Trust and privacy permissions for an ambient world

Linda Little, Stephen Marsh, and Pam Briggs

Linda Little
PACT Lab
School of Psychology &
Sports Science
Northumbria University
Northumberland Building
City Campus
Newcastle
UK, NE1 8ST
Tel: +44 191 2437250
Fax: +44 191 2273190
l.little@northumbria.ac.uk

Steve Marsh
NRC Institute for
Information Technology
55 Crowley Farm Road
Suite 212
Scientific Park
Moncton,
NB E1A 7R1
Tel**:** +1 506 861-0965
Fax**:** +1 506 851-3630
Stephen.Marsh@nrc-
cnrc.gc.ca

Pam Briggs
PACT Lab
School of Psychology &
Sports Science
Northumbria University
Northumberland Building
City Campus
Newcastle
UK, NE1 8ST
Tel: +44 191 2274570
Fax: +44 191 2273190
p.briggs@northumbria.ac.uk

TRUST AND PRIVACY PERMISSIONS FOR AN AMBIENT WORLD

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 and augments the need to understand how people will trust such systems and at the same time achieve and maintain privacy. 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. This chapter describes recent research related to privacy and trust with regard to ambient technology. The method used in the study is described and findings discussed.

INTRODUCTION

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 (cf Bohn et., 2005). Our own interest in trust and 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 concerns and ideas. This chapter documents the results of this study, and contextualises them through:

- Considering the concept of AmI and ambient technology, and the social implications of AmI use.
- Exploring relevant existing work in trust and privacy and discuss this in relation to ambient devices.
- Presenting and discussing general user concerns and highlighting problems of exclusion.

When trying to understand how trust and privacy issues are implicated in an ambient world focusing on purely technical approaches is not sufficient. In the e-commerce literature trust is well documented, traditionally emphasising the need to develop systems that appear trustworthy (e.g. Shneiderman, 2000). Bødker (2004) argues 'technical approaches seem to relate trust directly to the construction of secure systems, thereby implying that users are purely rational, economical actors.' In an ambient world e-services will be accessible anywhere, anytime. Therefore this chapter considers the social nature of trust and privacy with regard to ambient technology (see Egger 2003 for a review of trust in e-commerce).

The chapter is structured as follows. In the next section, we comprehensively discuss the concept of privacy and its meaning in both physical and virtual worlds. Following this, we discuss the phenomenon of trust and how, in the AmI future, trust will remain a cornerstone of social interaction. The results, and implications for AmI, of our study are presented in section 3. We conclude with a discussion about what privacy and trust considerations might mean in the light of these results, and a preliminary set of guidelines for the design of AmI devices and technology that take these implications into account.

The concept of Ambient Intelligence

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. Mark Weiser (1991) envisaged a world where computers would be implanted in nearly every artefact imaginable. A person might interact with hundreds of computers at anyone point in time, each device invisibly embedded in the environment and wirelessly communicating with each other. These embedded devices will communicate seamlessly about any number of different topics, e.g., your present state of health, when you last ate, and what it was you ate. Interactions with other devices, and at the same time other people, will become anywhere, anytime.

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; hence Punie (2003) has argued the societal and user implications of AmI should be made more explicit. 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. In the present we already carry around devices (mobile phones, personal digital assistants) that exchange personal information with other devices – but we initiate most exchanges ourselves. Nijholt et al (2004) 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.

As humans are inherently social beings, and our actions are always directly or indirectly linked to other people, how will AmI technologies impact upon our social world? Questions naturally arise: Will people begin to rely to heavily on AmI technology? Will people be comfortable exchanging all types of information, even when it is of a very personal nature? Will the way we socially interact change, and social norms along with it? Will society become one where people feel more at home interacting with their fridge instead of other people? Will AmI technology blur the boundaries between home and workplace boundaries, making a society where efficiency and productivity take precedence over love and leisure time?

The seamless exchange of information has vast social implications. Two important factors that will influence ambient technology adoption and use are trust and privacy issues. Streitz & Nixon (2005) argue ‘areas of security, privacy, and trust are critical components for the next stages of research and deployment of ubiquitous systems. Moreover, it was identified that these observations are not merely an amplification of the current concerns of Internet users with desktop computers. New approaches are required that take even more into account regarding both the social and technical aspects of this problem to ultimately determine the acceptance of this technology by the general public’ (p.35).

This chapter will focus on the social implications of information exchange in an ambient society and not the technical limitations or constraints of such systems. If we consider that the exchange of information is what makes AmI tick, we need to ask questions about

information that will have a direct impact on both trust and privacy, including: Who is receiving it? Who has access? Is the receiver credible, predictable and sensitive? Where is the information being sent and received? In what context is the device used? Does the user have choice and control? How does the device know whom to communicate with e.g. through-personalised agents?

To answer these questions we need to understand privacy and trust, and related underlying variables.

Privacy

Every major advance in information and communication technologies since the late 19th century has increased concern about individual privacy (e.g. Brandies & Warren,1890; Price et al 2005). Privacy remains a hot topic, widely discussed by academics and practitioners alike (Kozlov, 2004). AmI brings new and increased risks, including fraud and identity theft, and therefore we see privacy control as essential in AmI.

There is no universal definition of privacy, the concept is highly complex and involves different perspectives and dimensions. The need and desire for privacy varies between individuals, cultures, social and physical environmental factors (Kaya & Weber, 2003). The desired level of privacy relates to what an individual wants and the achieved level is what they actually obtain.

Research into privacy tends to take an individualist approach and uses North American or Northern European perspectives (e.g. Margulis, 2003; Boni & Prigmore, 2002). Generally models emphasise the individual's control and choice, and social relationships as either voluntary or as barriers to independence (Fiske, Kitayama, Markus & Nisbett,

1998). In the western world privacy definitions tend to involve management of personal information and space. According to Chan (2000) the ability to manipulate space is the primary way individuals achieve privacy. Several concepts have been linked to privacy, e.g., self-disclosure, social comparison, social facilitation, and social influence, attitude formation and change (Margulis, 2003).

In the psychological literature, privacy is classified as a human boundary control process that allows access by others according to one's own needs and situational factors (Westin, 1967). However, this definition is not sufficient when considering information exchange in an AmI world. We need to understand how privacy is achieved and maintained in both physical and virtual worlds.

Privacy in the virtual world

The majority of the Human-Computer Interaction (HCI) literature on privacy tends to focus on exchange and control of information over the Internet (e.g. Jackson et., 2003; Cranor, Reagle & Ackerman, 1999). The actual term 'privacy' is generally used by computer scientists and security specialists to refer to the security of data against various risks or during transmission (Clarke, 1999). Control of personal information is very important no matter where or what type of device is used. Individuals have a right to control and protect their personal information (Nguyen & Truong, 2003).

Future systems will enable more freedom and reduce the physical constraints of time and place. According to Lester (2001) development in technology is considered to be the main culprit responsible for increasing concern over the protection of privacy. As new forms of technology are introduced, personal information may be accessed using a

variety of different systems. Whichever type of system people use to access personal information the concept of privacy is of crucial concern in both the virtual and physical worlds.

However, not everyone shares the same concern, some designers and researchers appear to ignore the importance of privacy and the net effect it has on system use. Kozlov (2004) describes one such debate:

'…privacy design is not yet seen as a necessary requirement of an AmI design process in general, and that designers do not feel 'morally responsible' to deliver 'privacy management tools' (as stated in Kozlov, 2004, pp6).

We need to differentiate between the physical and virtual world to understand privacy implications. In the physical world we rely on various cues and signals that can be either physical e.g. architecture or conceptual e.g. perception of space. Through past experience we are familiar with most contexts and environments; therefore as humans we generally comply and perform behaviours in an accepted way. Physical environments are often designed to afford privacy i.e. we can close a door or find a quiet space to talk to friends. The physical world compared to the virtual world is tangible i.e. we experience the physical world through several dimensions. In the virtual world conceptual cues are often missing or when present e.g. a brand name on the Internet, the actual site might be fraudulent. When exchanging information in the physical world we generally know who will have access compared to the virtual world.

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 (Dritas et., 2005). 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.

We already know that perceptions of privacy impact upon current technology use (e.g. Little, Briggs & Coventry, 2005). For example, it is well documented that Internet users have major concerns regarding threat to their privacy and about who has access to the information they provide (Jackson et a, 2003). Cranor, Reagle & Ackerman (1999) found 87% of users were concerned about the threat to their privacy when online. Also Cranor et al (1999) found Internet users were less willing to use sites that asked for personally identifiable information and very uncomfortable providing sensitive information such as credit card details. This further emphasises the need to understand privacy in an AmI society.

Moor (1997) developed a Restricted Access Theory to understand intrusion, interference and in particular informational privacy. He suggests an individual has privacy in a situation with regard to others 'if and only if the individual is protected from intrusion, interference and information access by others'. Moor gives a vague description of what a 'situation' is or could be. He posits situations can mean activity, relationship or location. Moor also distinguished between naturally private situations (e.g. privacy is protected by the design of the environment) and normatively private situations (e.g. privacy is protected by laws). This approach helps differentiate between having privacy (natural) and having the right to privacy (normative). Although Moor argued privacy can be lost but not violated or invaded in natural situations because there are no norms (e.g.

conventional), this does not explain the dynamic nature of how people achieve and maintain privacy in different situations.

Individuals do not always have absolute control about every piece of information about them and once information is disclosed privacy is lost. However, individuals will disclose information as long as they perceive the benefit will exceed the risk (Thibaut & Kelly, 1959). Bies (2001) identified privacy as a major concern associated with unwarranted disclosure of information. Even when information disclosure is authorised, individuals are concerned with whom the information is disclosed to and the nature of the information disclosed. For example, Cranor, Reagle & Ackerman (1999) suggest that if the information is disclosed through cookies or disclosure is made to a specific party (e.g. Social Security number) and was not authorised, concern over privacy is more salient. Fears related to online privacy stem from the technologies' ability to monitor and record every aspect of the user's behaviour (Metzger, 2004). Many users are aware that their privacy is at risk when using the Internet and their online tour can be tracked. Users are aware after visiting some sites cookies can get implanted onto their hard drives and they then become a target for unsolicited mail. Users leave data trails almost everyday, e.g. credit card use. An individual's data can be collected from the trail he or she leaves behind and few legal restrictions exist on how the data can be used (McCandlish, 2002). The value of such information increases as more data is collected. At one time the collection of an individual's personal information was limited to: age, address, credit history (personal identity and life history). Now with technologies such as the Internet and surveillance other data can be collected about a person's behaviour and life:

movement, buying history, association with other people and unauthorised access to electronic records (Arndt, 2005).

Although several programs exist to stop personal details being collected, individuals may not know how to install or use them. Privacy preference protocols and systems such as Platform for Privacy Preferences Project (P3P) (Cranor, 2002). Allow users to set preferences in accordance with their privacy needs. When online users are informed that their preferences do not match the privacy policies of each site visited, they can therefore decide whether or not to continue the interaction. However, we must question whether this concept would truly work in an AmI society. Palen & Dourish (2003) 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. Olsen et al (2005) 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.

When interacting with technology privacy protection and disclosure of information is a two-way process. From the technological view point, e.g. use of the Internet, the Fair Information Practice-FIP (e.g. Federal Trade Commission of America, 2000) suggest companies should give users: notice, choice, access and security. Notice refers to the right of the individual to know what information is being collected and how it will be used. Choice means individuals have the right to object when personal information is collected for another purpose than the one described or shared with third parties. Access refers to the individual's right to see the information and correct errors. Security means

companies will honour and ensure data integrity and that data is secure from unauthorised access during both transmission and storage. Practices such as FIP 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 are important in an ambient society.

Academics, researchers and industry acknowledge that AmI technologies introduce a new privacy risk (e.g., Price et., 2005). Privacy control in an AmI world is essential to decrease risks such as fraud and identity theft. 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 (Dawson et., 2003). 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.

Privacy in the physical world

In the future individuals will be able to use systems in a multitude of different social environments and be interacting with a variety of people, such as friends, family or complete strangers.

Concerns already exist about certain technologies used in public places. One such system found in nearly all cities is the surveillance camera. Clark (1999) termed the phrase ‘dataveillance’ to capture the techniques of surveillance and data recording. People have been ‘watched’ and their behaviour recorded in public places for many years. Many arguments exist for the use of such cameras, e.g. crime reduction. However as advances in surveillance technologies are made many now argue that privacy no longer exists, or that if it does it is quickly disappearing as our activities are increasingly made public (Gotlieb, 1996; Brin, 1998).

Another area of growing concern for users of technology in public places that violates their privacy is tracking. Users of mobile telephones are already aware their service provider can track their location. However design specifications in future technologies may mean it is not only the service provider who knows where you are and what you are doing. The future could see systems developed that track users to specific locations whether their device is switched on or off. Tracking will not only be available to the service provider but to virtually anyone who wants to know where the user is. Although this may be a good idea, for example in the case of missing persons, it does raise important ethical issues.

A recent study by Consolvo et al (2005) 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.

Western models of privacy

Perception of privacy in the western world often differs from eastern cultures. For example, space in the west is generally considered a mechanism to achieve and maintain privacy but not as important in eastern cultures. This research employs western approaches to understand and describe privacy. Two western models that have been very influential in privacy research in the discipline of psychology are those developed by Altman in 1975 and Westin in 1967. Both theories are examples of a limited-access approach to privacy (Margulis, 2003). The theories both describe privacy in terms of needs and desires that are: control and regulation of access to oneself and a continuous dynamic regulation process that changes due to internal/external conditions. Both theories acknowledge regulation can sometimes be unsuccessful, different types of privacy exist and privacy is culturally specific.

Altman (1975) described privacy as an ideal, desired state or as an achieved end state. If the desired state matches the achieved state then an optimal level of privacy is obtained. Privacy is obtained by selective control of access to the self. Altman suggested that social interaction is at the heart of understanding privacy and that the environment provides mechanisms for regulation. Altman proposed four mechanisms to achieve privacy: verbal (e.g. what is said, tone of voice), non-verbal behaviour (e.g., eye contact in

communicating attitudes or intentions), environmental (e.g., personal space, physical aspects of the environment) and culture (e.g., norms, beliefs).

Westin (1967) suggested individuals use a limited-access approach to protect their privacy. He defined privacy as a dynamic process of regulation that is non-monotonic, i.e. an individual can have too much or too little. Westin proposed four types of privacy: solitude (being free from observation by others), intimacy (small group seclusion), anonymity (freedom from surveillance in public places) and reserve (limited disclosure of information to others). The four types serve various functions: personal autonomy (desire to avoid manipulation), emotional release (ability to release tensions from the social world), self-evaluation (ability to contemplate, reflect), limit (set boundaries) and protect communication (share information with trusted others). Westin's model has been extended several times to include other dimensions (e.g., seclusion, not neighbouring Marshall, 1970). Previous research that highlights the importance of additional dimensions shows how aspects of privacy can be context-specific.

Pedersen (1999, 1997, 1979) further developed Westin's model and categorised privacy into six main types: solitude (freedom from observation by others), reserve (not revealing personal information about one's self to others), isolation (being geographically removed from and free from others observation), intimacy with family (being alone with family), intimacy with friends (being alone with friends) and anonymity (being seen but not identified or identifiable by others). Pedersen suggests that the six types of privacy 'represent the basic approaches people use to satisfy their privacy needs'.

Although speculative, Burgoon (1982) suggested four dimensions of privacy: physical, psychological, social and informational. The physical dimension relates to how

physically accessible a person is to others and can be linked to such aspects as environmental design. The psychological dimension refers to a person's right to decide with whom they share personal information and the control of cognitive/affective inputs/outputs such as non-verbal communication. The social dimension is the ability to control social interactions by controlling distance between people. The informational privacy dimension relates to a person's right to reveal personal information to others, which is not always under a person's control.

Privacy regulation

The regulation of privacy is complicated due to the range of functions it maintains and protects. Levels of perceived privacy can be increased or decreased dependent upon an individuals experience, expectation, other people in the area, the task at hand, and the physical environment. Regulation is considered as a dynamic process with variable boundaries that are under continuous negotiation and management, continuously refined according to circumstance (Palen & Dourish, 2003). Generally individuals rely on features of their spatial world and the immediate environment. Regulation and control can also be sort by verbal and non-verbal behaviour.

Levels of privacy change dynamically and are affected by both internal and/or external conditions. To gain the desired level of privacy a person tries to regulate their interaction by altering or maintaining their behaviour dependent upon the situation they find themselves in.

Problems with privacy

Problems exist when trying to understand and investigate privacy issues that are related to both physical and virtual worlds. No one theory or approach is sufficient to explore this complex topic.

Findings from privacy research in the Human Computer Interaction (HCI) and computer science areas tend to focus on security aspects of existing or hypothetical systems. However recent studies are now acknowledging the complex nature of human-human interaction and the need for users to set multiple privacy preferences in an AmI world (e.g., Price et., 2005).

Privacy research has suffered from a lack of consensus regarding the different dimensions, functions and definitions of what 'the environment' actually consists of. Therefore we need to consider all dimensions if we are to understand how people achieve and maintain privacy in an AmI society. The dimensions proposed by Westin and Pedersen have been criticised as too confusing and overlapping (Burgoon, 1982). The dimensions appear to ignore physical privacy, i.e. the degree to which an individual is physically inaccessible. All of the proposed dimensions implicate psychological functioning there is no clear differentiation between other types of privacy such as informational. The types of privacy describe interaction with others that occurs in controlled situations and ignores unwanted input.

Although Burgoon's approach to privacy is speculative it lacks explanation of control over the various dimensions. For example, information pertaining to the social and physical aspects can be temporal i.e., an individual can choose to reveal a certain amount of information at any one time and control the level of interaction, for instance, they may

walk away. In comparison, once an individual reveals any type of information in the informational and psychological dimensions he or she is no longer in control of it and cannot take it back.

Concerns have also been raised in privacy research due to the actual concept itself, i.e. individuals both protect and manage it (Pedersen, 1999). No one theory fully describes the objective, physical environment or how environmental concepts are associated with the independent psychological descriptions of privacy (Margulis, 2003). Margulis states a complete explanation of privacy needs is required to understand how social activity is situated in context where objective, physical characteristics often affect behaviour. 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.

We know privacy is a multi-dimensional construct encompassing physical and social judgments (e.g. Pederson, 1999). There are four main dimensions of privacy relevant to AmI research: physical (in what type of environment is the system being used), informational (what type of information is being exchanged), psychological (is the information shared, and if so with whom) and social (who else is present at that time). Each dimension of privacy i.e. informational, psychological, physical and social needs to be evaluated if we are to understand fully the concept of privacy when related to AmI use. 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.

Trust

There is today a diffuse agreement about the fact that one of the major problems for the success of computer supported society, smart physical environment, virtual reality, virtual organisation, computer mediated interaction, etc. is trust*: people's trust in potential partners, information sources, data, mediating agents, personal assistants; and agents' trust in other agents and processes. Security measures are not enough, interactivity and knowledgability are not enough, the problem is how to build in users and agents trust and how to maintain it.*

(Falcone & Castelfranchi, 2001, pp55-56)

Trust and privacy are inter-related constructs – the more we trust, the more information we are prepared to reveal about ourselves (Teltzrow & Kobsa, 2004). Social commentators recognise that trust is essential for society (Bok, 1978; Fukuyama, 1996). An interesting picture is emerging about the ways in which individuals make trust judgments in technology-mediated interactions; however trust judgments are not always made on a rational basis. As trust is multi-faceted several factors are important when understanding AmI use: personalisation, motivation, expertise, familiarity, predictability, sensitivity and the actual source of the information.

Thinking about Trust

For all the studies on the subject (see for example Luhmann, 1979, 2000; Misztal, 1996; Sztompka, 1999; Dibben, 2000), trust remains something of an enigma: it is hard to define, hard to see, and difficult to explain, but everyone (at least in certain cultures)

seems to know what it is (for a discussion of this, see Dibben, 2000, especially p6-7). While that is somewhat annoying when you're trying to study it, it presents its own opportunities, and to a certain extent makes life easier when you ask people to talk about it, as in the sessions documented below (but it's hard to know, after the fact, what people really *meant*).

The enigmatic nature of trust is reinforced by the sheer volume, nowadays, of research in the area, and the almost pathological need of each and every article to define the phenomenon in some way. In social science alone, for instance 'the […] research on trust has produced a good deal of conceptual confusion regarding the meaning of trust and its place in social life.' (Lewis & Weigert, 1985, p975). The situation is hardly made better by the plethora of definitions within information and communication technologies, let alone computer security's somewhat muddled understanding of the term. Although thankfully similarities exist in most of the extant definitions, they remain different enough to try what is already an overloaded term. In this section we will try to pick apart the phenomenon with the aim of showing what the similarities are in the definitions, with the modest aim of arriving at something that makes sense in the context of this chapter (a more wide-reaching understanding will wait for a short while longer).

In the context of AmI, trust is a particularly important phenomenon. In the first instance, people are going to be put into situations where they may have to trust their own devices, and be influenced by these same devices. To a large extent, this situation is not unlike what exists now. There are many studies on trust in HCI, user interfaces, eCommerce, and so forth, and their results widely known. For instance, in a static setting, the design of an interface can have dramatic effects on the perceived trustworthiness of the system (for

instance, Cheskin, 1999, 2000; Riegelsberger & Sasse, 2001; Egger, 2000; Fung & Lee, 1999; Karvonen, 1999; Corritore et al. 2003). Indeed, much is also known about the effect on and development of trust in, for example, conversational interfaces (Bickmore & Cassell, 2001), digital systems in general (Corritore et., 2003), seeking on-line advice (Sillence et al 2004), and even to a lesser extent mobile technology (Siau & Shen, 2003). We find ourselves then in a situation where we are capable of at least beginning to understand how to build interfaces and systems that encourage and elicit trust.

There's more to AmI and trust than the interface, or even the system, however (for an excellent review of many AmI implications see Bohn et., 2005). For starters, it's not just an interface to a single device we're talking about. AmI is a whole environment, all around us, or invisible devices, all potentially 'talking' to each other, 'behind our backs.' The implications on trust, we conjecture, are extreme and somewhat pressing. For instance, am I placing trust in my device, or the devices it talks to, or the environment as a whole? When we consider that AmI is in fact nothing more than a collection of agents doing things for people, where then is the trust placed? In the agents, or the people, or both? Ultimately, AmI is about sharing information that is useful to the people in the environment so that they can enjoy themselves more, get more stuff, have easier lives, and so on. That being the case, the sharing of information and the potentials for transitivity in trust and privacy are amongst the more daunting challenges facing the vision. We think that proper models of and a deep understanding of trust, applied in all of these situations, can help in the design and implementation of not only secure but also usable and socially responsible ambient intelligence environments.

On a final note justifying the need for trust, consider the vision of AmI more closely. In its most pure form, AmI is a connected society of humans and artificial agents, from simple to complex, interacting as only a society can. This, if nothing else, requires us to *encourage, build, and study* trust in that society, because ultimately, a society without trust cannot exist (Good, 2000; Luhmann, 1979; Bok, 1978).

The Generalities: Exploring Definitions of Trust

- Trust is 'the expectation that arises, within a community, of regular and honest cooperative behaviour, based on commonly shared norms, on the part of other members of that community.' (Fukuyama, 1995, p26).
- Trust is 'a state involving confident positive expectations about another's motives with respect to oneself in situations entailing risk.' (Boon & Holmes, 1991, p194)
- Regardless of the underlying discipline of the authors […] confident expectations and a willingness to be vulnerable are critical components of all definitions of trust…' (Rousseau et., 1998, p394).
- 'Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both *before* he can monitor such action *and* in a context in which it affects his own action.' (Gambetta, 2000, p218).
- 'We define trust in the Internet store as a consumer's willingness to rely on the seller and take action in circumstances where such action makes the consumer vulnerable to the seller.' (Jarvenpaa et., 1999)

As can be seen, several accepted and acceptable definitions of trust exist – the interested reader is referred to (Dibben, 2000; Marsh & Dibben, 2003; Abdul-Rahman, 2004 (chapters 2 and 3 especially); Viljanen, 2005) for more in depth discussions. However, some salient points are important to note.

- The first is that trust is contextual, or situational – that is, it is based in a specific context and can only be generalised (to a greater or lesser extent) outside of that context.
- Secondly, trust exists in situations of risk – there is some discussion as to whether or not that risk is high or not for trust to exist, but in general it is accepted that without some degree of risk, trust is unnecessary.
- Third, there is some requirement for free will (or similar) on the part of the trustee – that is, that they are able to do something which is intentionally or otherwise detrimental to the truster, just as they are able to do what they are trusted to do.
- Fourth (perhaps more controversially), the phenomenon of trust requires a consideration of alternatives – without such a consideration, with a blind 'jumping into' a given situation, the phenomenon at work is not trust, but confidence (cf. Luhmann, 1990). In fact, it is from 'confidence' that the concept of 'blind trust' grows, with the subsequent argument (see Marsh, 1994) that blind trust is in fact not trust at all.

Rather than reinvent the trust wheel, we propose a definition that has worked relatively well for us in the past, and contains, in a succinct summary, most of the salient points of trust:

Trust is 'a positive expectation regarding the behaviour of somebody or something in a situation that entails risk to the trusting party.' (Patrick et., 2005)

What remains is to find out where this definition fits within AmI, what risks are involved, and what expectations are reasonable.

The Specifics: Trust in AmI, a Discussion

The Concept of Context

It is generally agreed that trust is a contextual phenomenon (some say, situationally dependent, meaning almost the same thing). This means that the trust given or received is dependent of who is the truster or the trustee, the task at hand, the opportunities for betrayal, the potential for gain or loss, and so on. In our own context, it will also bring to bear what tools are being used, what information may or may not be being considered, and so on. It is critically important to bear in mind that the concept of AmI introduces *artificial* trustees to users. The concept of *familiarity* then becomes something of importance in trusting deliberations. According to Luhmann (1990), 'trust has to be achieved within a familiar world, and changes may occur in the familiar features of the world which will have an impact on the possibility of developing trust in human relations.' (p.94). Thus, it is difficult to trust what is unfamiliar. In the context of AmI, for many people, the whole *edifice* is unfamiliar, and so a certain lack of trust may be expected, until familiarity is achieved either through use or, as in this work, through demonstrations of how AmI can, for example, benefit the user in specific, familiar contexts (shopping, banking, and so on).

Of course, if Weiser's (1991) original vision of ubiquitous computing (and by extension AmI) is to be realised, what we will see will in fact be nothing: the computers will become the background in which we all live (Bohn et., 2005). Therefore how do we conceptualise and explore familiarity and its associated problems? In this instance, does AmI just become another societal tool? If this is the case, what are the implications for trust?

Can We 'Trust' (Artificial) Technology?

The question of whether or not it is possible to trust technology has been raised in the past, with equally convincing arguments on either side. On one side (see for example Friedman et., 2000), the argument reads that since trust implies a freedom of action on the part of the trustee, it's impossible to refer to the relationship with technology (software, agents, cars, etc.) as one of trust, since technology does not in fact have free will: 'people trust people, not technology.' (*ibid*, p36) In many cases, this is at least a valid argument, but within AmI, the distinction between traditional technology, as seen by the proponents of this argument, and the 'free actor' is blurred almost to non-existence. To illustrate this argument, consider, information sharing between two agents in a closed network. Generally, it really doesn't matter *what* they share, because no-one is looking at it, and nothing gets done with it. Now, embed these agents in an ambient environment. Suddenly everything changes, but not because the agents have any more or less free will. The crucial addition to this environment is that of people (who, for our purposes, unquestionably *do* have free will!). If a human is able to query the agent(s) for what they know, and use it (on or off line), the concept of trust is not just important, but

absolutely imperative. Further, the trustee is becoming something of a blurred concept – is it the person who gets the information, or the agent that gives it to them – in other words, should we not think about trusting the agent as a surrogate, to do the right thing with the information it may have?

Largely, the discussion is philosophical, and somewhat moot – of course we can argue about whether technology can or cannot be validly trusted, but we inadvertently (or not) find ourselves in a situation where people are talking about trust in the environment in a fashion that sounds very much like trusting the technology behind that environment. Further, and critically, thinking in this way enables the people to more quickly assimilate and understand the environment. From a HCI perspective, this understanding, based on potentially flawed arguments though it might be, is a significant achievement (although we'd like to wean people off it somewhat (see below, and (Marsh, 2005)). Further, in terms of security and privacy, being able to think in terms of trust allows us to conceive much more powerful solutions to practical problems (for more discussion of which, see (Patrick et., 2005)).

The Structure of Trust: Rules for Trust Behaviour in AmI

For all its conceptual fuzziness, it's possible to put forward some rules that trust appears to obey. It's worth noting that these rules are still debated hotly amongst trust researchers, but two things apply here: first, it's worth putting up something for discussion to take place around, and second, there appears, at least to these authors, to be a movement towards accepting that these rules are for the most part correct. The rules allow designers and users to be able to reason about what can happen, should happen, or is happening

behind the scenes; how, for example, information gets shared with some agents and not others, or how much information gets shared, and so on. To a large extent, defining these rules for trust in AmI is a step along the road towards a system that can explain itself, much like expert systems can explain their chains of reasoning when queried. The interested reader is referred to Viljanen (2005), and Marsh, (1994, esp. ch.6) for the roots of these observations and rules. A different slant on some of the rules (especially regarding transitivity, the real 'hot' topic) can be found in (Chang et., 2004):

- *Trust is not symmetric*, that is, it is unidirectional: 'John trusts Bert' says little to nothing about Bert trusting John. Consider that we walk across the road every day 'trusting' that people we don't even know, and who don't know us, will not run us over. Moreover, it is not necessary for Bert to actually *know* that he is trusted by John for it to be the case.
- *Trust is not distributive*: as Viljanen (2005, p176) states: 'If "Alice trusts (Bob and Carol)," it does not follow that "(Alice trusts Bob) and (Alice trusts Carol)."' In fact, this has very far reaching implications for AmI, especially when one considers groups and organisations.
- *Trust is not associative*: '"(Alice trusts Bob) trusts Carol" is not a valid trust expression. However, "Alice trusts (Bob trusts Carol)" is a possibility' (*ibid.* p176). This has implications for transitivity, in fact.
- *Trust is not (strictly) transitive*: In fact, it makes sense in the context of AmI to think of it in some way as weakly transitive, but it is not necessarily the case. It is not possible in any given circumstance to say, however, that if Bert trusts John

and John trusts Scott, then Bert trusts Scott. It's a relatively easy step from some of the other rules (especially unidirectionality) to see that this is the case. However, if Bert trusts John and *knows* that John trusts Scott, there may be a way we can infer (and make rules for) Bert trusting Scott to some extent.

When we are thinking about AmI and trust, a very real consideration is how one can trust that the information held about one is given only to those who I trust with it, only for a specific requirement, for only a finite length of time, and so on. The observations above are relevant in this context. Only when the individual agents within an AmI environment can reason with rules derived from these observations can we expect AmI to behave in a socially responsible fashion – or to put it another way, at the very least in a fashion that people can understand and hopefully accept. We are currently developing a system of measurements and rules, that we call Boing, to address this issue.

We cannot fully understand trust without considering risk. Trust and risk are symbiotic concepts – where one cannot fully exist without the other. As Brien (1998) argues in the absence of risk trust is meaningless. Indeed some of the trust models that have been developed in recent years have explicitly included risk (Corritore, Kracher & Wiedenbeck, 2003). Sillence et al (2004) state when people seek online advice they are more willing to trust a site if perceived risk is low. Most models of trust implicate personalisation, source credibility and predictability as predictive factors (see Sillence et., 2004).

Social implications

Innovative technologies have been developed over centuries; their impact on society, social structure and behaviour is well documented (Kostakos et., 2005). For example, the Internet has had a huge impact on how we interact socially. Even after more than thirty years the social implications of Internet use are still not fully understood. When we use the Internet we disclose information about ourselves on nearly every mouse click. The trail we leave behind makes it possible for anyone with the required skill to follow us. The majority of people believe that they can control and regulate the disclosure of their personal information. However, will people be able to regulate and control all information pertaining to them when using AmI devices? It is not only the control of information that increases concerns in this future world; we must acknowledge that the social implications of such AmI devices are vast. The presence and use of these technologies will be major factors influencing our lives and how we socially interact. As systems become more ubiquitous and free the user from time and place, research suggests that although anytime, anyplace may be possible it may not always be acceptable (Perry et al 2001). People have existing expectations about how technology works, and social norms provide cues on how they should interact in any given situation (Jessup & Robey, 2002).

Discussed earlier was the concept of 'tracking'. Tracking is a departure from existing social norms in that a person knows information about you that you are unaware of i.e. where you are. Generally, when we socially interact with others (e.g., through face-to-face interaction or a telephone conversation) we reveal information about ourselves both verbally and non-verbally. The important point is that 'we' have made a decision to

disclose information to another person and generally we know who and where he or she is and vice versa. Will we need to have 'lie nodes' built into devices so our presence in every place or space we visit is not accounted for?

We already carry around a voluntary traceable microchip embedded in our mobile telephone. However, will the growth in tracking devices increase and make our lives so predictable that we lose the inherent social process of adventure and value? The introduction of social positioning maps will let us 'see before we go' and let others 'see where we are.' Ahas & Mark (2005) acknowledge that privacy and security of social positioning devices are important issue but argue 'fears people have will most likely diminish in future as people become accustomed to mobile positioning and begin to enjoy the service'. They also suggest concern over surveillance will also disappear.

Further questions arise related to AmI: How will people manage and control the amount of information revealed at any point in time? Who will people feel comfortable sharing different types of information with? How will people set and evaluate privacy and trust permissions that will govern what is being shared? The AmI challenge is particularly pressing, since in future there will be no obvious physical markers to tell us when we move from private to public cyberspaces (Beslay & Punie, 2002) and so individuals must be given a clearer vision of how and when to control personal data.

The aim of this research is to investigate how people will control information exchange when using AmI devices. To try to understand adoption and use we need to consider the concepts of trust and privacy and the related underlying variables.

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. These scenarios are briefly described below:

Health Scenario**:** *Bob is in his office talking on his personal digital assistant (PDA) to a council planning officer with regard to an important application deadline. Built into his PDA are several personalised agents that pass information seamlessly to respective recipients. A calendar agent records and alerts Bob of deadlines, meetings, lunch appointments and important dates. As Bob is epileptic his health agent monitors his health and can alert people if he needs help. An emergency management agent takes control in situations when a host of different information is needed; this agent has the most permissions and can contact anyone in Bob's contact list.*

Bob is going to meet his friend Jim for lunch when he trips over a loose paving slab. He falls to the ground and looses consciousness. His health agent senses something is wrong and beeps, if Bob does not respond by pressing the appropriate key on the PDA the agent immediately informs the emergency services. Within seconds the emergency services are informed of Bob's current situation and his medical history. An ambulance is on its way.

Paramedics arrive, examine Bob and then inform the hospital of Bob's condition on their emergency device. The hospital staff are now aware of Bob's medical history and his present state, therefore on arrival he is taken straight to the x-ray department. A doctor receives the x-rays on her PDA. After examining Bob she confirms that he has a broken ankle, slight concussion and needs to stay in hospital overnight. After receiving treatment Bob is taken to a ward. His emergency management agent contacts John (Bob's boss) of his circumstance. The emergency management agent transfers the planning application files to John's PDA so the company do not miss the deadline. The agent also informs his parents letting them know his current state of health, exactly where he is so they can visit and that his dog needs to be taken care of. As Bob is also head coach at a local running club the agent informs the secretary Bob will not be attending training the following week. The secretary only receives minimal information through the permissions Bob has set.

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

E-voting Scenario*: Natasha decides she wants to vote in the next election using the new on-line system. She goes on-line and requests electronic voting credentials. Shortly before polling day a polling card and separate security card are delivered to Natasha's home. They arrive as two separate documents to reduce the risk of interception. Natasha picks up two of the letters from the doormat and puts the letters in her pocket as she rushes out of the door to head for work. While travelling on the local underground railway system Natasha decides to cast her vote on her way to work. The letters have provided her with a unique personal voting and candidate numbers which allows her to register a vote for her chosen candidate. She takes out her mobile phone and types her unique number into it. Her vote is cast by entering this unique number into her phone and sending it to a number indicated on the polling card. Her phone then shows a text message: THANK YOU FOR VOTING. YOU HAVE NOT BEEN CHARGED FOR THIS CALL. When Natasha arrives at work she logs on to the voting site to see if her vote has*

been registered. While at her computer with her polling cards on the desk in front of her a colleague looks over her shoulder, she can see that Natasha is checking her vote but can't see who she has voted for. Once the result of the election has been announced Natasha checks that the correct candidate name is published next to her unique response number to ensure that the system has worked properly.

Financial Scenario: *Dave is at home writing a 'to do' list on his PDA. The PDA is networked and linked to several services that Dave has authorised. While writing his list he receives a reminder from his bank that he needs to make an appointment with the manager related to his yearly financial health check. He replies and makes an appointment for later that day. When he arrives at the bank he is greeted by the bank concierge system (an avatar presented on a large interface). The system is installed in the foyer of the bank where most customers use the banks facilities. The avatar tells Dave the manager, Mr Brown, will be with him soon. The avatar notes that Dave has a photograph to print on his 'to do' list and asks if he would like to print it out at the bank as they offer this service. The avatar also asks Dave to confirm a couple of recent transactions on his account prior to meeting Mr Brown.*

The analysis of the shopping and health scenario will be discussed further in this chapter.

Development of Videotaped Scenarios

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 focussed group discussion and has been shown to

be very effective in the elicitation of social rules (Little et., 2003). 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 focussed 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.

Participants

The VASc's were shown to thirty-eight focus groups, the number of participants in each group ranged from four to twelve people. The total number of participants was three-hundred and four. 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. Prior to attending one of the group sessions participants were informed about the aims and objectives of the study. 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). Overall this categorization process culminated in 24 main groups. Due to poor attendance at some group sessions these were run again at a later date. Although several participants with physical disabilities attended the main group sessions two group sessions for people with visual and auditory impairments were carried out at the Disability Forum in Newcastle. The forum was considered to have easier access and dedicated facilities for people with such disabilities.

Technical Classification

To classify participants into technical or non-technical six questions based on a categorization process by Maguire (1998) were used. Participants answer the questions using a yes/no response. Responding yes to questions 1, 3, 5 and 6, no to questions 2 and 4 would give a high technical score of 6. If the opposite occurred this would give a low technical score of 0. Participants in this study who scored 0-3 where classified as non-technical while participants who scored 4-5 as technical. The questions were:

If your personal devices e.g. mobile telephone or computer were taken away from you tomorrow, would it bother you?

Do you think that we rely too much on technology?

Do you enjoy exploring the possibilities of new technology?

Do you think technologies create more problems than they solve?

Is Internet access important to you?

Do you like to use innovative technology as opposed to tried and tested technology?

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 contribute to informal discussions on privacy and trust permissions for this type of technology. They were told all of the other participants in their particular group would be of approximately the same age and gender and informed the discussion groups would be recorded for further analysis. Participants were not informed about the technical/non-technical or the level of educational achievement classification that was used. An informal interview guide was used to help the moderator if the discussion deviated from the proposed topic.

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 issues or problems 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.

The moderator structured the discussions using an adaptation of the four-paned Johari Windows's methodology (Luft, 1969) where the four panes represent (i) information shared by the self and others, (ii) information available to the self but closed to others, (iii) information known by others but unknown to the self and (iv) information as yet unknown by self and others. Each window contracts or expands dependent upon the amount of information an individual wants to disclose. Briggs (2004) has described a means whereby the windows can be used to represent personal disclosure preferences for different agent technologies, organisations or individuals.

The duration of the sessions was approximately ninety minutes.

ANALYSIS

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.

The various themes and concepts that emerged from the analysis provided greater insight into the issues regarding information exchange in an ambient society. Different issues related to the user, device and stakeholder emerged. Further in-depth analysis revealed

several constructs related to risk, privacy, trust and social issues. These constructs were compared in relation to the user, device and stakeholder. These constructs are depicted in Table 1 (an x is used to depict whether the construct is associated with the user, device and/or stakeholder).

In the following section each concept related to trust, risk, privacy and social issues are further explained.

Trust concepts

a) *Personalisation*: the ability of people to personalise an AmI device, use personalised security mechanisms such as biometric verification systems e.g. fingerprints and the provision of personalised services from the stakeholder. Also the system and stakeholder's sensitivity regarding sending and receiving personalised information in a timely manner.

Participants agreed the benefits to some in society having systems that could exchange personal information when appropriate was advantageous. For example, people with medical problems or various disabilities having their health information being disclosed to the relevant people when needed.

Discussion revealed participants concerns over systems being truly sensitive to circumstances under which personal information could legitimately be exchanged. For example, if someone was injured should the device have permission to inform their next of kin that he or she had been taken to hospital? The transfer of sensitive personal information was discussed. Leakage of sensitive information in inappropriate circumstances was seen as very problematic:

'What if one of your agents gets corrupted and starts sending messages here, there and everywhere?'

b) *Source credibility*: linked to motivation and the credibility of the stakeholder

Participants raised concerns over supermarkets using AmI systems to pressure people in buying goods. Concerns were raised over companies have the capacity to create user profiles and monitor people with regard to their shopping habits. This in turn would create health or lifestyle profiles accessible by third parties which would lead to untold consequences.

Participants queried how they could trust 'agent' systems as they perceived they would be linked in some way to different stakeholders. For example, if an agent was used to find information out about a personal loan, would they only return information from company A and B? The issue of trust transfer (from a trusted to an unknown third party) may be threatening.

c) *Expertise:* the ability level of the user.

Participants discussed problems associated with the user's level of expertise and the complexity of setting preferences for information exchange. In other words, users with little confidence in their own ability to set privacy preferences may find it difficult to place their trust in agent systems.

d) *Predictability*: the predictability of interaction.

Discussions highlighted the dynamic nature of human interaction and that we are not predictable robotic entities. Participants agreed human behaviour is complex and the amount of information related to our everyday lives was too immense to programme preferences into AmI systems. Participants commented that we act and react in different ways depending upon with whom we are interacting, when and where. Setting up privacy preferences and permissions may become too time-consuming, reducing the utility of such systems. Participants expressed concern about the level of control stakeholders would have and questioned whether they could trust stakeholders to always act in a predictable way.

'The kind of ordered, regular lifestyle that you'd have to live for it. I don't know what I'm going to be doing next week. I really don't.'

'I mean if you know in your own mind what to program into this agent your average day you still haven't had anything taken into consideration about your non-average day, anything could happen out of the blue and the machine will be all to pot because it doesn't fit with what you've programmed into it'.

Risk Concepts

a) *Reliance and responsibility*: the user relying too much on the device to exchange information and the responsibility associated with this.

Participants discussed relying on either the system and/or themselves would be problematic. Concern arose over trust in the information received. For example in the

shopping scenario the user was informed of allergy content in food, participants discussed who would be liable if this information was wrong especially if they were buying food for another person.

'Now if I'm relying on a gadget like that in the store to say this is safe for somebody on a gluten free diet and it's not, what happens, who is liable then, me or the gadget?'

Discussion highlighted human fallibility in keeping the system up to date or losing the device (whilst acknowledging the fact that a truly AmI environment may or may not have this problem, we venture to suggest that the loss of something that gives us our identity bears similarities to this concern). Also, if the machine malfunctioned and the user was unaware of this what would the consequences be? Participants commented systems could not be truly aware of certain facts or always in control. They agreed AmI systems reduce cognitive load but questioned whether this was advantageous to humans in the long term.

'*I want to rely on myself and a network of human beings, not a network of communications and little chips'.*

'One is that there has to be a human input somewhere into the system and the reliability of the human input is dependent on the adaptability of that human being. I think we are all intelligent human beings, we're older, we're wiser than we were some years ago and I think we could all put in intelligent information but we can all make mistakes and that is a failing that we have to recognise.'

Privacy constructs

a) *Physical*: how physically accessible a person is to others

Participants commented that AmI devices would break down the boundaries of physical privacy – making an individual accessible anywhere, anytime. They discussed issues related to leakage of personal information in public settings and especially during interpersonal interaction. Participants queried whether AmI devices could truly be context aware and deliver the correct information in a timely and appropriate fashion.

'…you have no privacy, people know where you are, what you are eating, what you are doing, and that really bothers me.'

b) *Informational*: a person's right to reveal personal information to others.

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'.

c) *Social*: the ability to control social interactions between social actors.

Participants discussed the possibility that AmI would foster social isolation. Although systems would in fact increase social privacy as less human-human interaction would take place, this was considered very problematic with enormous negative consequences. Participants commented in our social world we already leak information to others in the form of visual cues e.g. items in your shopping trolley, without any serious implications. In the physical world strangers knowing certain information about you is not problematic, however people do not want to share the same information with friends. In the physical

world interactions are considered ‘open’ where people can see exactly what is happening compared to the closed nature of the virtual world. One participant described this with reference to a tin opener.

‘*You know if you are using a tin opener, you think oh, I see, but with a computer you can’t do anything like that. I mean with a vacuum cleaner you’ve got a fair idea of what to look for if the thing goes wrong but with a computer. They put computers on the market and they are supposed to be trouble free because they thought they were such a good idea, but if they had waited to iron out all the troubles, it would be another fifty years. You know look at the progress we have made.’*

d) *Psychological*: a person’s right to decide with whom they share personal information. Psychological privacy emerged as a key barrier to AmI adoption and use. Participants agreed the type of information shared normally depends on who, what, where and why, but crucially is informed by the type of relationship they have with the other person. If their relationship is close e.g. family then the majority of information is shared quite freely. However, sharing even with a close family member depends on situation and context. Participants discussed concern over stakeholders sharing personal information with third parties and suggested AmI systems needed transparency at times.

‘I don’t know who has got what information. If I asked anyone are they going to tell me if they didn’t want to and how would I know that they were telling me? So it goes into this kind of vacuum, but they are only going to tell me the information they want me to

know and they miss the bit that they really don't want me to know, that they do know or not know, I have no way of finding out.'

Complex preferences would have to be set for AmI systems and these would need to change dynamically. Participants commented, in some circumstances, relying on agent systems and the use of preset preferences for sharing information was socially unacceptable. This related to how we as humans are not predictable and interact with other in a dynamic way.

'One of the main issues is you have got all of these different types of information and how do people actually set the permissions so only person A gets that information and person B gets that and as humans we are continually changing and interacting with more and more people or less people and so the permissions change.'

e) *Choice*: the right to choose

Participants commented little or even no choice would exist in an AmI society. Comments suggested 'forced choice' would become the 'norm.' Participants expressed concern over the right not to reveal information having vast implications leading to exclusion in some circumstances. A sense of being damned simply because one might choose not to share certain types of information.

f) *Control*: the right to control

Participants were concerned about reliance on AmI systems reducing personal control. Discussions revealed AmI systems would create 'Big Brother' societies that lacked control and choice. Concern was raised over how information would be controlled by stakeholders, i.e. receiving information that is considered appropriate.

'What I don't like is where it starts taking control of that information from your hands and having information in an electronic device which fair enough you are supposed to have programmed in the first place but once you have programmed it what's your control over it then and it's transmitting information about you to all these various. I don't trust technology enough yet.'

'*That is (AmI system) structuring your life for you. You think you're in control but you're not.*'

g) *Security*: security aspects related to transmission and storage of information. Security of AmI systems emerged as key factor that would limit adoption and use. Hacking, access by third parties, leakage and storage were all areas discussed. Participants differed on the concept of using biometric systems for verification and authentication purposes. Participants classed as technical were more aware of problems related to biometric devices than those from a non-technical background. Most agreed biometric systems could alleviate the problems of human error (such as forgetting PINs); however concerns were raised with regard to exclusion when using biometric systems, e.g. the ability of the elderly to enrol and use such systems.

Social issues

a) *Exclusion*

Participants commented that exclusion would be a major problem with adoption and use of AmI systems. People would be excluded by age, ability, disability and membership of specific populations, e.g. business communities.

b) *Social and moral values*

Participants discussed several social and moral issues related to AmI systems. They suggested technologies are now undermining human responsibility. Participants agreed we now interact less socially with others. AmI systems could further decrease social interaction, reduce our social skills and take away the concept of inter-personal trust.

'We are so anti-social anyway, unless Andrew has his friends to the house and I must admit I mean I communicate with a lot of my friends now by text messages whereas before you would have called to them or you know send an email but I see less of people that I care about because it's more convenient to send them a text or an email and I hate it, I really do hate it and I think that's going to encourage more because then you're not even going to have to make the effort to send the text message, your machine is going to be sending them a text message because you're overdue writing to them.'

Although some participants in this study liked the idea of using biometric systems to access information and considered this a secure way, other participants viewed this as

‘depersonalising’ the task at hand. Discussion highlighted how life in general is becoming more depersonalised through increased interaction with technology and less with other human beings. Participants discussed issues related to the fact that if AmI systems were truly ‘context aware’ this depersonalises human interaction and thought processes.

‘If he had of collapsed (referring to hospital scenario) *and it wasn’t just a, say it was a brain tumour and he only had a few days to live when they got him into hospital and his family were informed of this via an electronic device I just think that’s terrible, it’s like totally depersonalising like the medical way of things and I mean I certainly wouldn’t like be told by somebody that one of my relatives was going to die or something over a little piece of metal or plastic or whatever it is so I think it’s one of those things in theory it all sounds well and good but in reality it just wouldn’t work.*

Concerns were raised over the fact existing technologies are often intrusive. Some participants commented that when we disclose information to others we often do not reveal the truth for various reasons. They contemplated what the consequence of this would be in an AmI world. For example, if a person told his or her partner they were shopping when in fact that was not true, would his or her partner be able to track the person’s exact location?

DISCUSSION

To evaluate the social impact of AmI use, trust and privacy issues need to be understood. The framework used in this study to evaluate trust and privacy has revealed different contexts, stakeholders, device type and actual users all need to be considered. This is important if we are to fully understand user interaction with AmI technologies.

As discussed earlier in this chapter trust is not symmetrical, distributive, associative or (at least strongly) transitive. The findings from this research support this view. Both privacy and trust are multidimensional constructs with underlying factors that dynamically change according to context. The findings support the view of Sillence et al. (2004) in that trust is multidimensional.

To establish trust and 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 trust and privacy preferences and communicate these to other agents (Marsh,1994).

Disclosure of information in any form or society is a two-way process. Findings support, the Fair Information Practice-FIP (e.g. Federal Trade Commission of America, 2000) that suggests companies should give users: notice, choice, access and security. 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) Trust and 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. Findings from this evaluation raise some interesting issues related to human values: Will people begin to rely to heavily on AmI technology? Will people be comfortable exchanging all types of information even when of a very personal nature? Will the way we socially interact change, and social norms along with it? Will our society become one where people feel more at home interacting with their fridge instead of other people? Will AmI technology blur the boundaries between home and workplace making society one of efficiency and productivity taking over from love and leisure time?

AmI systems do bring substantial benefits, including less time pressure, no queuing for goods, and memory enhancements. However the disadvantages in our social world might be far greater, e.g. less social interaction, reliance on machines, less privacy, and the potential erosion of trust. Distrust and suspicion of AmI systems appear key concepts that emerged from the group discussions in this study, and bear much further examination and understanding.

This book is dedicated to the concept of trust. However, if we begin to rely on systems to make decisions on our behalf by setting prior preferences do we actually need to understand the concepts of privacy and trust? For AmI systems to work societies need to be at least somewhat transparent. To be truly transparent then we need complete trust and have no concern over privacy. The enigmatic nature of trust, privacy and social values questions whether we can really understand this type of puzzle or even create a clear vision for future interactions with AmI systems.

Future directions

Ambient intelligence is now an area intensely researched and undergoing rapid development already visible in advanced mobile, PDA and notebook services. The vision of a future filled with smart and interacting everyday objects offers a whole range of possibilities. To some the scenarios described in this chapter might appear somewhat ‘unrealistic’. However if Weiser’s vision is to be realised then we must acknowledge the advantages and disadvantages this transformation will have on society. For example, sensor and communication mechanisms in the environment will help people with disabilities lead a more independent life. We will be able to track everything from

children, family, and friends to missing keys. However we must question whether the transformation that will take place is ethical or even socially acceptable. Do we want or need to rely on embedded devices seamless exchanging information on our behalf? Clear methodologies that allow in-depth investigation into how information exchange in an ambient world can be made trustworthy, secure and private are needed. This requires cross-disciplinary approaches where evaluation is based on both the technical and social aspects of such interactions.

The next stage in the research reported in this chapter is to develop a survey developed from the project findings. The survey will be a useful tool in measuring concepts related to trust, privacy and social issues when considering ambient devices and information exchange. The findings will give further insight into how ambient devices can be designed to deliver specific services and information and therefore acceptance.

References

Abdul-Rahman, A. (2004). *A Framework for Decentralised Trust Reasoning.* PhD Thesis, University of London.

Ahas, R., & Mark, Ü. (2005). Location based services - new challenges for planning and public administration? *Futures* 37(6): 547-561

Altman, I. (1975). *The Environment and Social Behavior.* Belmont, CA: Wadsworth.

Altman, I. & Chemers, M. (1989). *Culture and Environment.* Cambridge: Cambridge University Press.

Arndt, C. (2005). The loss of privacy and identity

Biometric Technology Today, Volume 13, Issue 8, Pages 6-7

Beslay, L. & Punie, Y. (2002). The virtual residence: Identity, privacy and security. IPTS Report 67, Institute for Prospective Technological Studies. Special Issue on Identity and Privacy.

Bies, R. J. (2001). Interactional (in) justice: The sacred and the profane. In J. Greenberg & R. Cropanzano (Eds.), *Advances in organisational justice.* (pp 89-118). Stanford CA: Stanford University Press

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F, & Rohs, M. (2005). Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In Weber, W., Rabaey, J. & Aarts, E. *Ambient Intelligence*. Berlin: Springer.

Bødker, M. (2004). Trust and the digital environment. Downloaded March 2006 http://www.itu.dk/people/boedker/trustpaper.pdf

Bok, S. (1978). *Lying: Moral Choice in Public and Private Life.* New York: Pantheon Books.

Boon, S. D. & Holmes, J. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. *Pp190-211 of* Hinde, R. A. & Groebel, J. (Eds), *Cooperation and Prosocial Behaviour*. Cambridge University Press.

Bickmore T. & Cassell, J. (2001). Relational Agents; A Model and Implementation of Building User Trust. *Proceedings CHI 2001, pp396-403.*

Brandies, L.D. & Warren, S. (1890). The right to privacy: the implicit made explicit. *Harvard Law Review, 4,* 193-220

Brien, A. (1998). Professional ethics and the culture of trust. Journal of Business Ethics 17 (4) 391-409.

Briggs, P. (2004). Key issues in the elicitation of disclosure preferences fro ambient intelligence – a view from a window. Paper presented at *Considering Trust in Ambient Societies* workshop, CHI 2004, Vienna, Austria.

Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. England: Perseus Press

Boni, M., & Prigmore, M. (2002). Cultural Aspects of Internet Privacy, Proceedings of the UKAIS 2002 Conference, Leeds, UK

Burgoon, J.K. (1982). Privacy & Communication. *Communication yearbook. 6. 206-249.*

Chan, Y. (2000). Privacy in the family: Its hierarchical and asymmetric nature. *Journal of Comparative Family Studies, 31 (1).* 1-23.

Chang, E., Thomson, P., Dillon, T. & Hussain, F. (2004). The Fuzzy and Dynamic Nature of Trust, pp 161-174 of Katsikas, S., López, J. & Perum, G. (Eds): *TrustBus 2005*. LNCS 3592. Berlin: Springer.

Cheskin Research & Studio Archetype/Sapient. (1999). *eCommerce Trust Study*. http://www.cheskin.com/think/studies/ecomtrust.html;

Cheskin Research. (2000). *Trust in the Wired Americas*.http://www.cheskin.com/p/ar.asp?mlid=7&arid=12&art=0

Clarke, R. (1999). Introduction to Dataveillance and Information privacy, and Definitions of terms. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html Downloaded January 2004

Consolvo, S., Smith, I.E. Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). 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

Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). Online trust: concepts, evolving themes, a model. *International Journal of Human Computer Studies 58:737-758.*

Cramer, L. (2002). *Web privacy with P3P*. USA: O'Reilly & Associates

Cranor, L.F., Reagle, J., & Ackerman, M.S. (1999). Beyond concern: understanding net users' attitudes about online privacy. In I. Vogelsang & B. Compaine (Eds.), *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*. USA: MIT Press. pp 47-60.

Dawson, L., Minocha, S., & Petre, M. (2003). *Social and Cultural Obstacles to the (B2C) E-Commerce Experience.* Paper presented at the People and Computers XVII - Designing for Society, 225-241

Dibben, M. R. (2000). *Exploring Interpersonal Trust in the Entrepreneurial Venture.* Hampshire: MacMillan Press.

Dritsas, S., Gritzalis, D., & Lambrinoudakis, C. (2005). Protecting privacy and anonymity in pervasive computing trends and perspectives. *Telematics and Information*. In Press

Egger, F.N. (2003). From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce. PhD Thesis, Eindhoven University of Technology (The Netherlands).

Egger, F N. (2000). Trust Me, I'm an Online Vendor. Pp101-102 of *CHI 2001 Proceedings Extended Abstracts.*

Falcone, R. & Castelfranchi, C. (2001). The Socio-Cognitive Dynamics of Trust; Does Trust Create Trust?, in Falcone, R., Singh, M. & Tan, Y-H. (Eds): *Trust in Cyber-Societies. LNAI 2246,* pp55-72. Berlin: Springer.

Fiske, A.P., Kitayama, S., Markus, H.R., & Nisbett, R.E. (1998). The cultural matrix of social psychology. In D.T. Gilbert, S.T. Fiske & G. Lindzey (Eds.). *The handbook of Social Psychology, 4th Edition, Vol.2.* Boston: McGraw-Hill. (pp. 915-981).

Friedman, B., Kahn, P. H., & Howe, D. C. (2000). Trust Online. *Communications of the ACM*43 (12):34-40. December.

FTC Study (2000) Privacy Online: Fair Information Practices in the Electronic Marketplace. A Report to Congress May.

Fukuyama, F. (1996). *Trust: The Social Virtues and the Creation of Prosperity*. New York: Free Press.

Fung R. K. K., & Lee, M. K. O. (1999). EC-Trust (Trust in Electronic Commerce): Exploring the Antecedent Factors. Pp517-519 of *Proceedings of the American Conference on Information Systems.*

Good, D. (2000). Individuals, Interpersonal Relations, and Trust. in Gambetta, D. (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 3 pp31-48. http://www.sociology.ox.ac.uk/papers/good31-48.pdf

Gambetta, D. (2000). Can we Trust Trust, in Gambetta, D. (ed.) *Trust: Making and Breaking Cooperative Relations,* electronic edition, Department of Sociology, University of Oxford, chapter 13, pp213-237. http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

Gotlieb, C.C. (1996). Privacy: A concept whose time has come and gone. In D. Lyon and E. Zureik (Eds.), *Computers, Surveillance and Privacy.* USA: University of Minnesota Press. pp 156-171.

Jackson, L., von Eye, A., Barbatsis, G., Biocca, F., Zhao, Y., & Fitzgerald, H.E. (2003). Internet Attitudes and Internet Use: some surprising findings from the HomeNetToo project. *International Journal of Human-Computer Studies, 59.*

Jarvenpaa, S., Tractinsky, N., & Saarinen, L.(1999). Consumer Trust in an Internet Stroe: A Cross-Cultural Validation. *Journal of Computer Mediated Communication* 5(2):December. http://jcmc.indiana.edu/vol5/issue2/jarvenpaa.html

Jessup L., & Robey D. (2002) The Relevance of Social Issues in Ubiquitous Computing Environments. Communications of the ACM 45(12). 88-91.

Karvonen, K.(1999). Creating Trust. In *Proceedings of the 4th Nordic Workshop on Secure IT Systems (NordSec 99).* November 1-2, 1999, Kista, Sweden.

Kaya, N., & Weber, M.J. (2003). Cross-cultural differences in the perception of crowing and privacy regulation: American and Turkish students. *Journal of Environmental Psychology. 32.* 301-309

Kozlov, S. (2004). *Achieving Privacy in Hyper-Blogging Communities: privacy management for Ambient Technologies.*

http://www.sics.se/privacy/wholes2004/papers/kozlov.pdf Downloaded June 2004

Lester, T. (2001). The Reinvention of Privacy. *The Atlantic online*. http://www.theatlantic.com/issues/2001/03/lester-pt.htm Downloaded September 2001

Lewis, J. D., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces 63(4):967-*985. June.

Little, L., Briggs, P., & Coventry, L. (2005). Public Space Systems: Designing for privacy? *International Journal of Human Computer Studies*.63, 254-268

Little, L., Briggs, P., & Coventry, L. (2004). Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. BHCIG Conference, Leeds, September 2004

Luhmann, N. (1979). *Trust and Power*. Chichester: Wiley.

Luhmann, N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives, in Gambetta, D. (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 6, pp94-107. http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf

Luft, J. (1969). *Of Human Interaction.* Palo Alto, CA:National Press

Margulis, S.T. (2003). On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social issues, 59 (2).* 411-429.

Marsh, S. (1994). *Formalising Trust as a Computational Concept.* PhD Thesis, University of Stirling, Scotland. Available online via www.stephenmarsh.ca

Marsh, S. (2005). *Artificial Trust, Regret, Forgiveness, and Boing.* Seminar given at University of St Andrews, Scotland, 4th October, 2005. Available online via www.stephenmarsh.ca

Marsh, S., & Dibben, M. R. (2003). The Role of Trust in Information Science and Technology, in Cronin, B. (Ed.), Annual Review of Information Science and Technology, 37 (2003): 465-498.

McCandlish, S. (2002). EFF's Top 12 ways to Protect Your Online Privacy. *Electronic Frontier Technology*. http://www.eff.org/Privacy/eff_privacy_top_12.html Downloaded January 2004

Metzger, M. J. (2004). Exploring the barriers to electronic commerce: Privacy, trust, and disclosure online. Journal of Computer-Mediated Communication, 9(4)

Misztal, B. (1996). *Trust in Modern Societies*. Cambridge: Polity Press.

Moor, J.H. (1997) Towards a Theory of Privacy in the Information Age. *Computers and Society, 27*, 3, 27-32.

Nguyen, D.H.,& Truong, K.N. (2003). PHEmail: Designing a Privacy Honoring Email System. *Proceedings of CHI 2003 Extended Abstracts*, Ft. Lauderdale, Florida,

Nijholt, A. Rist, T., & Tuinenbrejier, K. (2004). Lost in ambient intelligence? In: Proc. *ACM Conference on Computer Human Interaction (CHI 2004),* Vienna, Austria.

Olsen, K., Grudin, J., Horvitz, E. (2005) 'A study of preferences for sharing and privacy'. *CHI, 2005 extended abstracts on Human factors in computing systems*

Palen, L., & Dourish, P. (2003). Unpacking Privacy for a Networked World. *Proceedings of the ACM, CHI 2003,5 (1), 129- 135.*

Patrick, A., Briggs, P. & Marsh, S. (2005). Designing Systems that People Will Trust, in Cranor, L. F. & Garfinkel, S., *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly.

Pedersen, D.M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology, 19.* 397-405.

Pedersen, D.M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17.* 147-156.

Pedersen, D.M. (1979). Dimensions of privacy. *Perceptual and Motor skills, 48.* 1291-1297.

Perry, M. O'Hara, K. Sellen., Brown. & Harper, R. (2001). Dealing with Mobility: Understanding Access Anytime, Anywhere. *ACM Transactions on Computer-Human Interaction, 8, (4).* 323-347.

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. *International Journal of Human-Computer Studies, Volume 63, Issues 1-2, Pages 228-253*

Punie, Y. (2003). *A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend?* Key deliverable, The European Media and Technology in Everyday Life Network (EMTEL).

Riegelsberger, J. & Sasse, M. A. (2001). Trustbuilders and Trustbusters. pp 17-70 of *Towards the E-Society: Proceedings of the First IFIP Conference on E-Commerce, E-Society, and E-Government*. London: Kluwer.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. & Camerer, C. (1998). Not so Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*. 23(3):393-404.

Siau, K.& Shen, Z. (2003). Building Consumer Trust in Mobile Commerce. *Communications of the ACM* 46(4):91-94. April.

Sillence, E., Briggs, P., Fishwick, L. & Harris, P. (2004). Trust and Mistrust of Online Health Sites. Proceedings of CHI'2004, April 24-29 2004,Vienna Austria, p663-670. ACM press

Shneiderman, B. (2000). Designing Trust Into Online Experiences, in Communications of the ACM, December 4.12

Streitz, N., & Nixon, P. (2005). The disappearing computer. *Communication of the ACM, 48, 3,* 32-35

Sztompka, F. (1999). *Trust: A Sociological Theory*. Cambridge University Press.

Thibaut, J. W. and Kelley, H. H. (1959) *The social Psychology of Groups*, New York: Wiley

Viljanen, L. (2005). Towards an Ontology of Trust. pp 175-194 of Katsikas, S., López, J. & Perum, G. (Eds): *TrustBus 2005*. LNCS 3592. Berlin: Springer.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American* 265(3):66-75. September.

Westin, A. (1967). *Privacy and freedom.* New York: Atheneum

Table 1: Privacy, trust and social issues related to AmI use

	Information		
	Device	User	Stakeholder
Trust:			
personalisation	x	x	x
expertise		x	
predictability		x	x
source		x	x
Risk:			
reliance and responsibility	x	x	x
Privacy:			
physical		x	
informational	x	x	x
psychological		x	x
social		x	x
choice		x	
control		x	
security	x	x	x
Social issues:			
exclusion		x	
social and moral values		x	x