

E-voting in an AmI world: Trust, privacy and social implications

Linda Little¹, Tim Storer², Pam Briggs¹& Ishbel Duncan²

¹PACT Lab, Northumbria University, UK

²School of Computer Science, University of St. Andrews, UK

l.little@unn.ac.uk

Ambient Intelligence (AmI) evokes a near future in which humans will be surrounded by ‘always-on’, unobtrusive, interconnected intelligent objects. 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. This seamless exchange of information has vast social implications, in particular the protection and management of personal information. As a result, we have recently conducted a wide reaching study of people’s attitudes to potential AmI scenarios. This research project investigates the concepts of trust and privacy issues specifically related to the exchange of health, financial, shopping and e-voting information when using AmI system. The findings related to the e-voting scenario will be discussed in this paper.

1 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 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.

Although this form of intelligent communication is still a vision of the future, we already use a host of different technologies to send and receive information and communicate with others. When using existing technologies to exchange information generally we initiate and control the process, know who will receive the information and are aware of the actual message content. 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.

As humans are inherently social beings, and our actions are always directly or indirectly linked to other people, how will AmI systems impact upon our social world? Friedewald et al (2005) question whether AmI systems will fulfil most of the promises made by researchers or whether the vision is just an illusion? Living in an AmI society suggests effortless communication, our needs, wants and desires met. The seamless exchange of information has vast social implications and might not decrease but actually increase the complexity of life.

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 paper will focus on the social implications of information exchange in an ambient society, in particular the use of an e-voting system, 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?

.

1.1 The Context of E-Voting

People regularly take part in electronic voting using devices such as mobile telephones and Internet linked personal computers. The type of vote cast is often novel and trivial e.g. choosing a contender in a reality television show. When considering use of such systems to vote in political elections the concepts of privacy, trust and security need fully understood.

Recently, a number of government's have begun experimenting with the use of new electronic voting (e-voting) systems for the purpose of public elections. In 2002, the United States Congress passed the Help America Vote Act (Federal Election Committee 2002) which mandated the use of Direct Recording Electronic (DRE) voting machines in all polling stations to support disabled voters who wished to vote without assistance or by proxy. A further intention of the move towards DRE machines in the US is to improve the accuracy and integrity of vote casting in a relatively complex electoral system, given the experience of failures during the 2000 presidential election attributed to other voting systems (Kimball, Owens & Keeney 2002). However, the use of DRE machines has proved controversial, with many academic, journalists and voting rights advocates arguing that the use of electronic voting systems simply hides the evidence of system failures, rather than eliminating the problem itself (Gumbel 2005, Dill 2003, Mercuri 2001). Many of such critics advocate the introduction of Voter Verified Paper Audit Trails (VVPAT), in essence paper receipts printed by the DRE checked by the voter against the electronic representation and used as the final

arbiter in a disputed count. Others have argued that VVPATs introduce as many problems as they are purported to solve, and in particular their crude may violate the privacy of disabled voters, if they require assistance in order to verify their vote.

In the United Kingdom (UK), the government recently conducted a range of pilots of new voting systems, including a number of pilots of remote electronic voting (REV) systems (The Electoral Commission 2002, 2003). The introduction of remote electronic voting systems occurred in the context of a rapidly declining turnout to elections at European, national and local levels. In 2001, turnout to the General Election dropped to 59.4%, the lowest since the advent of universal suffrage (Electoral Commission 2001). In this context, the major aim of the use of these new technologies is to improve the convenience of voting and (it is hoped) voter participation and turnout to elections. The piloting of remote electronic systems was commonly conducted using a security mechanism proposed by CESG as a simple means of vote casting and reassuring voters that their vote had been collected by an Election Authority (CESG 2002). However, several commentators and studies identified weaknesses in the security mechanism (Mercuri 2002, Kitcat 2002). The pilots of REV systems were generally considered to be of mixed success with respect to their primary goal of improving turnout, compared with other more established systems such as postal voting. From a technological perspective, the pilots were considered relatively successful, with few problems reported using the systems, or counting votes.

In the academic community, electronic voting (both remote and polling station based) have traditionally been considered as within the remit of cryptography, and in particular an example application of a secure multi-party computation. A variety of cryptographic constructs have been proposed to support REV systems, including mixnets (Chaum 1981) homomorphic schemes (Benaloh 1996) and schemes employing blind signature techniques (Fujioka et al 1992). More recently, the use of cryptography has been proposed to support polling station DRE systems, including the use of visual cryptography (or similar) to provide voters with non-transferable receipts for their votes (Chaum 2004, Chaum et al 2004). In addition, the notion of *pollsterless* remote voting systems has been introduced, which attempt to remove the requirement for voters to use trusted software artefacts in order to engage in a cryptographic protocol (Malkhi et al 2003). The scenario described in this paper is based on one such pollsterless system, mCESG (Storer & Duncan 2004). The current controversy regarding DRE machines has also spurred academic interest in voting systems from other fields out with cryptography, including dependability (Bryans & Ryan 2003) and usability (Laskowski & Quenesbery 2004, Bederson et al 2003, Mercuri 2002) There is now an accepted view that research into voting systems has become a multi-disciplinary activity, requiring expertise from a multitude of fields.

2 Method

To understand and investigate the concept of AmI technology and subsequent use key stakeholders provided specific scenarios illustrating the ways in which privacy, trust and

identity information might be exchanged in the future. The stakeholders included relevant user groups, researchers, developers, businesses and government departments with an interest in AmI development. Four scenarios were developed, related to health, e-voting, shopping and finance that included facts about the device, context of use, type of service or information the system would be used for. These scenarios are briefly described below:

*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.

2.1 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., 2004). 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.

2.2 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.

2.3 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 were 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?

2.4 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 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. 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, 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 disclosure, privacy, trust and usability issues associated with the use of e-voting systems. These constructs were compared in relation to the user, device and stakeholder.

Trust concepts

a) Credibility of the stakeholder

Participants raised concerns over political parties and government using AmI systems to monitor voting habits. Participants feared stakeholders would alter, change or add votes. Concerns were raised over government having the capacity to create user profiles. This in turn would create lifestyle profiles accessible by third parties which would lead to untold consequences.

'I think I would trust the system providing it was entrusted to the same electoral registration officers

as it is at the moment.'

b) Motivation

Participants discussed e-voting systems in terms of motivation related to their own use and the stakeholder. Advantages for personal use related to convenience, the mobility of the system and the concept of voting verification. Older age groups debated whether e-voting systems would encourage younger age groups to vote in elections. Concern was raised that e-voting systems would make voting appear a casual event. Stakeholder motivation was discussed in terms of monitoring votes and voters. Monitoring actual voters was considered a major disadvantage. Also concern was raised over stakeholders using such systems to alter and change votes.

'I would say the young ones, because the technology is acceptable to them. It makes it more relevant to today's youth and more interactive I guess.'

'I'm not saying it does happen but with a candidate, if he wants to make sure that is who is elected, he could hack in to the voting to play around with the figures.'

c) Personalisation

The ability of people to use a personal device for voting and use personalised security mechanisms e.g. passwords. Also the system and stakeholder's sensitivity regarding sending and receiving personalised information in a timely manner.

Discussion revealed participants concerns over systems being truly sensitive to circumstances under which personal information could legitimately be exchanged. The transfer of sensitive personal information and anonymity were discussed. Leakage of sensitive information in inappropriate circumstances was seen as very problematic:

'You punch your number in and press Enter. They don't know your number. That's the idea of personalising it, do you know what I mean. But what I am saying is where does it go from that machine, does anybody else contribute, you know access to a big computer with all these numbers in, transactions where do they go?'

'It does not do anything different; but it would be yours. So if you are putting the information in it's not going to tell anyone. If everybody has got one you want to be a little bit different.'

d) Falibility

Discussion highlighted human fallibility in using an e-voting system, entering numbers and 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). Participants were also concerned about making mistakes and voting for the wrong person.

'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.'

e) Reliability

Participants discussed the reliability of the system. For example, if the machine malfunctioned and the user was unaware of this what would the consequences be? Participants questioned whether e-voting systems complicated the voting process and increased the cognitive load on the voter compared to existing systems.

'I think that with something important like the vote, the amount of times that new technology goes wrong you are sort of taking a big gamble voting that way. At least if the cross is on a bit of paper and it is counted by another human being, you feel safe that your vote is actually registered in the right place.'

f) Reliance and responsibility

Participants discussed the user relying too much on the system 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, how would the user be assured that his or her vote was actually secure and free from interference from others. Participants were also concerned some people would adopt e-voting systems and not consider

the responsibility of what it means to cast a vote and who to actually vote for. This in turn would reduce the overall level of trust in political groups.

'I think over dependence on say electronic voting would be very dangerous.'

'The people that are providing the service they have got to get it right; the level of information they are passing to one another. Will that information be protected; how will I know when I pick a device up I can trust that device to only do what I said to do; will it be interfered with.'

'They would have to extend the data protection act wouldn't they so that there was some sort of control as to where that information went. At the moment I don't think there are, the information can just go anywhere.'

g) Security

Security of e-voting systems emerged as key factor that would limit adoption and use. Fraudulent use, hacking, access by third parties, leakage and storage of information were all areas discussed. Participants agreed that being able to verify their vote was a positive aspect of the system. However participants did question whether the actual verification process could be trusted compared to actually physically voting at a polling station.

'I think the problem with all new technologies like this is someone comes up with a brilliant idea to increase the number of people voting, whatever the motive is, to make it easier to vote on the web. I think where the problem arises is that the safeguards are not always in place or not enough thought has been given to the security of that information, when this technology is developed initially.'

'I have serious worries about the security of this, because when we go into a booth, they've got your name, you get a bit of paper, there's no marking on the paper, you put a cross and you vote in secret, but with this, you can trace it and I don't like it.'

Privacy concepts

h) Physical privacy

Participants commented when using e-voting systems physical privacy was a major issue. They discussed issues related to leakage of personal information in public settings and other people being able to see what they were doing. Participants were also concerned that using such systems would lead to surveillance.

'It's great that you can sit on the Metro and do it, assuming that nobody is looking over your shoulders while you are physically pulling your number. You couldn't do it standing up on the London Tube for example.'

i) Informational privacy

The concept of informational privacy was a major concern for all participants..Participants acknowledged stakeholders 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 employment as his or her profile states which particular political party he or she voted for.

'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.'

'Even if you can justify your answer, they can always find flaws in that, so you really don't want to tell anybody who you voted for. There could be other personal information where you are voting that could leak out.'

'I think the only danger with that is if you vote for one of the parties and the other party get in and they know that you didn't vote for them, it could cause all kinds of difficulties do you not think?'

j) Social privacy

Participants discussed the possibility that e-voting systems 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. The act of actually going to a polling station was considered a social event, one in which interaction with others took place. Participants also 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 e.g. your voting preference. 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.

'I don't know whether this is because we are primarily discussing technology, I don't know how far this is relevant. I would not want to see that kind of thing happening in elections for quite different reasons. I think there are areas of life in which technology is inappropriate and politics is an area in which there is already too little involvement and too little contact of the individual and the act of getting out and voting is as an important thing for an individual citizen to do and I think it would be wrong, not wrong, it would be unfortunate that if it is replaced by a little electronic thing that you can do in the privacy of your own home it privatises something that should be public and shared.'

Disclosure

k) Risk and disclosure preferences

Participants discussed the levels of risk involved when personal information is disclosed. 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, creating profiles, making inferences from personal information and suggested AmI systems(including e-voting) need 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.'

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.

'It is not confidential, because if you cannot see the postal vote form, by law the form has got to be of a certain size. It can't really be enlarged or made bigger. Some people will actually have to ask somebody to do it for them. So again it is not confidential'

1) Autonomy (choice and control)

Participants commented little or even no choice would exist in an AmI society. Comments suggested 'forced choice' would become the 'norm', making people vote electronically even

if they did not want to. Participants expressed concern over the right not to reveal information having vast implications leading to exclusion in some circumstances.

Participants were concerned about reliance on AmI systems such as e-voting 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. storage and transmission.

'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.'

Usability concepts

m)Complexity

Participants discussed concern over the complexity of e-voting systems. Comments related to the fact existing technologies are difficult to use. Participants commented the e-voting system had several tasks which were time consuming and complicated compared to casting a vote at a polling station. Discussion also focused on age differences in technology use, experience and familiarity.

'I would have thought that there were a number of people, dare I say, probably myself included, who

would find that type of technology rather difficult. I find it difficult enough to make a mobile phone call.'

'I'm not sure whether I would necessarily use it but it is just getting used to new systems isn't it, you think you are not going to use the things and when they are available you think yes, what a good idea. I would worry about having to learn another number and I'm a Maths teacher! But it drives me mad all these security codes and you have got to know so many different ones.'

n)Exclusion & accessibility

Participants commented widespread exclusion would occur if people had to adopt e-voting systems. Exclusion would occur due to age, ability, disability and socio-economic status. The hearing and visually impaired group in this study found the system very complex and commented that it would acutally deter voting. Visually impaied participants discussed exclusion due to text messaging and the reduction in physical privacy if audio equipment had to be used.

'Because not everybody has the access to a computer do they. You see all these old people round my place the council estate, in the bungalows, they haven't got computers. They wouldn't know what to do with them if they did, so.'

o)System – type

All participants agreed the mobility of voting electronically was advantageous and that

through diffusion adoption would probably occur. Participants commented systems needed to be transparent and accessible so information could be verified and changed. Decentralised systems were considered more secure than centralised. For example, the amount of votes could be accounted for in a decentralised system.

'The danger in setting up a system like this is that there could be some element of central control in this system that is not there either by the present postal voting or by the present going to the polling station.'

'If they are still keeping their electoral areas, so this information goes to a returning officer, so we are not talking about a totally centralized system where all the information goes to London and all the results are announced in London. You don't have anything like Newcastle's group of MPs, North Tyneside whatever they are will be announced by the returning officers in the respective areas, so if the information is being collated that way, I don't have any problem because you know how many voters there are from the electoral role, you know how many votes have been cast. Half the time you find out if there is a glitch in the system because too many people are voting from the population of the area or whatever, so there are certain safeguards in that respect.'

4 Discussion

To evaluate the social impact of AmI use, trust, privacy and usability need to be understood. Findings from this study show use of an e-voting system is affected by trust, privacy,

disclosure and usability issues. Also different contexts, stakeholders, device type and the actual user all need to be considered. This is important if we are to fully understand user interaction with e-voting systems and in particular AmI technologies.

Findings from this research support the view 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 in an e-voting context: 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?

Interestingly, although participants were grouped by technical stance, age, gender and educational achievement the recurrence of themes across groups were similar. This suggests e-voting systems raise similar issues for all relevant users. The majority of participants agreed the mobility and convenience were positive aspects of e-voting. However, concern over excluded groups with regard to using e-voting systems was frequently discussed. For example, discussion highlighted how disabled groups have little or no privacy when using technologies as they often have to ask for help from others. In the case of e-voting a visually impaired person would have to reveal his or her vote to someone else, this trusted other would

then vote on his or her behalf.

Participants were also concerned about the 'behind the scenes' processing of personal information, the complexity and security of the system. The concerns raised by participants related to trust in the system and the actual stakeholder e.g. altering votes, third party access and exploitation. These findings have major implications for AmI systems. Therefore, to increase trust AmI systems need to be transparent and decentralised. These findings support the Fair Information Practice-FIP (e.g. Federal Trade Commission of America, 2000) that suggests stakeholders should give users: notice, choice, access and security.

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 and privacy questions whether we can really understand this type of puzzle or even create a clear vision for future interactions with AmI systems. Findings support the view of Friedewald et al (2005) and question whether AmI systems will actually increase the complexity of life.

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?

AmI systems do bring substantial benefits, including convenience and mobility. 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 and in particular e-voting, appear key concepts that emerged from the group discussions in this study, and bear much further examination and understanding.

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. 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 seamlessly 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 of this research is to develop a survey 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.

5 References

Bederson, B.B, Bongshin L., Sherman, R.M., Herrnson, P.S., & Niemi, R.G. (2003).

Electronic voting system usability issues. *Proceedings of CHI 2003*, 145–152.

Benaloh, J. (1996). *Verifiable Secret Ballot Elections*. PhD thesis, Yale University.

Bryans, J. & Ryan, P. (2003). A dependability analysis of the Chaum digital voting scheme.

Technical Report CS-TR-809, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK.

Communications and Electronic Security Group (CESG). (2002). E-voting security study.

Downloaded August 2006

http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/uk/uk54.pdf

- Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88.
- Chaum, D. (2004). Secret-ballot receipts: True voter verifiable elections. *IEEE Security and Privacy*, 2(1):38–47.
- Chaum, D., Ryan, P. & Schneider, S.A. (2004). A practical, voter-verifiable election scheme. Technical Report CS-TR-880, School of Computing Science, University of Newcastle upon Tyne, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, UK.
- Dill, D. (2003). Resolution on electronic voting.
- Electoral Commission (2001). *Election 2001: The official results*. The Electoral Commission, Trevelyan House, Great Peter Street, London, SWP 2HW.
- Electoral Commission. (2002). Modernising elections, a strategic evaluation of the 2002 electoral pilot schemes. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P Downloaded August 2006
<http://www.electoralcommission.org.uk/elections/modernisingelections.cfm>
- Electoral Commission. (2003). The shape of elections to come: A strategic evaluation of the 2003 electoral pilot schemes. The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P 2HW. Downloaded August 2006
<http://www.electoralcommission.org.uk/about-us/03pilotscheme.cfm>
- Federal Election Committee. (2002). Help America Vote Act, (P.L. 107-252). Downloaded

August 2006 <http://www.fec.gov/hava/hava.htm>

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

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

Fujioka, A., Okamoto, T., & Ohta, K (1992) A practical secret voting scheme for large scale elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - ASIACRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques*, volume 718 of *Lecture Notes in Computer Science*, pages 244–251.

Gumbel, A. (2005). *Steal this vote*. New York: Nation Books

Kimball, D.C., Owens, C & Keeney, K. (2002). Unrecorded votes in the 2000 presidential election. Similar to a paper later published at APSA99,

Kitcat, J (2002) E-voting security study response: FREE e-democracy project. Downloaded August 2006 http://www.j-dom.org/files/evote_sec_response.pdf

Laskowski, S., & Quesenbery, W. (2004). Putting people first: The importance of user-centered design and universal usability to voting systems. NAS Framework for Understanding Electronic Voting, white paper, November.

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

September 2004

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

Malkhi, D., Margo, O., & Pavlov, E. (2003). E-voting without 'cryptography'. In Matt Blaze, editor, *Financial Cryptography, 6th International Conference, FC 2002, Revised Papers*, volume 2357 of *Lecture Notes in Computer Science*, 1-15.

Mercuri, R. (2001). *Electronic Vote Tabulation: Checks and Balances*. PhD thesis, University of Pennsylvania.

Mercuri, R. (2002). Humanizing voting interfaces. In *Usability Professionals Association Conference*, Orlando, Florida, USA.

Mercuri, R. (2002). Response to formal request for comment by the CESG (UK) on internet voting

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

Storer, T., & Duncan, I. (2004). Polsterless remote electronic voting. *Journal of E-Government*, 1(1):75-103.

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

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

September.