Pervasive healthcare: the elderly perspective

Linda Little
PaCT Lab
School of Psychology & Sports Science
Northumbria University
+44 191 243 7250
l.little@northumbria.ac.uk

Pam Briggs
PaCT Lab
School of Psychology & Sports Science
Northumbria University
+44 191 227 4750
p.briggs@northumbria.ac.uk

Abstract
The pervasive vision of future technologies raises important questions on how people, especially the elderly, will be able to use, trust and maintain privacy. To begin to address such issues, we conducted focus group sessions with elderly participants aged from 65 to 89 years. The groups were shown three Videotaped Activity Scenarios [5] depicting pervasive or ubiquitous computing applications in three contexts: health, commerce and e-voting. The resultant data was coded in terms of stakeholder, user and system issues. The data is discussed here from the user perspective – specifically in terms of concerns about trust and privacy.

Categories and Subject Descriptors
K.4.1 privacy, K.4.2 social issues, k.6.5 security

General Terms
Design, Reliability, Security, Human Factors,

Keywords
Trust, privacy, ubiquitous computing, elderly

1. INTRODUCTION
Pervasive systems and ubiquitous computing (ubicomp) refer to the convergence of communication technologies, computing devices, and interfaces that adapt to the needs and preferences of the user. Ubicomp will surround people and be 'always-on', unobtrusive, interconnected intelligent objects. Devices embedded in the environment will communicate seamlessly about any number of different topics e.g. your present state of health. Interactions with devices and at the same time other people will become anywhere, anytime. However, we question whether ubicomp systems will be accessible and usable by all members of society. This two-year research project investigated trust, privacy, identity and inclusion issues for ubiquitous computing systems. We were interested in finding out what advantages and disadvantages ubicomp systems would have for the elderly population.

The world aging population is growing [9]. Aging causes physiological, psychological and social changes in humans. The physical and cognitive deficits of the elderly are well documented [e.g.11]. These deficits include reduced mobility, sensory functioning as well as limitation in memory .and impaired information processing.

Ubiquitous computing will either provide clear advantages or disadvantages this particular age group. Many ubicomp style applications have been employed to investigate assistive living through healthcare and home monitoring systems for the elderly [e.g. 10]. However, the majority of these applications focus on functionality and often ignore the non-functional aspects e.g. human values, inclusion [8].

Living in an information society social inclusion is essential to be able to participate in many everyday activities [3]. Elderly people often have to overcome additional problems before they can use and benefit from a range of technologies and services. Generally technology is considered accessible if the system can be used in an identical or reasonable manner by all. Often elderly people need additional assistive technologies to be able to use systems e.g. screen readers, voice synthesizers. The embedded design of ubicomp creates a problem if a person requires some form of assistive technology to be able to interact and use the system effectively.

The features and complexity of new technologies are forever increasing. For example, mobile telephones now have complex options and features that exclude the elderly. For example, imagine an elderly person with a visual impairment trying to use a touch screen on a mobile telephone. Not being able to use a system transforms a physical disability into a social disability. Goggin & Newell [2] argue accessibility for elderly and disabled people is often ignored in the design of technologies and subsequently creates new barriers.

The exchange of information is crucial if ubicomp systems are to be successful. A key issue 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. However, people already have concerns over personal data storage, exchange, mining and unauthorized access by third parties [4]. Will the elderly be able to manage and control information exchange, trust stakeholders with personal data, set and maintain privacy preferences related to who has access to their personal information?

In short, we are interested in knowing more about user requirements, in particular the elderly, for inclusion, privacy and trust management in a ubiquitous computing world.

PETRA'09, June 09-13, 2009, Corfu, Greece.

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. The results in this paper focus on the health example [see 6 for a review of the other scenarios].

2.1 Development of videotaped scenarios

The elicited scenarios were then used to create a Videotaped Activity Scenario (VASc). The VASc method is an exciting new tool for generating richly detailed and tightly focused group discussion and has been shown to be very effective in the elicitation of social rules [12]. VAScs 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. A professional media company was employed to recruit actors and videotape all scenarios. The production was over seen by both the producer and the research team to ensure that the essence of the scenario was being captured appropriately. British Sign Language (BSL) and subtitles were also added to a master copy of the VAScs for use with participants who had auditory impairments. However due to technical constraints BSL was not added to the finance VASc. All scenarios were approximately three minutes in length. An illustration of 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 was shown to focus groups, the number of participants in each group ranged from 12 to 15 people. The total number of participants was 110 (53 males, 57 females, aged from 65 to 89 years. Participants were drawn from all sectors of society in the Newcastle upon Tyne area of the UK. 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: 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.

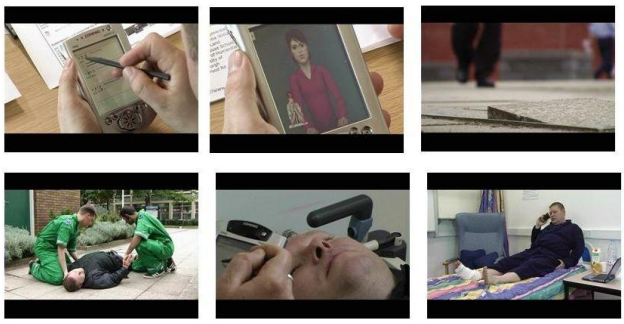

Figure 1: Screen shots taken from a VASc

Technical classification

To classify participants into technical or non-technical six questions based on a categorization process by Maguire [7] were used. Participants answer the questions using ayes/no response. Responding yes to questions 1, 3, 5 and 6, no to questions 2 and 4 would give a high technical score of6. 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?

2.3 Procedure

On recruitment all participants received an information sheet that explained the study and very briefly introduced the concept of

ubicomp in very neutral terms. 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 a short videotaped scenario showing people using an ubicomp system 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. After the initial introduction, the videotaped scenario was shown (the moderator briefly described the concept of ubicomp in a neutral way to avoid influencing participants opinions). Immediately after this each group was asked for their initial thoughts concerning the system and to envisage what they would like or dislike about using a system like that. The same procedure was used for the other three videotaped scenarios [described elsewhere in 6]. 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 a ubicomp society. Participants' attitudes in general towards ubicomp systems were also noted. The duration of the sessions was around ninety-minutes.

3. RESULTS

3.1 Trust

Participants expressed concerns about various risk factors, and whether stakeholders 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, flexibility, personalisation and risk.

Table 1: Trust concepts

Concept	Interpretation	Quote
Stakeholder credibility	Credibility is underpinned by concepts such as loyalty and reputation. For example, medical institutions were seen as credible with good reputations in terms of privacy.	*'I would be quite happy about generalised medical services knowing my medical history but you always have the risk with others basically going through or having access to your health records.'*
Stakeholder motivation	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:	*'I mean you are talking about the information they know which bank you are using, where you go shopping and how regular, having all information together about you people will find out information about you from one source.'*
Monitoring by stakeholders	Monitoring was considered very problematic. For example, if someone was diabetic and shopping for the family would a company decline or stop insurance because certain food was bought that he or she was not suppose to eat? Implications were discussed in terms of social change and everyone having to shop individually	*'If you are buying for a family there is not an obvious way that they can decide which product you are buying for whom, I would have thought, so if you have got an insurance for two people, how are they going to assume correctly which one is eating the wrong things?'*
Flexibility	Participants queried the extent to which systems could be trusted to faithfully reflect unpredictable day-to-day changes in human behaviour. 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.	*'If you go shopping with and have to use a biometric finger scanner for identification and you are called up in an emergency and you want somebody else to do the shopping for you, what are you going to do chop your finger off and say get on with the shopping, I have to go off you know!'*
Personalisation	Participants recognised that a personalised system would be useful and more reflective of their needs. Participants discussed whether services would cover all user requirements.	*'I think certain aspects of that could be very useful, the fact that he was known to have an aspirin allergy, that was flagged up, but the fact that he had an x-ray before he was seen, before he got to the hospital, this is taking it too far.'*
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 think the basic thing with the information is if it is a scheme that is spread with other agencies and healthcare or whatever, financial, we are open to confidentiality, fraud and various other issues, which doesn't make me sit very safely at all, you know basically it needs to be an open system so we can check details.'*
Risk and responsibility	Participants discussed issues of risk and responsibility acknowledging both system and self might be unreliable. Participants discussed liability and litigation - who would be liable if this information was wrong and how would it be changed?	*'So it says, I see that you are allergic to aspirin, but say actually I was allergic to something else. If that was wrong then, although she verified that, you could verify that I suppose, but you would worry that there were going to be pieces of information that might be false, that people are acting upon.'*

3.2 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 in a surveillance society.

Table 2: Privacy concepts

Concept	Interpretation	Quote
Informational (Relates to a person's right to reveal personal information to others, which is not always under a person's control).	The concept of informational privacy was a major concern for all participants. Participants highlighted complex patterns and exchange of personal information would be required to be able to control who receives what and when. 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.	*'So there is certain information that the bank has but the banks know everything financially about you, but maybe some information they don't have that we maybe should retain private.'*
Social (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).	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. 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.	*'I still think the personal touch to our relationships is nice. I think the equipment, the technical knowledge is just there for support and I don't want it to take over the personal, everyday side.'*
Physical (How physically accessible a person is to others and can be linked to such aspects as environmental design).	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. 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. Tracking was discussed both in terms of positive and negative aspects.	*'Maybe it is suitable for vulnerable people, maybe for old people who have got memory problems or something or maybe if they want to go out and they think well if I had this, this granny or whatever, and you take it out with you, they may feel safer going out. It might be quite a good thing to have and you can find out if your husband is having an affair.'*

4. DISCUSSION

Findings revealed having systems that could exchange personal information when appropriate was advantageous for some groups in society. For example, people with medical problems or various disabilities, or those on different types of medication, having their health information disclosed to the relevant people when needed. However, trust and privacy management were found to be core concepts related to the adoption and use of ubicomp systems.

Design and implementation of ubicomp cannot be solely based on accessibility. Several accessibility issues emerged from this discussion related to exclusion, cost, complexity and adaptability. The complexity of such systems was widely discussed across all groups. Participants commented not only on trust and privacy management but also social issues. Stakeholders and designers of ubiquitous systems need to acknowledge the fact humans are inherently social beings and their actions are always directly or indirectly linked to other people. Therefore designers need to consider whether people will rely to heavily on ubiquitous technology, be comfortable exchanging all types of information even when of a very personal nature, how we socially interact change, and social norms along with it.

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 and indeed result in a divided society. 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 [1] 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.

Development in technology has never had the explicit goal of altering civilisation [1] and it is possible that the ubiquitous vision we have portrayed in our scenarios will not ever be fully realised, 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] Bohn, J., Coram, V., Langheinrich, M., Mattern, F., Rohs, MSocial, Economic, and Ethical Implications of Ubiquitous computing and Ubiquitous Computing. *Ubiquitous computing*, Springer-Verlag, 5-29 . (2005)..

[2] Goggin, G., & Newell, C. An end to disabling policies? Toward enlightened universal service. *Information Society, 16*, 127-133. (2000)

[3] Jaeger, P.T. Telecommunications policy and individuals with disabilities: issues of accessibility and social inclusion in the policy and research agenda. *Telecommunications Policy, 30*, 112-124 (2006).

[4] Little, L., Briggs, P., & Coventry, L. Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. *British HCI Conference, Leeds*. (2004).

[5] Little, L. and Briggs, P. Privacy factors for successful ubiquitous computing. In press: *International Journal of E-Business Research* (2009). .

[6] Little, L., Marsh, S., & Briggs, P. Trust and privacy permissions for an ambient world. In R. Song, L. Korba, G. Yee (Eds.) Trust in e-services: technologies, practices and challenges. New York: Ideas Group (2007).

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

[8] Poole, E.S., Dantec, C.A., Eagan, J.R., & Edwards, W.K. Reflecting on the invisible: understanding end-user perceptions of ubiquitous computing. ACM International Conference Proceeding Series; Vol. 344 Proceedings of the 10th international conference on Ubiquitous computing. 192-201. 2008

[9] UK National Statistics *Population Estimates UK population grows to 60.6 million*. Downloaded December 2007 http://www.statistics.gov.uk/CCI/nugget.asp?ID=6 (2007).

[10] Varshney, U. Pervasive healthcare and wireless health monitoring, Mobile Networks and Applications, v.12 n.2-3, p.113-127, March 2007

[11] Webb, J.D. & Weber, M.J. Influences of Sensory Abilities on the Interpersonal Distance of the Elderly. *Environment & Behavior. 35*, 695-711(2003).