E-Voting in an Ubicomp World
Trust, Privacy, and Social Implications

Linda Little, Tim Storer Pam Briggs Ishbel Duncan

The advances made in technology have unchained the user from the desktop into interactions where access is anywhere, anytime. In addition, the introduction of ubiquitous computing (ubicomp) will see further changes in how we interact with technology and also socially. Ubicomp evokes a near future in which humans will be surrounded by "always-on," unobtrusive, interconnected intelligent objects where information is exchanged seamlessly. This seamless exchange of information has vast social implications, in particular the protection and management of personal information. This research project investigates the concepts of trust and privacy issues specifically related to the exchange of e-voting information when using a ubicomp type system.

Keywords: *ubiquitous computing; e-voting; privacy; trust; usability*

Ubiquitous Computing (Ubicomp)

Ubicomp refers to the convergence of ubiquitous communication and interfaces that are both socially aware and capable of adapting to the needs and preferences of the user. Ubicomp 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 artifact imaginable. A person might interact with hundreds of computers at any one 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 ubicomp 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 ubicomp systems affect our social world? Friedewald, Costa, Punie, Alahuhta, and Heinonen (2005) question whether ubicomp systems will fulfil most of the promises made by researchers or whether the vision is just an illusion. Living in a ubicomp 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 ubiquitous technology adoption and use are trust and privacy issues. Currently, many users are unaware that their privacy is at risk when using the Internet and that their online tour can be tracked. Users are often unaware that after visiting some sites, Cookies can get implanted onto their hard drives and they then become a target for unsolicited mail. Users leave data trails almost every day (e.g., credit card use). An individual's data can be collected from the trail he or she leaves behind, and few legal restrictions exist on how the data can be used (McCandlish, 2002). Although several programs exist to stop personal details being sent, individuals may not know how to install or use them (e.g., Platform for Privacy Preferences). In a ubicomp society, will setting preferences for information exchange be too complex?

A few architectures and models have been proposed for understanding privacy issues with regard to ubicomp systems (e.g., Privacy Risk Model—Hong, Ng, Lederer, & Landay, 2004; Five Pitfalls for Designers—Lederer, Hong, Dey, & Landay, 2004). Other researchers have discussed the need to understand privacy and consider issues in ubicomp systems related to feedback and control (Bellotti & Sellen, 1993), Fair Information Practice (FIP; Langheinrich, 2001), and negotiation of boundaries (Palen & Dourish, 2003).

When interacting with technology, privacy protection and disclosure of information is a two-way process. From the technological viewpoint (e.g., use of the Internet), the FIP (Federal Trade Commission Study, 2000) suggests that companies should give users notice, choice, access, and security. Notice refers to the right of the individual to know what information n 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 honor and ensure data integrity and that data are secure from unauthorized access during both transmission and storage. Practices such as FIP are needed to mediate privacy, empower the individual, increase the user's control, and create assurance. These policies also reduce data gathering, data exchanging, and data mining and therefore are important in a ubiquitous 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 (Teltzrow & Kobsa, 2003).

Computing devices are already embedded and used in a variety of environments, and the persuasiveness of these systems often goes unnoticed. Raisinghani et al. (2004) state ubicomp currently affects our lives and we don't even notice (e.g., users are mobile, communication is made easier between individuals, between individuals and things, and between things). Electronic voting (e-voting) might not be considered truly ubiquitous, but these type of systems allow mobility and personal information to be exchanged anywhere, anytime.

This article will focus on the social implications of information exchange in a ubiquitous 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 ubicomp tick, we need to ask questions about information that will have a direct impact on both trust and privacy, including the following: 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 with whom to communicate (e.g., through personalized agents)?

The Context of E-Voting

People regularly take part in e-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 to be fully understood.

Recently, a number of governments have begun experimenting with the use of new 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 toward DRE machines in the United States 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 e-voting systems simply hides the evidence of system failures rather than eliminating the problem itself (Dill, 2003; Gumbel, 2005; 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 may violate the privacy of disabled voters, if they require assistance to verify their vote.

In the United Kingdom, the government recently conducted a range of pilots of new voting systems, including a number of pilots of remote e-voting (REV) systems (Electoral Commission, 2002, 2003).

The introduction of REV 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 Communications and Electronic Security Group (CESG, 2002) as a simple means of vote casting and reassuring voters that their vote had been collected by an election authority. However, several commentators and studies identified weaknesses in the security mechanism (Kitcat, 2002; Mercuri, 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 computer science community, e-voting (both remote and polling station based) has traditionally been considered as within the remit of cryptography and in particular an example application of a secure multiparty 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, Okamoto, & Ohta, 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 nontransferable receipts for their votes (Chaum, 2004; Chaum, Ryan, & Schneider, 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 artifacts to engage in a cryptographic protocol (Malkhi, Margo, & Pavlov, 2003).

The scenario described in this article 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 (Bederson, Bongshin, Sherman, Herrnson, & Niemi, 2003; Laskowski & Quesenbery, 2004; Mercuri, 2002).There is now an accepted view that research into voting systems has become a multidisciplinary activity, requiring expertise from a multitude of fields.

Method

To understand and investigate the concept of ubicomp 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 ubicomp development. Four scenarios were developed, related to health, e-voting, shopping, and finance, that included facts about the device, context of use, and type of service and information for which the system would be used. In this article, the results and focus are based on the e-voting scenario briefly described below:

E-voting Scenario: Natasha decides she wants to vote in the next election using the new online system. She goes online and requests e-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 number that 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 onto 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 for whom she has voted. 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.

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 focused group discussion and has been shown to be very effective in the elicitation of social rules (Little, Briggs, & Coventry, 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 and express their beliefs and expectations. This generates descriptions that are rich in detail and focused on the topic of interest. For this research, a media production company based in the United Kingdom 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 for use in groups where participants had various visual or auditory impairments.

Participants

The VASc were shown to 38 focus groups, and the number of participants in each group ranged from 4 to 12. The total number of participants was 304. Participants were drawn from all sectors of society in the Newcastle upon Tyne area of the United Kingdom, including representative groups from the elderly, the disabled, and 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 nontechnical. This was used to investigate any differences that might occur because of existing knowledge of technological systems. Therefore, participants were allocated to groups initially by technical classification (i.e., technical/nontechnical), followed by gender, then level of educational achievement (high = university education or above vs. low = college education or less), and finally age (young = younger than 25 years old, middle = 26 to 65 years old, old = older than 65). Overall, this categorization process culminated in 24 main groups. Because of 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, a group session for people with visual and auditory impairments was carried out at the Disability Forum in Newcastle. The forum was considered to have easier access and dedicated facilities for people with such disabilities.

Technical Classification

To classify participants into technical or nontechnical groups, six questions based on a categorization process by Maguire (1998) were used. Participants answered the questions using a “yes/no” response. Responding “yes” to Questions 1, 3, 5, and 6 and “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 to 3 where classified as nontechnical, whereas participants who scored 4 or 5 were classified as technical. The questions were as follows:

If your personal devices (e.g., mobile telephone or computer) were taken away from you tomorrow, would it bother you?
Do you think that we rely too much on technology?
Do you enjoy exploring the possibilities of new technology?
Do you think technologies create more problems than they solve?
Is Internet access important to you?
Do you like to use innovative technology as opposed to tried and tested technology?

Procedure

On recruitment, all participants received an information sheet that explained the study and the concept of ubicomp technologies. Participants were invited to attend Northumbria University, in the United

Kingdom, to take part in a group session. The groups ran at various times and days during a 3-month period. Participants were told they would be asked to watch four short videotaped scenarios showing people using ubicomp 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 that the discussion groups would be recorded for further analysis. Participants were not informed about the technical/nontechnical 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 ubicomp technologies. After the initial introduction, the first videotaped scenario was shown. Immediately after this, each group was asked if it thought there were any issues or problems it could envisage if it 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 a ubiquitous society. Participants' attitudes in general toward ubicomp systems were also noted. The duration of the sessions was approximately 90 min.

Analysis and Results

All group discussions were transcribed and then read; a sentence-by-sentence analysis was employed using the Atlas.ti qualitative software program. The data were open coded using qualitative techniques, and several categories were identified. The data were 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 a ubiquitous 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

Participants expressed concerns about whether the stakeholders or their agents could be trusted to control and contain the exchange of voting information. The ability of individuals to interrogate the system or influence the release of personal data was a key issue. In the thematic analysis, trust was positively associated with the key constructs of credibility, motivation, personalization, fallibility, reliability, reliance, responsibility, and security.

Stakeholder credibility. Stakeholder credibility is underpinned by concepts such as loyalty and expectation.

"I think I would trust the system providing it was entrusted to the same electoral registration officers as it is at the moment." (technical, high education, female, middle age group)

Participants raised concerns over political parties and government using ubicomp systems to monitor voting habits. Participants feared stakeholders would alter, change, or add votes. Concerns were raised over the 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.

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:

"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." (nontechnical, low education, male, young age group)

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'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." (technical, high education, male, young age group)

Personalization. Personalization is the ability of people to use a personal device for voting and use personalized security mechanisms (e.g., passwords):

"You punch your number in and press Enter. They don't know your number. That's the idea of personalizing it, do you know what I mean." (nontechnical, visually impaired, female, middle age group)

Also, personalization includes the system and stakeholder's sensitivity regarding sending and receiving personalized 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:

"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?" (nontechnical, low education, female, middle age group)

Fallibility. Discussion highlighted human fallibility in using an e-voting system, entering numbers, and losing the device (although acknowledging the fact that a truly ubicomp 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 recognize." (technical, high education, male, old age group)

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. (nontechnical, high education, male, middle age group)

Reliance and responsibility. Participants discussed the user relying too much on the system to exchange information and the responsibility associated with this:

"I think overdependence on say e-voting would be very dangerous." (technical, high education, male, old age group)

Participants discussed that relying on either the system 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?

"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?" (nontechnical, low education, female, young age group)

Participants were also concerned some people would adopt e-voting systems and not consider the responsibly of what it means to cast a vote and for whom to actually vote. This in turn would reduce the overall level of trust in political groups:

"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." (technical, high education, female, old age group)

Security. Security of e-voting systems emerged as a key factor that would limit adoption and use. Fraudulent use, hacking, access by third parties, leakage, and storage of information were all areas discussed:

"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." (technical, high education, male, middle age group)

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 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." (nontechnical, high education, male, middle age group)

Privacy Concepts

Participants recognized physical, informational, and social privacy but were also keen to discuss issues of privacy management. This went beyond the issue of how much information related to voting and political preferences to disclose and encompassed discussion of whether individuals would be able to live their lives outside of the ubiquitous lens.

Physical privacy. Participants commented that 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." (technical, high education, female, old age group)

Informational privacy. The concept of informational privacy was a major concern for all participants. Participants acknowledged that 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:

"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." (nontechnical, high education, male, middle age group)

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 consequences. 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 [third parties] can get details from there and there's companies buying and selling that information." (technical, high education, female, middle age group)

"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?" (technical, high education, male, middle age group)

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 that 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" when 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 privatizes something that should be public and shared." (nontechnical, low education, male, old age group)

Disclosure

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

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, and making inferences from personal information and suggested ubicomp 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." (technical, low education, male, young)

It is interesting that 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." (technical, hearing impaired, male, old age group)

Autonomy (Choice and Control)

Participants commented that little or even no choice would exist in a ubicomp society. Comments suggested that "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 ubicomp systems, such as e-voting reducing personal control. Discussions revealed ubicomp 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." (technical, high education, female, middle age group)

Usability Concepts and Social Concerns

Participants commented that exclusion would be a major problem with adoption and use of e-voting systems. People would be excluded by age, ability, and disability. Also discussed were moral issues related to e-voting systems. Participants suggested that technologies are now taking away human responsibility. Ubicomp systems will further decrease social interaction, reduce our social skills, and take away the concept of trust.

Complexity. Participants discussed concern over the complexity of e-voting systems. Comments related to the fact that existing technologies are difficult to use:

"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." (nontechnical, low education, male, old age group)

Participants commented that the e-voting system had several tasks that 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'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 math teacher! But it drives me mad all these security codes, and you have got to know so many different ones." (technical, high education, female, middle age group)

Exclusion and accessibility. Participants commented that widespread exclusion would occur if people had to adopt e-voting systems. Exclusion would occur because of age, ability, disability, and socioeconomic status. The hearing and visually impaired group in this study found the system very complex and commented that it would actually deter voting. Visually impaired participants discussed exclusion because of 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." (nontechnical, low education, male, middle age group)

System type. All participants agreed that the mobility of voting electronically was advantageous and that through diffusion, adoption would probably occur. Participants commented that systems needed to be transparent and accessible so information could be verified and changed. Decentralized systems

were considered more secure than centralized systems. For example, the amount of votes could be accounted for in a decentralized 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." (technical, high education, male, middle age group)

"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." (technical, high education, male, middle age group)

Discussion

To evaluate the social impact of ubicomp use, trust, privacy, and usability need to be understood. Findings from this study show that 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 ubicomp technologies.

Findings from this research support the view that privacy and trust are multidimensional constructs with underlying factors that dynamically change according to context. The findings support the view of Sillence, Briggs, Fishwick, and Harris (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? These findings support the work of Hong et al. (2004). Hong et al. suggest that designers of ubicomp systems need to deploy a privacy risk analysis considering social and organizational content. This type of analysis considers the following questions: Who are the users? What kind of personal information is being shared? How is personal information collected?

It is interesting that although participants were grouped by technical stance, age, gender, and educational achievement, the recurrence of themes across groups was similar. This suggests that 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, and this trusted other would then vote on his or her behalf.

Participants were also concerned about the "behind the scenes" processing of personal information and 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 ubicomp systems. Therefore, to increase trust, ubicomp systems need to be transparent and decentralized. These findings support the FIP (e.g., Federal Trade Commission Study, 2000), which suggests stakeholders should give users notice, choice, access, and security.

For ubicomp systems to work, societies need to be at least somewhat transparent. To be truly transparent then, we need complete trust and to 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 ubicomp systems. Findings support the view of Friedewald et al. (2005) and question whether ubicomp systems will actually increase the complexity of life.

We need to consider the fact that 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 too heavily on ubicomp 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?

Ubicomp 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 ubicomp systems and in particular e-voting appear to be key concepts that emerged from the group discussions in this study and bear much further examination and understanding.

Ubiquitous computing is now an area intensely researched and 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. If Weiser's vision is to be realized, 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 a ubiquitous 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.

References

Bederson, B. B., Bongshin, L., Sherman, R. M., Herrnson, P. S., & Niemi, R. G. (2003). Electronic voting system usability issues. *Proceedings of CHI Letters, 5*(1), 145-152. Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. In *Computer- Human Interaction (CHI) Conference, 2003* (pp. 145-152). New York: ACM Publications.

Benaloh, J. (1996). *Verifiable secret ballot elections*. Unpublished PhD thesis, Yale University, New Haven, Connecticut.

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). Newcastle upon Tyne, UK: University of Newcastle upon Tyne.

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-80, School of Computing Science, University of Newcastle upon Tyne). Newcastle upon Tyne, UK: University of Newcastle upon Tyne.

Communications and Electronic Security Group. (2002). *E-voting security study*. Retrieved August 1, 2006, from http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/uk/uk54.pdf

Dill, D. (2003). *Resolution on electronic voting*. Retrieved August 1, 2006, from http://verify.stanford.edu/evote.html

Electoral Commission. (2001). *Election 2001: The official results*. London: Author.

Electoral Commission. (2002). *Modernising elections, a strategic evaluation of the 2002 electoral pilot schemes*. London: Author. Retrieved August 1, 2006, from 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*. London: Author. Retrieved August 1, 2006, from http://www.electoralcommission.org.uk/about-us/03pilotscheme.cfm

Federal Election Committee. (2002). *Help America Vote Act* (P.L. 107-252). Retrieved August 1, 2006, from http://www.fec.gov/hava/hava.htm

Federal Trade Commission Study. (2000, May). *Privacy online: Fair Information Practices in the electronic marketplace* (a report to Congress). Washington, DC: Author.

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

Fujioka, A., Okamoto, T., & Ohta, K. (1992). A practical secret voting scheme for large scale elections. In J. Seberry & Y. Zheng (Eds.), *Advances in cryptology–ASIACRYPT '92, workshop on the theory and application of cryptographic techniques* (Vol. 718 of *Lecture Notes in Computer Science*, pp. 244-251). Gold Coast, Queensland, Australia: Springer-Verlag.
Gumbel, A. (2005). *Steal this vote*. New York: Nation Books.
Hong, J. I., Ng, J. D., Lederer, S., & Landay, J. (2004). *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, Massachusetts.
Kimball, D. C., Owens, C., & Keeney, K. (2002). *Unrecorded votes in the 2000 presidential election*. Unpublished manuscript.
Kitcat, J. (2002). *E-voting security study response: FREE e-democracy project*. Retrieved August 1, 2006, from http://www.j-dom.org/files/evote_sec_response.pdf
Langheinrich, M. (2001). Privacy by design—Principles of privacy-aware ubiquitous systems. In *Proceedings of the 3rd international conference on ubiquitous computing* (pp. 273-291). London: Springer-Verlag.
Laskowski, S., & Quesenbery, W. (2004, November). *Putting people first: The importance of user-centered design and universal usability to voting systems* (NAS Framework for Understanding Electronic Voting, white paper). Washington, DC: National Research Council, Committee on Electronic Voting, National Academies Press.
Lederer, S., Hong, J. I., Dey, K., & Landay, A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, *8*(6), 440-454.
Little, L., Briggs, P., & Coventry, L. (2004, September). *Videotaped activity scenarios and the elicitation of social rules for public interactions*. Paper presented at the British Human Computer Interaction Group Conference, Leeds, UK.
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 M. Blaze (Ed.), *Financial cryptography, 6th International Conference, FC 2002, revised papers* (Vol. 2357 of *Lecture Notes in Computer Science*, pp. 1-15). London: Springer-Verlag.
McCandlish, S. (2002). EFF's top 12 ways to protect your online privacy. *Electronic Frontier Technology*. Retrieved January 1, 2007, from http://www.eff.org/Privacy/eff_privacy_top_12.html
Mercuri, R. (2001). *Electronic vote tabulation: Checks and balances*. Unpublished PhD thesis, University of Pennsylvania, Philadelphia.
Mercuri, R. (2002, July). *Humanizing voting interfaces*. Paper presented at the Usability Professionals Association Conference, Orlando, Florida.
Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *CHI Letters*, *5*(1), 129-136.
Raisinghani, M. S., Benoit, A., Ding, J., Gomez, M., Gupta, K., Gusila, V., et al. (2004). Ambient Intelligence: Changing forms of human-computer interaction and their social implications. *Journal of Digital Information*, *5*(4), No. 271.
Sillence, E., Briggs, P., Fishwick, L., & Harris, P. (2004). Trust and mistrust of online health sites. In *Proceedings of CHI'2004, April 24-29 2004, Vienna, Austria* (pp. 663-670). New York: ACM Press.
Storer, T., & Duncan, I. (2004). Pollsterless remote electronic voting. *Journal of E–Government*, *1*(1), 75-103.
Teltzrow, M., & Kobsa, A. (2003). *Impacts of user privacy preferences on personalized systems—A comparative study*. Paper presented at "Designing Personalized User Experiences for eCommerce: Theory, Methods, and Research" workshop, Fort Lauderdale, Florida.
Weiser, M. (1991). The computer for the 21st century. *Scientific American*, *265*(3), 66-75.

Linda Little is a lecturer within the Division of Psychology, Northumbria University, United Kingdom, and a member of the Psychology and Communication Technologies Lab. She has researched and published in the areas of privacy, trust, technology use in public places, and the impact of age and disability on technology use. She may be reached at l.little@unn.ac.uk.

Tim Storer is a research fellow at the School of Computer Science, University of St Andrews, Scotland, where he is a member of the Complex Systems Engineering Group. He may be reached at tws@cs.st-and.ac.uk.

Pam Briggs is a professor and dean of the School of Psychology and Sport Sciences and the director of the Psychology and Communication Technologies Lab. She has been involved with the field of human–computer interaction for the past 15 years. She has been principal investigator on a number of U.K. Research Council projects, including two Economic Social Research Council E-Society projects. She is particularly interested in trust, privacy, and identity issues in social technologies and in e-inclusion. She may be reached at p.briggs@unn.ac.uk.

Ishbel Duncan is a lecturer in the School of Computer Science at the University of St Andrews, Scotland. Her research interests are in software testing, mobile agents and privacy, security, and trust in online environments. She may be reached at ishbel@cs.st-and.ac.uk.