will be undertaken to find if differences exist between the type of information exchanged, device, age, gender and level of technological expertise.

References

1. Consolvo, S., Smith, I.E. Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. Location disclosure to social relations: why, when, & what people want to share, Proceedings of the SIGCHI conference on Human factors in computing systems, April, Portland, Oregon, USA (2005)
2. Dawson, L., Minocha, S., & Petre, M. Social and Cultural Obstacles to the (B2C) E-Commerce Experience. Paper presented at the People and Computers XVII - Designing for Society, (2003). 25-241
3. FTC Study. Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress May (2000).
4. Little, L., Briggs, P., & Coventry, L. Public Space Systems: Designing for privacy? International Journal of Human Computer Studies.63, (2005). 254-268
5. Little, L., Briggs, P., & Coventry, L. Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. BHCIG Conference, Leeds, September (2004)
6. Marsh, S., Formalising Trust as a Computational Concept. PhD Thesis, University of Stirling, Scotland. (1994)
7. Nijholt, A., Rist, T., & Tuinenbrejier, K. Lost in ambient intelligence? In: Proc. *ACM Conference on Computer Human* Interaction *(CHI 2004)*, Vienna, Austria.
8. Olson, K., Grudin, J., Horvitz, E. 'A study of preferences for sharing and privacy'. CHI, 2005 extended abstracts on Human factors in computing systems
9. Palen, L. & Dourish, P. Unpacking Privacy for a Networked World. Proceedings of the ACM, CHI (2003), 5 (1), 129- 135.
10. Price, B. A., Adam, K., & Nuseibeh, B. Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. International Journal of Human-Computer Studies, 63, (2005) 228-253