Pervasive Prying? Trust, Privacy and Identity Issues for Ubiquitous Computing

Abstract

Developments in ubiquitous and pervasive computing herald a future in which computation is embedded into our daily lives. Such a vision raises important questions about the circumstances under which we would trust such systems, the means by which we might achieve and maintain privacy and manage online identities. To begin to address such issues, we have recently conducted a wide reaching study eliciting trust, privacy and identity concerns about pervasive computing. Over three hundred UK citizens participated in 38 focus groups. Each group was shown four Videotaped Activity Scenarios [22] depicting pervasive or ubiquitous computing applications in four contexts: health, finance, commerce and e-voting. The resultant data was coded in terms of stakeholder, user and system issues. The data is discussed here from the stakeholder perspective – specifically in terms of concerns about trust, privacy and identity.

Keywords

Ubiquitous computing, pervasive computing, trust, privacy, disclosure, identity management.

1 Introduction

Ubiquitous computing (ubicomp) refers to the convergence of communication technologies, computing devices, and interfaces that adapt to the needs and preferences of the user. It evokes 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.

One of the key issues for ubicomp research concerns just how much information an individual is prepared to reveal about him or herself at any one time. We commonly carry devices (mobile phones, personal digital assistants) that exchange personal information with other devices – often without our explicit knowledge. Ubiquitous computing depicts a future in which devices embedded in the environment and potentially in the body will use software agents to communicate seamlessly about any number of different things: our present state of health, our preferences for what to eat, our schedule, our credentials, our immediate destination, our need for a taxi to get us there in 10 minutes. Questions naturally arise: Do people want information to be shared in this way? What are the social and psychological consequences? How will people manage the process, given the vast quantity of information exchanged?

Development in technology has never had the explicit goal of altering civilisation [2]. The ubicomp vision is to fully computerise society, therefore we must question whether ubiquitous technology will change the way humans interact socially. Friedewald et al [10] question whether ubicomp systems will fulfil most of the promises made by researchers or whether the vision is just an illusion? Living in a ubiquitous society suggests effortless communication, our needs, wants and desires met. The exchange of information has vast social implications and might not decrease but actually increase the complexity of life.

Ubiquitous systems hold the danger of increasing social pressure and the digital divide [10]. Ubicomp has the potential to create an invisible and comprehensive network

monitoring our private and public life [2]. There is a chance people will become monitored and penalised by stakeholders for not adopting and using such systems. For example, insurance companies only insuring a person if they have a health monitoring system. What will motivate people to use such systems if there is a chance of exploitation?

The ubicomp vision involves multiple stakeholders, delivering services in a timely, convenient and appropriate fashion. However, people already have concerns over personal data storage, exchange, mining and unauthorized access by third parties [24]. The aim of this study is to develop a better understanding of such concerns. Specifically we are interested in knowing more about the kinds of stakeholders or agents that will be trusted within the ubiquitous computing network, about the privacy preferences that might be acceptable and the disclosure permissions that might control the passage of personal information and finally, about how different levels of disclosure might be associated with the maintenance and communication of electronic identities. In short, we are interested in knowing more about user requirements for privacy, trust and identity management in a ubiquitous computing world.

1.1 Privacy

Privacy is a multi-dimensional construct encompassing physical and social judgments [28]. Two types of privacy – physical and informational privacy – are particularly relevant to ubicomp research. Physical privacy in the anywhere, anytime, ubiquitous society is a critical issue. Individuals will have access to information in a huge variety of environments – often while interacting with friends, family or work colleagues. The act of receiving personal information in the presence of others can be a highly stressful event, often resulting in feelings of anxiety and intimidation [23]. Research has shown how concerns about privacy and personal space have a direct affect on attitude and intention to use public technologies [21].

Informational privacy is also a crucial issue for the E-Society. Internet users have major concerns about the threat to their privacy [8] and many are very anxious about the information they provide online [14]. Privacy preferences vary considerably between users and so various architectures have been suggested that allow personalized settings [18]. A few architectures and models have been proposed for understanding privacy issues with regard to ubicomp systems e.g. Privacy Risk Model [17], Five Pitfalls for Designers [20]. Other researchers have discussed the need to understand privacy and consider issues in ubicomp systems related to feedback and control [1], Fair Information Practise [19], negotiation of boundaries [27].

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 [11] 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. However, these architectures or models tend to focus on the design of the system and often ignore the transference of responsibility to the individual [31].

In such a complex information environment, how do users set the rules regarding when to relax permission preferences and when to tighten them? How will users know their personal information is transmitted and stored securely? To a certain extent this emerges as a judgment of trust.

1.2 Trust

Trust and privacy are inter-related constructs – the more we trust, the more information we are prepared to reveal about ourselves [4, 31]. For many ordinary users, the simple act of posting an opinion on a discussion board, filling in an online form or making an e-commerce purchase is an act enabled by trust [7, 13]. This shouldn't be surprising, since social commentators recognise that trust is essential for society [3, 12], however an interesting picture is emerging about the ways in which individuals make trust judgments in technology-mediated interactions. In rapid, short-term exchanges over the Internet, for example, trust is secured on the basis of some emotional reaction to the look and feel of a site [9, 30]. True, more protracted engagement is dependent upon issues such as perceived credibility and familiarity with the vendor – but trust judgments are not always made on a rational basis. This raises interesting questions regarding permission setting within an ubiquitous 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 [26]. In order to address these issues we need to improve the user's understanding about the mechanics of trust in mediated interactions, i.e. do they have enough knowledge to be in control, and if not, how can informed control be achieved?

1.3 Identity management

One inevitable aspect of ubiquitous information exchange is that devices will be empowered to communicate personal identifiable information to other devices – but the whole constructs of identity and disclosure are complex [15, 29]. Any individual holds multiple identities and in face-to-face communication chooses to engage the identity most appropriate for that particular context. The same process holds true of an individual interacting with technology – although we should note here that people can quickly become uncomfortable when asked to provide identity details online [e.g. 8].

Joinson [15] found three times as much self-disclosure in computer-mediated communication dyads compared to face-to-face pairs. However, later work [16] suggests that this effect is reduced when people's anonymity is compromised through personalization technologies, particularly when a powerful audience may be viewing the disclosed material. This implies that people may well be faced with a form of generalised anxiety if and when identity detection becomes automatic. How can they be sure that their identity information is screened appropriately, so that the right information is offered at the right time?

2 Method

The first requirement of the project was to find a means to communicate the concept of Ubiquitous computing to the ordinary citizen. There are many potential visions of the future and so we engaged with a number of key stakeholders in order to generate specific scenarios capable of communicating something about agent technologies and the trust, privacy and identity issues they evoke. The stakeholders included relevant user groups, researchers, developers, businesses and government departments with an interest in ubiquitous computing 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 and category of information transmitted.

2.1 Development of Videotaped Scenarios

The elicited scenarios were then used to create four 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 [22]. 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. 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. All scenarios were approximately three minutes in length. As an illustration, the health scenario is 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) about his circumstance. The emergency management agent transfers the planning application files to John's PDA so the company does not miss the deadline. The agent also informs Bob's 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.

2.2.Participants

The VASc's were shown to 38 focus groups, the number of participants in each group ranged from four to twelve people. The total number of participants was 304 and they received £10 each for attending a session. 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 additional sessions were held 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 upon Tyne. The forum was considered to have easier access and dedicated facilities for people with such disabilities.

2.3. Technical Classification

To classify participants into technical or non-technical six questions based on a categorization process by Maguire [25] 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:

1) If your personal devices e.g. mobile telephone or computer were taken away from you tomorrow, would it bother you?
2) Do you think that we rely too much on technology?
3) Do you enjoy exploring the possibilities of new technology?
4) Do you think technologies create more problems than they solve?
5) Is Internet access important to you?
6) 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 ubiquitous 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 ubiquitous 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 ubiquitous 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. This was to maintain the same experience for all groups and make the transcriptions easier to document. 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 ubiquitous systems were also noted. The duration of the sessions was approximately ninety minutes.

3 Analysis

All group discussions were transcribed then read; a sentence-by-sentence analysis was employed using the Atlas.ti™ qualitative software programme. Two members of the research team coded and compared the data for consistency, good inter-rater reliability was found. The data was open coded using qualitative techniques and several categories were identified. The data was then grouped into categories using sentences and phrases from the transcripts. Categories were then grouped into the different concepts, some of the main concepts were found to be multidimensional and interrelated e.g. trust and privacy.

A number of network views were derived from the analysis, relating issues surrounding the stakeholder, the user and the device. In this paper we unpack the trust, privacy and disclosure issues surrounding the stakeholder.

3.1 Trust

Participants expressed concerns about whether the stakeholders or their agents could be trusted to control and contain the exchange of information. The ability of individuals to interrogate the system or influence the release of personal data was a key issue. Trust was positively associated with the constructs of credibility, predictability, personalisation,

Stakeholder credibility

Credibility in a ubicomp world is underpinned by concepts such as loyalty and reputation, but undermined by fears of monopolization. For example, banks were seen as credible institutions with good reputations in terms of privacy and security, but were also seen as powerful institutions capable of changing the rules of the game.

'Banks have been established for years and people have always trusted them more. … but if banks changed to become more impersonal with more technology that view would probably change'.

Stakeholder motivation was perceived as a key component of trust in the system, given that stakeholders were capable of monitoring goods and people. Participants raised concerns over stakeholders using ubiquitous systems to pressure people in buying goods, creating user profiles and monitoring people's behaviour:

'it will bind you into the supermarkets even more than we are bound in now. The fact that all your details are registered with someone … as supermarkets become more powerful and then they have got a monopoly, the choice will be less rather than more. So you are sucked into one supermarket and then they have got you.'

Participants also queried the credibility of 'agent' systems as they felt agents would be inextricably linked to different stakeholders, each with differing credibility. For example, if an agent was used to find information out about a personal loan, would they only return information from credible companies? The issue of trust transfer (from a trusted to an unknown third party) was seen as threatening.

'I don't like the feeling that the avatar knows everything about me. It's as though I can't differentiate between who is who.'

Flexibility

Participants queried the extent to which systems could be trusted to faithfully reflect unpredictable day-to-day changes in human behaviour. In other words, participants felt that the human capacity for capriciousness should be honoured, but worried that it may be threatened by rigid computational systems. Participants commented that we act and react in different ways depending upon with whom we are interacting, when and where.

Setting up privacy profiles and permissions may become too time-consuming, reducing the utility of such systems.

'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'.

Personalisation

Participants recognised that a personalised system would be useful to them and more reflective of their needs, often discussing these issues in terms of the kinds of personal services they used to receive before the advent of computer-based services:

'I've been with the same bank… for forty odd years … I don't think people have the sense of loyalty to organisations that they used to have, because the attitudes of the banks themselves has changed. I mentioned the fact that the bank manager knew you and you knew him, usually a him, but that has all changed so they're a little more impersonal than they were.'

Participants also expressed concern that personal information could be exploited and wondered about the stakeholder's sensitivity regarding sending and receiving personalised information in a timely manner (recognising the potential for privacy violations).

'If your fourteen year old uses condoms or whatever and it is shouting at you in the supermarket saying 'you need more condoms'. Is that social inclusion or exclusion?'

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, or those on different types of medication, having their health information being disclosed to the relevant people when needed.

'Well it would be very handy if you had a serious complaint. … I'm on loads of tablets and that way if something happened … I could find it a lot easier than having to tell people what you're on and what you're not'

Participants were also aware of the need for good standards of authentication – generally feeling that secure authentication mechanisms such as biometric verification systems would be beneficial.

Transparency

Transparency was also linked to data storage, mining, exchange and access by third parties. Participants commented systems needed to be transparent and accessible so information could be verified and changed. Participants acknowledged stakeholders already hold information about you that you are unaware of and this should be made more transparent.

'I mean they don't really know where the information is going and what individuals are actually accessing it or is it just completely churned up by computers? I don't even know but the information is going somewhere and the customer, the consumer should actually have, be allowed to know where that information is going and it should be an

open process, open to the consumer, if the consumer wants to know of course, some people might not want to know, but if the consumer wants to know how all that information is processed it should be open.'

3.2 Identity

Identity was discussed both in terms of disclosure preferences and self-reliance incorporating issues of autonomy and control. Participants were keen to discuss the kinds of risk involved in being too open about personal matters, but also recognized that certain benefits would be denied in circumstances where disclosure was closed.

Disclosure preferences

Participants expressed concerns about controlling the disclosure of personal information. 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 as, for example, with family then the majority of information is shared quite freely. However, sharing even with a close family member depends on situation and context. Participants expressed concern over stakeholders sharing personal information with third parties, creating profiles, making inferences from personal information.

'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.'

Interestingly, visually impaired participants commented they have to generally disclose personal information to family, friends and even strangers when they want to use different technologies even when they don't want to. For example, visually impaired participants discussed disclosing personal information when using an automated teller machine.

Risk and responsibility

Participants discussed issues of risk and responsibility in relation to self-reliance. They acknowledged that both system and self might be unreliable. For example in the shopping scenario the user was given an alert about a food allergy. Participants discussed liability and litigation - 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?'

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 ubiquitous 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'*.

Autonomy – choice and control

Participants commented little or even no choice would exist in an ubiquitous 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, or because someone else hasn't thought to include you in their circle:

'It is all going to become mechanical isn't it. What is laid out and certain people are in, certain people are out. No I don't really see that that is an advantage at all.'

Participants were concerned about reliance on ubiquitous systems reducing personal control. Discussions revealed ubiquitous 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.'

3.3 Privacy

Participants recognized various types of privacy but were also keen to discuss issues of choice and control. This went beyond the issue of how much information to disclose and encompassed discussion of whether or not individuals would be able to live their lives outside of the ubiquitous lens.

In this study the analysis for privacy was interpreted and based on three dimensions proposed by Burgoon [5]: informational, physical and social. 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. The physical dimension relates to how physically accessible a person is to others and can be linked to such aspects as environmental design. The social dimension is the ability to control social interactions by controlling distance between people. This dimension is associated with physical privacy and often a natural consequence of it.

Informational

The concept of informational privacy was a major concern for all participants. Participant's highlighted complex patterns and exchange 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 and exchange 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.

'Because I'm worried if they have got that information like a Smartcard, you know life insurance … so if you buy any cigarettes or any alcohol, you know it is going to maybe invalidate the life insurance that you have'.

'…for example, if I was a smoker, which I am not, and I was buying cigarettes it is the first step to typing up with your health record and whether you get health treatment through your doctor'.

Social
Participants discussed the social elements of ubiquitous technologies – fearing on the one hand that ubiquitous technology would foster social isolation. Participants believed that as systems increased social privacy less human-human interaction would take place, with enormous negative consequences.

'Unseen by a human, did not speak to a human, you don't need any human beings in a place like that, oh crumbs! Gosh!'

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 – as a consequence, 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 always want to share every detail and this could be a problem with future technologies:

Physical
Participants commented that ubiquitous 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.

'What I wouldn't like would be if you stepped inside the door and it started greeting before you even as much as blinked.'

Participants commented on the lack of physical privacy through surveillance systems, although they agreed surveillance would be beneficial for some people with certain medical conditions.

'It could work against you like at work for checking what you are doing and everything. Will your boss know what you are doing outside of work?'

'Nowadays there is the CCTV so therefore they could 'track' you if they wanted to but its how they use this information itself. This one offends me. Too much is taken out of your hands. What I do not like is that you cannot get away from them'

'In fact I wouldn't mind being tracked if I had epilepsy, if I was in certain circumstances or had a heart condition. In that situation I wouldn't mind.'

4 Discussion
Our stakeholders provided more questions than answers: Who is receiving the information? Who else has access? Is the receiver credible? Why do they want to know? Can we see where the information goes? Can we control access or change the permissions? Will we have any choice in becoming part of the system? How will agents determine who to trust? Who will be liable when things go wrong? Who controls the legal rights in an international exchange? Will technology change the nature of what it is to be human?

A common question was whether an individual might be allowed to make day to day decisions about who or what to trust on an ad hoc basis, or would be drawn to adopt agents to represent their personal trust and privacy preferences and communicate these to other agents [26]. Participants also commented that entrusting and relying on agent systems to exchange information was dehumanising Stakeholders and designers of ubiquitous systems need to consider the fact humans are inherently social beings and their actions are always directly or indirectly linked to other people.

Disclosure of information in any form or society is a two-way process. Findings support the Fair Information Practice-FIP [e.g. 11] that suggests companies should give users: notice, choice, access and security.

Hong et al [17] suggest designers of ubicomp systems need to deploy a privacy risk analysis considering social and organisational content. This type of analysis considers: Who are the users? What kind of personal information is being shared? How is personal information collected? Hong et al [17] suggest after the initial privacy risk analysis designers need to prioritise the findings and develop a privacy risk management record. The privacy risk management considers: What are the default settings? How does unwanted disclosure take place? [See 17 for a complete review]. Although our findings generally support the work of [17] we need to further understand how the user will manage information exchange in an ubicomp world.

We need to consider the following guidelines when considering adoption and use of ubiquitous systems:
Choice: the option to reveal or hide information and to use or not use ubicomp systems
Control: the ability to manage, organise and have power over all information exchanged and to be notified of information held about you
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
Global rules and regulations: a global infrastructure of rules related to information exchange
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
Trust and privacy preference: the need for the user to set preferences that can be dynamic, temporary and secure
Context: the need to know the location and exact environment of the user
Social: the need to know who else is present and the current situation the user is in

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 ubiquitous 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 ubiquitous technology blur the boundaries between home and workplace making society one of efficiency and productivity taking over from love and leisure time?

Interestingly, although participants were grouped by technical stance, age, gender and educational achievement the recurrence of themes across groups were similar. This suggests ubiquitous systems raise similar issues for all relevant users. The majority of participants agreed ubiquitous systems for monitoring health were advantageous, especially for people with medical conditions. Participants reported high levels of trust with the stakeholders involved in the healthcare scenario and were keen to discuss the benefits of ubiquitous in this context e.g. healthcare professionals being alerted to any allergies and automatic access to health records. However, concerns were raised over unauthorised access and misuse of key information (e.g. insurance companies having uncontrolled access to confidential health information; employers accessing health records). These findings support the view of California Healthcare Foundation [6] in that people are worried about third party access. These findings have major implications for ubiquitous systems.

Ubiquitous systems were associated with substantial perceived benefits, including less time pressure, no queuing for goods, and memory enhancements. However potential social costs were felt to be great – involving reduced social interaction, reliance on machines, little or no privacy, and the potential erosion of trust. Distrust and suspicion of ubiquitous systems appear key concepts that emerged from the group discussions in this study, and such concepts would bear further examination.

Ubiquitous computing is 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, but our participants invite us to pause and ask whether the transformation that will take place will be socially acceptable. In the views of many of our participants, this will never be an issue of individual choice. Market forces, peer pressure or fear-fuelled state policies will bring the change about – and new tools and toys, sometimes delightful and sometimes sinister, will proliferate – few of them judged on the basis of social value. The vision of a comprehensive network of agents capable of monitoring our private and public life [2] is not entirely welcomed by our own participants who worry that non-adoption will be penalised by stakeholders (e.g. insurance companies only insuring a person if they have a health monitoring system) or will lead to social exclusion.

The data in this study is vast and still being explored. Comparisons need to be made between groups, gender, age and the four different scenarios. All four scenarios related to everyday happenings e.g. shopping, a medical emergency, finance, however, further in-depth analysis might reveal that exchange of information in an ubicomp world has different levels and disclosure patterns. From the findings in this study a large scale survey has been developed and is currently being distributed to participants on a global scale.

Development in technology has never had the explicit goal of altering civilisation [2] and it is possible that the ubiquitous vision we have portrayed in our scenarios will not ever be fully realised [9], but we would welcome a research agenda that encourages the development of explicit tools and techniques designed to place human values at the heart of technological development.

5 References

1. Bellotti, V., Sellen, A. Design for Privacy in Ubiquitous Computing Environments. Proc. ECSCW '93, Kluwer A.P., Dordrecht, The Netherlands (1993).

2. Bohn, J., Coram, V., Langheinrich, M., Mattern, F., Rohs, M. Social, Economic, and Ethical Implications of Ubiquitous computing and Ubiquitous Computing. Ubiquitous computing, Springer-Verlag, (2005). 5-29.

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

4. Briggs, P., Simpson, B., and De Angeli, A. Trust and personalisation: A reciprocal relationship? In C-M Karat, J. Blom and J. Karat (Eds), Designing Personalized User Experiences for eCommerce. Kluwer. (2004).

5. Burgoon, J.K. Buller, D.B. & Woodhall, W.G. (1989). *Nonverbal communication: The unspoken dialogue*. New York: Harper Row.

6. California Healthcare Foundation. Ethics survey of consumer attitudes about health web sites. (2000). Downloaded August 2006 http://www.chcf.org/press/viewpress.cfm?itemID=1015)

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

8. Cranor, L.F., Reagle, J., & Ackerman, M.S. 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. (1999). pp 47-60.

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

10. Friedewald, M., Costa, O., Punie, Y., Alahuhta, P., Heinonen, S. Perspective of ubiquitous computing in the home environment. Telematics Information, 22 (3), (2005). 221-238

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

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

13. Huang, H., Keser, C., Leland, J., and Shachat, J. Trust, the internet, and the digital divide. IBM Systems Journal, 42(3) (2003).507–518

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

15. Joinson, A. N.. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. European Journal of Social Psychology, 31, (2001)177-192.

16. Joinson, A.N., Woodley, A., & Reips, U-R. Personalization, authentication and self-disclosure in self-administered Internet surveys. In press, Computers in Human Behavior, 23, (2007). 275-285.

17. Hong, J.I., Ng, J.D., Lederer, S. & Landay, J. Privacy risk models for designing privacy-sensitive ubiquitous computing systems, Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques, Cambridge, MA, USA

18. Kobsa, A. A component architecture for dynamically managing privacy constraints in personalized web-based systems. In Proceedings of the Third Workshop on Privacy Enabling Technology, Dresden, (2003).Germany. Springer Verlag.

19. Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, Proceedings of the 3rd international conference on Ubiquitous Computing, p.273-291, September 30-October 02, 2001, Atlanta, Georgia, USA

20. Lederer, S., Hong, J.I. Dey,K., & Landay,A. Personal privacy through understanding and action: five pitfalls for designers, Personal and Ubiquitous Computing, v.8 n.6, p.440-454, November 2004

21. Little, L., Briggs, P., Coventry, L., & Knight, D.J. Attitudes Towards Technology Use in Public Areas: The Influence of External Factors on ATM use. In C. Stephanidis & J. Jacko (Eds.) *Human-Computer Interaction: Theory and Practice (Part II). Volume 2.* (2003). (pp. 1233 – 1237). Lawrence Erlbaum Associates: NJ

22. Little, L., Briggs, P., & Coventry, L. Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. British Human Computer Interaction Conference, Leeds, September 2004

23. Little, L., Briggs, P., & Coventry, L. Private whispers/public eyes: Assessing the psychological cost of receiving highly personal information in a public space Journal of Experimental Psychology Applied. Submitted April 2006

24. Little, L., Marsh, S., & Briggs, P. Trust and privacy permissions for an ambient world. Book chapter to appear in R. Song, L. Korba, G. Yee (Eds.) Trust in e-services: technologies, practices and challenges. (2006).

25. Maguire, M.C. A Review of User-Interface Guidelines for Public information kiosk Systems. International journal of Human-Computer Studies, 50. (1998). 263-286

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

27. Palen, L. and P. Dourish, Unpacking "Privacy" for a Networked World. CHI Letters, 2003. 5(1): p. 129--136.

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

29. Schlosser, F. So, how do people really use their handheld devices? an interactive study of wireless technology use. Journal of Organizational Behaviour, 23: (2002). 401–423.

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

31. Teltzrow M., & Kobsa, A. "Impacts of User Privacy Preferences on Personalized Systems - a Comparitive Study", In Proc' CHI2003.

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