Lamming, M. and Newman W. (1991): "Activity-Based Information Retrieval Technology in Support of Personal Memory", EuroPARC Technical Report, EPC-91-103.1, 1991.

Lampson, B., Paul, M. and Siegert, H. (1981): *Distributed Systems - Architecture and Implementation*. Springer Verlag, 1981.

Louie, G., Mantei, M. and Sellen, A. (in press) "Making Contact in a Multi-Media Environment", to appear in *Behaviour and Interaction Technology*.

Mackay, W. (1991): "Ethical Issues in the Use of Video: Is it Time to Establish Guidelines?" SIGCHI Discussion Forum in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 403-405.

MacLean, A., Young, R., Bellotti, V. and Moran, T. (1991): "Questions, Options, and Criteria: Elements of a Design Rationale for user interfaces", *Human Computer Interaction*, vol 6 (3&4), pp. 201-250.

Mantei, M., Becker, R., Sellen. A., Buxton, W., Milligan, T. and Wellman, B. (1991): "Experiences in the Use of a Media Space" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 203-208.

McCarthy, J., Miles, V. and Monk, A. (1991): "An Experimental Study of Common Ground in Text-Based Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 209-215.

McGuffin, L. and Olson, G. (1992): "ShrEdit: A Shared Electronic Workspace", CSMIL Technical Report, Cognitive Science and Machine Intelligence Laboratory, University of Michigan, 1992.

Minneman, S. and Bly, S. (1991): "Managing à Trois: A Study of a Multi-User Drawing Tool in Distributed Design Work", in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April- May 1991, pp. 217-224.

Mullender, S. (1989) "Protection", in S. Mullender (ed.) *Distributed Systems*. Addison Wesley, 1989.

Parker, D., Swope, S. and Baker, B. (1990): *Ethical Conflicts in Information and Computer Science, Technology, and Business*, QED, Information Sciences Inc. Wellesley, MA, 1990.

Pedersen, E., McCall, K., Moran, T. and Halasz, F. (1993): "Tivoli: An Electronic Whiteboard for Informal Workgroup Meetings", in *Proc. INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Privacy Protection Study Commission (1991): "Excerpts from Personal Privacy in an Information Society" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 453-468.

Richards, E. (1991): "Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy", in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 436-438.

Root, R. (1988) "Design of a Multi-Media Vehicle for Social Browsing" in *Proc. ACM Conference on Computer Supported Cooperative Work, CSCW'88*, Portland Oregon, September 26-29, 1988, pp. 25-38.

Stults, R. (1988): "The Experimental Use of Video to Support Design Activities", Xerox PARC Technical Report SSL-89-19, Palo Alto, California, 1988.

Tang, J. and Minneman, S. (1991): "VideoWhiteboard: Video Shadows to Support Remote Collaboration" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 315-322.

Want, R., Hopper, A., Falcco, V. and Gibbons, J.(1992): "The Active Badge Location System", *ACM Transactions on Office Information Systems*, January, 1992, 10(1), pp. 91-102.

Weiser, M. (1991): "The Computer for the 21st Century", *Scientific American*, September, 1991, pp. 94-104.

References

Anderson, R. (1991): *The Ethics of Research into Invasive Technologies*. Technical Report, EPC-91-107, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Bellotti, V. (1993): "Integrating Theoreticians' and Practitioners' Perspectives with Design Rationale" in *Proceedings of INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Buxton, W. and Moran, T. (1990): "EuroPARC's Integrated Interactive Intermedia Facility (IIIF): Early Experiences". *IFIP Conference on Multi-User Interfaces and Applications*, Herakleion, Crete, September 1990.

Clarke, R. (1988): "Information Technology and Dataveillance", *Communications of the ACM*, 31, 5, 1988, pp. 498-512.

Cool, C., Fish, R., Kraut, R. and Lowery, C. (1992): "Iterative Design of Video Communication Systems" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 25-32.

Dourish, P. (1991): "Godard: A Flexible Architecture for A/V Services in a Media Space" Technical Report EPC-91-134, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Dourish, P. and Bly, S. (1992): "Portholes: Supporting Awareness in Distributed Work Groups" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'92*, Monterey, California, May 1992. pp. 541-547.

Dourish, P. (1993): "Culture and Control in a Media Space", in *Proc. European Conference on Computer-Supported Cooperative Work ECSCW'93*, Milano, Italy, September, 1993.

Dunlop, C. and Kling, R. (1991): *Computerization and Controversy: Value Conflicts and Social Choices*. Academic Press, Inc., 1991.

Eldridge, M., Lamming, M. and Flynn, M. (1992): "Does a Video Diary Help Recall?" in *People and Computers VII, Proceedings of the HCI'92 Conference*, York, UK, September, 1992, pp. 257-269.

Fish, R., Kraut, R. and Root, R. (1992): "Evaluating Video as a Technology for Informal Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May, 1992, pp. 37-47.

Gaver, W. (1991): "Sound Support for Collaboration" in *Proc. European Conference on Computer-Supported Cooperative Work, ECSCW'91*, Amsterdam, The Netherlands, September, 1991, pp. 293-308.

Gaver, B., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter K. and Buxton, B. (1992): "Realising a Video Environment: EuroPARC's RAVE System" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May 1992, pp. 27-35.

Gaver, B. (1992): "The Affordance of Media Spaces for Collaboration" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 17-24.

Goffman, E., *Behaviour in Public Places*. The Free Press, 1963.

Harper, R., Lamming, M. and Newman, W. (1992): "Locating Systems at Work: Implications for the Development of Active Badge Applications", *Interacting with Computers*, 4, 3, 1992, pp.343-363.

Heath, C. and Luff, P. (1991): "Disembodied Conduct: Communication through Video in a Multi-Media Office Environment" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 99-103.

Heath, C. and Luff, P. (1992): "Collaboration and Control: Crisis Management and Multimedia Technology in London Underground Line Control Rooms", *Computer Supported Cooperative Work (CSCW)*, 1, 1992, 69-94.

Hindus, D. and Schmandt, C. (1992): "Ubiquitous Audio: Capturing Spontaneous Collaboration" in *Proc. ACM Conference on Computer-Supported Cooperative Work, CSCW'92*, Toronto, Canada, October-November, 1992, pp. 210-217.

Ladd, J. (1991): "Computers and Moral Responsibility: A Framework for Ethical Analysis" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 664-675.

style media space could seem very sinister indeed. It is thus quite understandable that many visitors to the lab experience some trepidation.

RAVE is a research tool and is also itself the object of research, like all of the ubiquitous computing systems at EuroPARC. It is not intended to be a model for a commercial, standard media space. Rather, it is an instance of a facility which has evolved inextricably with a culture of use and is only thus acceptable to members of that culture. The problems highlighted by our framework could, however, point to design refinements which might be essential in other contexts.

Another issue which the framework helps to elucidate, is the delicate balance that exists between awareness and privacy. Providing too much awareness of other people's activity and availability may be seen as intrusive. However, too little awareness may result in inadvertent invasions of privacy such as when people cannot tell how receptive another person is to being disturbed. The aim then is to provide awareness without crossing the line into intrusiveness.

A related issue is that data which could be feedback to one person may feature someone else's personal information which they might not want to make available. For example, our proposal to display large Portholes images of people currently connected to the Commons camera may make them feel as if they are on display. This suggests that designs which solve some privacy problems may cause others. Our framework must therefore be applied not only to the systems in place, but also to the privacy solutions themselves.

It is often the case that design decisions involve trade-offs and compromises. Designing to protect privacy is extreme in this respect. There is no guarantee that features put in place to protect privacy will confer the benefits that the designer intends. We therefore aim to prototype some the design refinements we have suggested and evaluate these in use at EuroPARC in the near future.

The framework described in this paper aims to provide a systematic basis for tackling a range of user-interface design problems. The problems we have been dealing with are those that interfere with interactions between people and the exchange of personal information and that are likely to arise with CSCW systems and, in particular, media space and other ubiquitous computing systems. Perhaps more important, we have made the case that *privacy is a user-interface design issue*, and one which we hope will become an increasingly integral part of the design process of information technology in general.

Acknowledgements

We wish to thank Mike Molloy and Paul Dourish for their support in implementing some of our design ideas. We also thank Bob Anderson, Sara Bly, Graham Button, Matthew Chalmers, Paul Dourish, Bill Gaver, Steve Harrison, Mik Lamming, Paul Luff, Wendy Mackay, Allan MacLean, Scott Minneman, William Newman and Peter Robinson for interesting discussions and helpful comments on drafts of this paper.

Anyone who objects to this can either avoid the label wearers or ask the researchers concerned to make sure that they are not recorded.

Use of the framework

In the example, our framework serves three important purposes.

- It helps to clarify the existing state of affairs with respect to privacy problems, and social norms and practices currently in place.
- By clarifying the problems, it helps to point to possible design solutions and explore a range of possibilities.
- It is used to assess the solutions in terms of how they might reduce the existing problems as well as how they might cause new ones.

With regard to this last issue, it is important to point out that, while the framework and design criteria help us evaluate proposed solutions prospectively, it is only by implementing these solutions that we can truly judge their usefulness. A case in point is the software infrastructure, Godard, whose privacy feature allows users to select who is allowed to connect to them. Consistent with the criterion of being fail-safe, the default is that lab newcomers are automatically denied access until each person in the lab explicitly allows them access. Unfortunately, because lab members generally forget to change their settings, newcomers find that they are unable to connect to anyone. As a result, they have been known to give up trying and thus never get in the habit of using RAVE. There are simple solutions to this problem, like automatically notifying people to whom an unsuccessful attempt to connect has been made. However, many problems are not foreseen and thus evaluation through use must always be part of the design cycle.

In addition, the framework itself needs to be evaluated and refined. To do this we will be applying it to a range of existing ubiquitous computing technology at EuroPARC. In doing so we hope to identify how it needs to be enhanced or extended.

Discussion and conclusions

In this paper we have focused on technical, rather than social or policy solutions for protecting privacy in ubiquitous computing environments. We have argued that this is an important design focus, and offered a framework as guidance. That being said, it is interesting that the framework has also highlighted ways in which cultural norms and practices affect and sometimes ameliorate privacy concerns.

In spite of shortcomings which our framework highlights, RAVE is, in general, very acceptable to lab members. In part, this is because feedback and control of information capture are well attended to overall in its design, enabling people to orient themselves appropriately to the technology. Further, lab members know roughly how it works, and trust the benign culture which governs its use. Visitors have no such knowledge or trust, and one can imagine that, other contexts, a RAVE

images of who is currently connected to the camera onto the wall. However, this would be *expensive*, and possibly *intrusive* to those who connect to a public area.

Audio feedback: In private offices audio feedback alerts occupants to onset and termination of short term glance connections. Such feedback about video connections to the Commons would be *inappropriately timed*, since they are normally of the long term background variety which outlast most visits to the room.

Q: What feedback is provided about the purposes of using information about me?

No Existing Solution

There is no technical feedback about the intentions of those who access the video signal. However, lab members are reasonably confident that their privacy is not threatened by others' uses of information, probably because, in a public area, they already behave in what they consider to be a publicly presentable and acceptable fashion.

Proposed Solution:

We cannot provide technological feedback about people's intentions. These may only be deduced from feedback about capture, access and utilisation of information, together with knowledge of the culture, context and individuals concerned.

Q: What control is there over when and when not to give out what information?

Existing Solutions:

Moving off camera: People can move on or off camera; there is a "video-free zone" in the commons for those who want to relax in private. This kind of solution is very *easy to learn*.

Covering the camera: If certain activities, such as the potentially embarrassing "weekly step-aerobics work-out," are taking place in the commons, the camera lens is covered. This is an extremely *trustworthy* solution.

Behaving appropriately: If people have to walk in front of the camera, they can orient themselves appropriately to it given the *meaningful* feedback they obtain from the confidence monitor (for example, they will probably not get too close or stare into it for fear of appearing foolish).

Control over what happens to information, who can access it and for what purposes it is used?

We do not propose to give individuals any additional technical control over the capture, construction and access of the Commons video signal because it is a *public* rather than a private information source. Technical control over purposes for which information can be used, however, is impractical with any information source, whether public or private. At EuroPARC, social control is effectively exercised. The culture of acceptable use which has evolved with RAVE dictates that certain practices are frowned upon.

Lab members are always expected to warn others that constructions and access other the normal background connection, glance and Portholes services, are occurring. For example, Vepys video diary experiments, in which subjects have their picture taken wherever they go, are announced to all lab members and the subjects wear labels to warn of potential recording of camera images in areas they enter.

however it is less *meaningful* because it doesn't tell you whether the camera is on, or if you are in its view.

Alternative Solution:

Movement Sensors: A solution which might supplement the use of confidence monitors would be to try using infra-red devices to alert people, either with an audio or visual signal, when they move into the field of view of a camera. These would provide *appropriately timed* feedback about onset of capture of video information, however they would not be *meaningful* without some other form of feedback.

Q: What feedback is there about what happens to information about me inside the system?

No Existing Solution:

The confidence monitor does not inform visitors and newcomers to the lab that the video signal is sent to a switch. This can potentially direct the signal to any number of nodes, recording devices or ubiquitous computing services in the lab. Unfortunately Toby cannot tell you whether recording or some other construction of video data is taking place. In fact the EuroPARC policy is that recording never takes place without warnings to lab members.

Proposed Solutions:

LED display: A simple design solution would be to have an LED status display by the camera, connected to the media space switch and other devices responsible for collecting, recording and distributing the video signal. This is a *low cost* proposal to give *appropriately timed* feedback about when and which services are actively collecting information. Unfortunately it might not be sufficiently *perceptible*.

Audio and video feedback: We could provide audio feedback to indicate connections and image framegrabbing but it could be *obtrusive* and *annoying* to provide repeated audio feedback to a public area at a sufficient volume to be heard all round the room. An alternative would be to superimpose the flashing word "Recording" on the screen of the confidence monitor. This would have to be refined to find a solution which draws attention whilst being *unobtrusive*.

Q: What feedback is given about who has access to information about me and what information they see?

Existing Solutions:

Textual information: In order to warn people that they might be "watched", Toby wears a sweatshirt with the message "I may be a dummy but I'm watching you!" printed on it. Together with the fact that Toby is holding a camera, the *meaning* of this is fairly clear in a general sense, but not specific enough about who is doing the watching and when.

Proposed Solutions:

Viewer display: One option is to display a list of names or pictures on the wall to indicate who can watch a public area. If we want to update the information we could adapt Portholes, an "awareness sever" which distributes images to EuroPARC and PARC media space users (Dourish & Bly, 1992). In order to be *perceptible* to passers by, the display would have to be larger than a normal monitor. We could project

Meaningfulness: Feedback and control must incorporate meaningful representations of information captured and meaningful actions to control it, not just raw data and unfamiliar actions. They should be sensitive to the context of data capture and also to the contexts in which information is presented and control exercised.

Learnability: Proposed designs should not require a complex model of how the system works. They should exploit or be sensitive to natural, existing psychological and social mechanisms that allow people to perceive and control how they present themselves and their availability for potential interactions.

Low cost: Naturally, we wish to keep costs of design solutions down.

The first seven criteria are especially relevant to protection of privacy. The final four are more general design concerns. Some of these criteria have to be traded off against one another in the search for design solutions.

Applying the framework: Feedback and control for video data from a public area

We have begun to apply our framework to RAVE to reveal aspects of its design which can be refined. For the sake of brevity, we focus on just one aspect of this media space which involves a video connection from the Commons, a public reading and meeting area at EuroPARC.

In RAVE, people can access the camera in the Commons either in the form of short glance or indefinite, background, video-only connections. The video data can sent to devices such as a framegrabber which takes digitised video snaps. These can be used by various services such as Vepys, a video diary which takes still images of people via media space cameras, every so often, wherever they are, and stores the series of images as a browsable record of their day-to-day activity (Eldridge, 1992).

Providing feedback and control mechanisms over video data taken from this public area is a challenging problem but it is an important one, since the Commons is an area where many visitors to EuroPARC spend their time.

Our framework prompts us to ask the following questions for which we describe existing or potential design solutions (relevant criteria appear in italics):

Q: What feedback is there about when and what information about me gets into the system?

Existing Solutions:

Confidence monitor: A monitor is positioned next to the camera to inform passers by when they are within range, and what they look like. This solution fulfils the design criteria of being *trustworthy, meaningful* and *appropriately timed*.

Mannequin (the Toby): In order to alert people to the presence of the camera, a mannequin affectionately named Toby is positioned holding the camera. Toby draws people's attention because he looks like another person in the room. Originally the camera was in his head, but this concealed it and some visitors thought it was deliberately being hidden. Now Toby holds the camera on his shoulder. This feedback is *less obtrusive* than the confidence monitor (which can be distracting),

questions, are explicitly represented together with proposed solutions and their assessments (for more details see MacLean et al., 1991; Bellotti, 1993).

The issues in the cells within the framework are not necessarily independent of one another. For instance, in order to be fully informed about the purpose of information usage, one must know something about each of the other behaviours. Likewise, in order to appreciate access, one must know about capture and construction. Understanding construction requires knowing something about capture. Hence there is a dependency relationship for design of feedback between these behaviours. Control over each of them may, however, be relatively independently designed.

For those concerned about privacy, and the potential for subversion in particular, control over, and thus feedback about, capture is clearly the most important. Given appropriate feedback about what is being captured, users can orient themselves appropriately to the technology for collaboration or communication purposes and exercise appropriate control over their behaviour or what is captured in the knowledge of possible construction, access and purposes of information use.

Evaluating solutions

Our framework emphasises design to a set of criteria, which may be extended through experience and evaluation. Whilst questions about what feedback and control to provide set the design agenda, criteria represent additional and sometimes competing concerns which help us to assess and distinguish potential design solutions. The set of criteria acts as a checklist helping to encourage systematic evaluation of solutions. They have been identified from our experiences with the design and use of a range of ubiquitous computing services. Particularly important in our current set are the following eleven criteria.

Trustworthiness: Systems must be technically reliable and instill confidence in users. In order to satisfy this criterion, they must be understandable by their users. The consequences of actions must be confined to situations which can be apprehended in the context in which they take place and thus appropriately controlled.

Appropriate timing: Feedback should be provided at a time when control is most likely to be required and effective.

Perceptibility: Feedback should be noticeable.

Unobtrusiveness: Feedback should not distract or annoy. It should also be selective and relevant and should not overload the recipient with information.

Minimal intrusiveness: Feedback should not involve information which compromises the privacy of others.

Fail-safety: In cases where users omit to take explicit action to protect their privacy, the system should minimise information capture, construction and access.

Flexibility: What counts as private varies according to context and interpersonal relationships. Thus mechanisms of control over user and system behaviours may need to be tailorable to some extent by the individuals concerned.

Low effort: Design solutions must be lightweight to use, requiring as few actions and as little effort on the part of the user as possible.

	Feedback About	Control Over
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Figure 1. A framework for designing for feedback and control in ubiquitous computing environments: Each cell contains a description of the ideal state of affairs with respect to feedback or control of each of four types of behaviour.

Accessibility: Is information public, available to particular groups, certain persons only, or just to oneself? What applications, processes, and so on utilise personal data.

Purpose: To what uses is information put? How might it be used in the future? The intentions of those who wish to use data may not be made explicit. It may only be possible to infer what these are from knowledge of the person, the context, patterns of access and construction.

We now consider each of these four classes of concerns in relation to the following two questions:

What is the appropriate feedback?

What is the appropriate control?

We thus have eight design questions which form the basis for a design framework (Figure 1) with which we can analyse existing designs and explore new ones, with respect to a range of privacy issues. This framework is a domain specific example of the QOC approach to design rationale in which design issues, couched as

It must be pointed out that the technology itself is not inherently problematic. Resources used in face-to-face situations can be exploited, simulated, or substituted through design. For example media space systems can embody the principle “If I see your face, you see mine,” which is natural in face-to-face situations (e.g., VideoTunnels; Buxton & Moran, 1989) or they can supply means to convey availability (e.g., Louie et al., 1992). Dissociation problems in CSCW systems have been reduced by means of conveying gestures, or even body posture (e.g. Minneman & Bly, 1991; Tang & Minneman, 1991).

Our ongoing research assumes that problems of interaction, communication and privacy in ubiquitous computing systems, can be reduced through technological design refinements and innovations. Disembodiment and dissociation may be reduced through the provision of enriched feedback about the state of the technology and information being projected about users. Users must also have practical mechanisms of control over that personal information. We now present a framework for systematically addressing these issues. Although it may have general use for designing CSCW technology to support social interaction and communication, we focus in particular on how it helps us confront privacy as a central design concern.

A design framework

Based on our experience with privacy issues in RAVE and other similar systems, we have developed a simple design framework aimed at counteracting the kinds of problems we have outlined.

Addressing the problems

Much of the mutual awareness, which we normally take for granted may be reduced or lost in mediated interpersonal interactions. We may no longer know what information we are conveying, what it looks like and how permanent it is, who it is conveyed to, or what the intentions of those using that information might be. In order to counteract problems associated with this loss, our framework proposes that systems must be explicitly designed to provide feedback and control for at least the following potential user and system behaviours:

Capture: What kind of information is being picked up? Candidates include voices, actual speech, moving video or framegrabbed images (close up or not), personal identity, work activity and its products such as keypresses, applications used, files accessed, messages and documents.

Construction: What happens to information? Is it encrypted or processed at some point or combined with other information and, if so, how? Is it stored? In what form? Privacy concerns in ubiquitous computing environments are exacerbated by the fact that potential records of our activity may be kept and possibly manipulated, and used at a later date and out of their original context. This leads to numerous potential ethical problems (Mackay, 1991).

In CSCW and ubiquitous computing environments disembodiment means that these resources may be attenuated. So you may not be able to present yourself as effectively to others as you can in a face-to-face setting. For example, in an AV connection, you may only be a face on a monitor (Gaver, 1992) with your voice coming out of a loudspeaker, the volume of which you may not be aware or able to control. You may only appear as a name (McCarthy et al., 1991) or a name associated with a room displayed on a screen (e.g., Harper et al., 1992). At worst (e.g., in a RAVE background connection) you may have no perceptible presence at all. On the other hand, disembodiment also means that you may be unaware of when you are convey information to others because of a lack of feedback from the technology.

Dissociation occurs in CSCW applications when only the results of actions are shared, but the actions themselves are invisible. In other words when you cannot easily determine who is doing, or did, what (e.g., ShrEdit, a shared editor with no telepointers; McGuffin & Olson, 1992).

Gaining information: In face-to-face situations, cues given by others influence your judgements about whether to attempt conversation, what to say and how to act.

In media spaces, there is usually no way to gauge how available someone else is before connecting to them (Louie et al., in press). Once connected, awareness of the person at the other end of the link or their actions is likely to be limited to the fixed and narrow field of view of a camera, and whatever a microphone picks up (Gaver, 1992). That person also has a reduced, disembodied presence. In turn, you are likely to receive fewer cues when someone is observing you, or your work.

Breakdown of social and behavioural norms and practices

The effects of disembodiment and dissociation manifest themselves in a variety of breakdowns in behavioural and social norms and practices. For example, breakdowns associated with disembodiment include a tendency for users to engage in unintentional, prolonged observation of others over AV links (Heath & Luff, 1991). Users may intrude when they make AV connections, because they cannot discern how available others are (Louie et al., in press). Furthermore, the intuitive principle that if I can't see you then you can't see me, does not necessarily apply to computer mediated situations where one person may be able to observe others' activities without themselves being observed.

A major problem related to dissociation is one's inability to respond effectively to a perceived action because one does not know who is responsible for it. A familiar example of this problem exists with telephones where it is impossible to identify nuisance callers before picking up the receiver.

Problems of disembodiment and dissociation receive far less attention in the literature than insidious exploitation of technology. This is unfortunate as they are also problems for social interaction and communication mediated by technology and likely to be much more pervasive, particularly because they often relate to purely unintentional invasions of privacy. Furthermore, by addressing these problems through careful design, we may reduce the potential impact of system abuse.

glances, audio feedback (Gaver, 1991) alerts users to onset and termination of a connection and can even announce who is making it. For the two-way office connections, reciprocity acts as a form of feedback about the connection (if I see you, you see me) and, in the case of an attempted v-phone connection, an audio "ringing" signal is given and the caller's name is displayed on the workstation, whereupon the recipient can decide whether to accept or reject the connection. Office-shares, being very long term, do not require such a protocol.

Public areas have cameras which can be accessed by a glance or a "background" connection which is indefinite, one-way and video-only. We provide feedback about the presence of a camera in a public place in the form of a video monitor beside the camera which displays its view.

Control and feedback also figure strongly in the design of RAVE's architecture. Connection capability lists and an access control model define who can connect to whom and provide long term, static control over accessibility. Providing distinct connection types can also allow users to exercise discriminating dynamic control over their accessibility as in the v-phone call (for a fuller description of these features see Dourish, 1993). Our concern, however, is with the moment-to-moment continuous control that people exercise over how they present themselves in public as respectable, social beings (Goffman, 1963). In the next section we indicate why people, especially newcomers and visitors to places with media spaces and other kinds of ubiquitous computing technology, can feel uneasy about their ability to monitor and control their self presentation and consequently their privacy.

Disembodiment and dissociation

A number of problems with RAVE relate to the extended duration of v-phone calls and office-shares. Users tend to forget about their existence and associated implications. Even seasoned users can get confused about the nature of their connections. For example, if a colleague with whom you have an office-share switches off their camera or moves out of shot, it is easy to forget that they can still see you.

Problems in public areas include the fact that monitors next to cameras only suggest (and then only to those familiar with a media space) that a video image may be being broadcast to many people, via background connections. They cannot inform people when or to whom the image is being sent. For most EuroPARC "regulars" this is not a major concern, but for newcomers to the building, it may be.

The underlying causes of such problems lie in the fact that the technology results in *disembodiment* from the context into and from which one projects information (Heath & Luff, 1991) and *dissociation* from one's actions. These phenomena interfere with conveying information about oneself or gaining information about others.

Conveying information: In the presence of others you convey information in many ways. These include position, posture, facial expression, speech, voice level and intonation, and direction of gaze. Such cues influence the behaviour of others. For example, they can determine whether or not others will try to initiate communication with you.

ing without leaving one's office. Various kinds of flexible video-only and AV connections between nodes are set up and broken by central switching devices which are controlled from individual workstations.

Whilst media space technology improves the accessibility of people to one another, some may feel that their privacy is compromised. The very ubiquity of such systems means that many of the concerns with existing workstation-based information systems are aggravated. A much wider variety of information can now be captured. People are much less likely to be "off-line" (inaccessible) at any given moment. Further, the design of many of these systems is such that it may not be clear when one is off- or on-line and open to scrutiny (Mantei et al., 1991; Gaver, 1992). People also express concern about their own intrusiveness to others when they try to make contact without being able to determine others' availability (Cool et al., 1992). Concerns about such problems have strongly influenced the installation and ongoing design of RAVE, as well as the way in which people use it.

Feedback and control in RAVE

At EuroPARC people generally do not worry much about privacy. They feel that the benefits of RAVE outweigh their concerns. This is because the design has evolved together with a culture of trust and acceptable practices relating to its use. Individual freedom was fostered to use, customise, or ignore the technology. Design was informed by studies of how collaborative work is socially organised and how such technology impacts it (e.g. Heath & Luff, 1991; 1992). Users' views and reactions were obtained via questionnaires and interviews. The varied individual feelings about privacy were accommodated by ensuring that users could decide how accessible they were to others via the media space (Dourish, 1991; Gaver et al., 1992; Dourish, 1993).

In designing for privacy in RAVE, two important principles have emerged (Gaver et al, 1992). These are *control* and *feedback*, which we define as follows:
Control: Empowering people to stipulate what information they project and who can get hold of it.
Feedback: Informing people when and what information about them is being captured and to whom the information is being made available.

RAVE users can control who may connect to them and what kind of connections each person is allowed make. If they omit to do so, automatic defaults are set to reject connections. User control via the workstation is supported by "Godard", the software infrastructure which provides the primary interface to the complex AV signal-switching and feedback mechanisms (Dourish,1991). These mechanisms comprise the kinds of connections which can be made between people, to different public areas, and to media services (e.g., video-players).

Feedback depends on the type of RAVE connection being made. Three kinds of interpersonal connection are "glance", "v-phone call" and "office-share". Glance connections are one-way, video-only connections of a few seconds' duration. V-phone and office-share connections are longer two-way AV connections. For

with one such environment. However, our framework may also be related to the design of CSCW systems and distributed computing environments in general.

In the following sections we first introduce the context and nature of the technology which is the focus of our interest, we then go on to outline our design framework and provide a brief example of its application.

Maintaining privacy in a media space

The need to understand and protect personal privacy in sophisticated information systems is becoming critical as computing power moves out of the box-on-the-desk into the world at large. We are entering the age of *ubiquitous computing* (e.g., Weiser, 1991; Lamming & Newman, 1991; Hindus & Schmandt, 1992) in which our environment comes to contain computing technology in a variety of forms.

Increasingly, we are seeing such systems incorporate sensors such as microphones, cameras and signal receivers for wireless communication. These sensors have the potential to transmit information such as speech, video images, or signals from portable computing devices, active badges (Want et al., 1992), electronic whiteboards (Pederson et al., 1993), and so on. These devices can be networked so that multimedia information can be stored, accessed, processed and distributed in a variety of ways. Services include audio-video (AV) interconnections, information retrieval, diary systems, document tracking and so on (e.g., Lamming & Newman, 1991; Gaver, 1992; Eldridge et al., 1992).

Ubiquitous computing usually implies embedding the technology unobtrusively within all manner of everyday objects which can potentially transmit and receive information from any other object. The aims are not only to reduce its visibility, but also to empower its users with more flexible and portable applications to support the capture, communication, recall, organisation and reuse of diverse information. The irony is that its unobtrusiveness both belies and contributes to its potential for supporting potentially invasive applications.

In light of these developments, it is dangerously complacent to assume that social and organisational controls over accessibility of personal information are sufficient, or that intrusions into privacy will ultimately become acceptable when traded against potential benefits. Such a position could leave individual users with a heavy burden of responsibility to ensure that they do not, even inadvertently, intrude on others. It also leaves them with limited control over their own privacy.

"Media spaces" (Stults, 1988) are a recent development in ubiquitous computing technology, involving audio, video and computer networking. They are the focus of an increasing amount of research and industrial interest into support for distributed collaborative work (e.g., Root, 1988; Mantei et al., 1991; Gaver et al., 1992; Fish et al., 1992). EuroPARC's RAVE environment is just one of several media spaces which have been set up in various research laboratories around the world.

In RAVE, cameras, monitors, microphones and speakers are placed in every office, to provide everyone with their own personal RAVE *node*. This allows one to communicate and work with others and to be aware of what is going on in the build-

Deliberate or poorly considered design resulting in invasive applications and sophisticated subversion of supposedly secure systems are discouraged by cultural censure and law (although these forces trail behind the advances in sophistication of the technology). However, software must still be secure in order to reduce the risks of covert abuse of personal data and this is an important area of research. There are already a number of useful software protection models and standards which are designed to reduce the risks (see e.g., Lampson et al., 1981; and Mullender, 1989).

The second class of problem is related to very different concerns about a fast growing, less well understood set of issues. These arise from user-interface design features which interfere with social behaviour. These features may foster unethical use of the technology but, more significantly, they are also much more conducive to inadvertent intrusions on privacy (Heath & Luff, 1991).

Mediated interactions between people via technology are prone to breakdowns due to inadequate feedback about what information one is broadcasting and an inability to control one's accessibility to others. This disrupts the social norms and practices governing communication and acceptable behaviour. Our concern in this paper is tackle the latter kind of problem in the context of systems design.

In attempting to design systems which reduce perceived invasions of privacy, it would be useful to have a practical working definition of the concept. Unfortunately, although privacy is widely considered to be an important right, it is difficult to define this notion in more than an intuitive fashion (Anderson, 1991). Attitudes to what is and what is not private data vary between people in different contexts and roles (Harper et al., 1992). Codes of practice and the law offer inadequate guidance on what actually counts as violation of privacy in technologically sophisticated environments (Clarke, 1988) and it may take lengthy court proceedings to determine what the case may be (Privacy Protection Study Commission, 1991).

Any realistic definition of privacy cannot be static. With the introduction of new technology, patterns of use and social norms develop around it and what is deemed "acceptable" behaviour is subject to change. Naturally evolving social practices may interact with organisational policies for correct usage (Harper et al., 1992). In addition, people are more prepared to accept potentially invasive technology if they consider that its benefits outweigh potential risks (e.g., Ladd, 1991; Richards, 1991). In recognition of these facts we take privacy to be a personal notion shaped by culturally determined expectations and perceptions about one's environment.

The social practices and policies that determine any *rights* an individual has to privacy interact with the technical and interface design aspects of the technology they use. Technology is not neutral when it comes to privacy. It can increase or reduce the extent to which people have control over personal data. Our concern is to ensure that privacy should be a central design issue in its own right.

We present a framework for addressing the design of *control* and *feedback* of information captured by multimedia, ubiquitous computing environments. These two issues are fundamental to successful communication and collaboration amongst users as well as to maintaining privacy. We ground our examples largely in the domain of networked audio-video environments and in particular in experiences

Design for Privacy in Ubiquitous Computing Environments

Victoria Bellotti* and Abigail Sellen*†
* Rank Xerox EuroPARC, Cambridge, UK
bellotti@europarc.xerox.com; sellen@europarc.xerox.com

†MRC Applied Psychology Unit, Cambridge, UK

Abstract: Current developments in information technology are leading to increasing capture and storage of information about people and their activities. This raises serious issues about the preservation of privacy. In this paper we examine why these issues are particularly important in the introduction of ubiquitous computing technology into the working environment. Certain problems with privacy are closely related to the ways in which the technology attenuates natural mechanisms of feedback and control over information released. We describe a framework for design for privacy in ubiquitous computing environments and conclude with an example of its application.

Introduction

Information technology can store, transmit and manipulate vast quantities and varieties of information. Whilst this is critical to government, public services, business and many individuals, it may also facilitate unobtrusive access, manipulation and presentation of personal data (Parker et al., 1990; Dunlop & Kling, 1991).

The term “Big Brother” in the context of computing technology, seems to imply two classes of problem. The first is due to the fact that computer technology may be put to insidious or unethical uses (e.g., Clarke, 1988). All information systems, and particularly distributed systems, are potentially vulnerable to covert subversion (Lampson et al., 1981) and, although it can be made extremely difficult to tamper with data in computing systems, protection mechanisms “are often only secure *in principle*. They are seldom secure *in practice*.” (Mullender, 1989).

Lamming, M. and Newman W. (1991): "Activity-Based Information Retrieval Technology in Support of Personal Memory", EuroPARC Technical Report, EPC-91-103.1, 1991.

Lampson, B., Paul, M. and Siegert, H. (1981): *Distributed Systems - Architecture and Implementation*. Springer Verlag, 1981.

Louie, G., Mantei, M. and Sellen, A. (in press) "Making Contact in a Multi-Media Environment", to appear in *Behaviour and Interaction Technology*.

Mackay, W. (1991): "Ethical Issues in the Use of Video: Is it Time to Establish Guidelines?" SIGCHI Discussion Forum in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 403-405.

MacLean, A., Young, R., Bellotti, V. and Moran, T. (1991): "Questions, Options, and Criteria: Elements of a Design Rationale for user interfaces", *Human Computer Interaction*, vol 6 (3&4), pp. 201-250.

Mantei, M., Becker, R., Sellen. A., Buxton, W., Milligan, T. and Wellman, B. (1991): "Experiences in the Use of a Media Space" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 203-208.

McCarthy, J., Miles, V. and Monk, A. (1991): "An Experimental Study of Common Ground in Text-Based Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 209-215.

McGuffin, L. and Olson, G. (1992): "ShrEdit: A Shared Electronic Workspace", CSMIL Technical Report, Cognitive Science and Machine Intelligence Laboratory, University of Michigan, 1992.

Minneman, S. and Bly, S. (1991): "Managing à Trois: A Study of a Multi-User Drawing Tool in Distributed Design Work", in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April- May 1991, pp. 217-224.

Mullender, S. (1989) "Protection", in S. Mullender (ed.) *Distributed Systems*. Addison Wesley, 1989.

Parker, D., Swope, S. and Baker, B. (1990): *Ethical Conflicts in Information and Computer Science, Technology, and Business*, QED, Information Sciences Inc. Wellesley, MA, 1990.

Pedersen, E., McCall, K., Moran, T. and Halasz, F. (1993): "Tivoli: An Electronic Whiteboard for Informal Workgroup Meetings", in *Proc. INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Privacy Protection Study Commission (1991): "Excerpts from Personal Privacy in an Information Society" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 453-468.

Richards, E. (1991): "Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy", in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 436-438.

Root, R. (1988) "Design of a Multi-Media Vehicle for Social Browsing" in *Proc. ACM Conference on Computer Supported Cooperative Work, CSCW'88*, Portland Oregon, September 26-29, 1988, pp. 25-38.

Stults, R. (1988): "The Experimental Use of Video to Support Design Activities", Xerox PARC Technical Report SSL-89-19, Palo Alto, California, 1988.

Tang, J. and Minneman, S. (1991): "VideoWhiteboard: Video Shadows to Support Remote Collaboration" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 315-322.

Want, R., Hopper, A., Falcco, V. and Gibbons, J.(1992): "The Active Badge Location System", *ACM Transactions on Office Information Systems*, January, 1992, 10(1), pp. 91-102.

Weiser, M. (1991): "The Computer for the 21st Century", *Scientific American*, September, 1991, pp. 94-104.

References

Anderson, R. (1991): *The Ethics of Research into Invasive Technologies*. Technical Report, EPC-91-107, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Bellotti, V. (1993): "Integrating Theoreticians' and Practitioners' Perspectives with Design Rationale" in *Proceedings of INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Buxton, W. and Moran, T. (1990): "EuroPARC's Integrated Interactive Intermedia Facility (IIIF): Early Experiences". *IFIP Conference on Multi-User Interfaces and Applications*, Herakleion, Crete, September 1990.

Clarke, R. (1988): "Information Technology and Dataveillance", *Communications of the ACM*, 31, 5, 1988, pp. 498-512.

Cool, C., Fish, R., Kraut, R. and Lowery, C. (1992): "Iterative Design of Video Communication Systems" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 25-32.

Dourish, P. (1991): "Godard: A Flexible Architecture for A/V Services in a Media Space" Technical Report EPC-91-134, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Dourish, P. and Bly, S. (1992): "Portholes: Supporting Awareness in Distributed Work Groups" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'92*, Monterey, California, May 1992. pp. 541-547.

Dourish, P. (1993): "Culture and Control in a Media Space", in *Proc. European Conference on Computer-Supported Cooperative Work ECSCW'93*, Milano, Italy, September, 1993.

Dunlop, C. and Kling, R. (1991): *Computerization and Controversy: Value Conflicts and Social Choices*. Academic Press, Inc., 1991.

Eldridge, M., Lamming, M. and Flynn, M. (1992): "Does a Video Diary Help Recall?" in *People and Computers VII, Proceedings of the HCI'92 Conference*, York, UK, September, 1992, pp. 257-269.

Fish, R., Kraut, R. and Root, R. (1992): "Evaluating Video as a Technology for Informal Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May, 1992, pp. 37-47.

Gaver, W. (1991): "Sound Support for Collaboration" in *Proc. European Conference on Computer-Supported Cooperative Work, ECSCW'91*, Amsterdam, The Netherlands, September, 1991, pp. 293-308.

Gaver, B., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter K. and Buxton, B. (1992): "Realising a Video Environment: EuroPARC's RAVE System" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May 1992, pp. 27-35.

Gaver, B. (1992): "The Affordance of Media Spaces for Collaboration" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 17-24.

Goffman, E., *Behaviour in Public Places*. The Free Press, 1963.

Harper, R., Lamming, M. and Newman, W. (1992): "Locating Systems at Work: Implications for the Development of Active Badge Applications", *Interacting with Computers*, 4, 3, 1992, pp.343-363.

Heath, C. and Luff, P. (1991): "Disembodied Conduct: Communication through Video in a Multi-Media Office Environment" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 99-103.

Heath, C. and Luff, P. (1992): "Collaboration and Control: Crisis Management and Multimedia Technology in London Underground Line Control Rooms", *Computer Supported Cooperative Work (CSCW)*, 1, 1992, 69-94.

Hindus, D. and Schmandt, C. (1992): "Ubiquitous Audio: Capturing Spontaneous Collaboration" in *Proc. ACM Conference on Computer-Supported Cooperative Work, CSCW'92*, Toronto, Canada, October-November, 1992, pp. 210-217.

Ladd, J. (1991): "Computers and Moral Responsibility: A Framework for Ethical Analysis" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 664-675.

style media space could seem very sinister indeed. It is thus quite understandable that many visitors to the lab experience some trepidation.

RAVE is a research tool and is also itself the object of research, like all of the ubiquitous computing systems at EuroPARC. It is not intended to be a model for a commercial, standard media space. Rather, it is an instance of a facility which has evolved inextricably with a culture of use and is only thus acceptable to members of that culture. The problems highlighted by our framework could, however, point to design refinements which might be essential in other contexts.

Another issue which the framework helps to elucidate, is the delicate balance that exists between awareness and privacy. Providing too much awareness of other people's activity and availability may be seen as intrusive. However, too little awareness may result in inadvertent invasions of privacy such as when people cannot tell how receptive another person is to being disturbed. The aim then is to provide awareness without crossing the line into intrusiveness.

A related issue is that data which could be feedback to one person may feature someone else's personal information which they might not want to make available. For example, our proposal to display large Portholes images of people currently connected to the Commons camera may make them feel as if they are on display. This suggests that designs which solve some privacy problems may cause others. Our framework must therefore be applied not only to the systems in place, but also to the privacy solutions themselves.

It is often the case that design decisions involve trade-offs and compromises. Designing to protect privacy is extreme in this respect. There is no guarantee that features put in place to protect privacy will confer the benefits that the designer intends. We therefore aim to prototype some the design refinements we have suggested and evaluate these in use at EuroPARC in the near future.

The framework described in this paper aims to provide a systematic basis for tackling a range of user-interface design problems. The problems we have been dealing with are those that interfere with interactions between people and the exchange of personal information and that are likely to arise with CSCW systems and, in particular, media space and other ubiquitous computing systems. Perhaps more important, we have made the case that *privacy is a user-interface design issue*, and one which we hope will become an increasingly integral part of the design process of information technology in general.

Acknowledgements

We wish to thank Mike Molloy and Paul Dourish for their support in implementing some of our design ideas. We also thank Bob Anderson, Sara Bly, Graham Button, Matthew Chalmers, Paul Dourish, Bill Gaver, Steve Harrison, Mik Lamming, Paul Luff, Wendy Mackay, Allan MacLean, Scott Minneman, William Newman and Peter Robinson for interesting discussions and helpful comments on drafts of this paper.

Anyone who objects to this can either avoid the label wearers or ask the researchers concerned to make sure that they are not recorded.

Use of the framework

In the example, our framework serves three important purposes.

- It helps to clarify the existing state of affairs with respect to privacy problems, and social norms and practices currently in place.
- By clarifying the problems, it helps to point to possible design solutions and explore a range of possibilities.
- It is used to assess the solutions in terms of how they might reduce the existing problems as well as how they might cause new ones.

With regard to this last issue, it is important to point out that, while the framework and design criteria help us evaluate proposed solutions prospectively, it is only by implementing these solutions that we can truly judge their usefulness. A case in point is the software infrastructure, Godard, whose privacy feature allows users to select who is allowed to connect to them. Consistent with the criterion of being fail-safe, the default is that lab newcomers are automatically denied access until each person in the lab explicitly allows them access. Unfortunately, because lab members generally forget to change their settings, newcomers find that they are unable to connect to anyone. As a result, they have been known to give up trying and thus never get in the habit of using RAVE. There are simple solutions to this problem, like automatically notifying people to whom an unsuccessful attempt to connect has been made. However, many problems are not foreseen and thus evaluation through use must always be part of the design cycle.

In addition, the framework itself needs to be evaluated and refined. To do this we will be applying it to a range of existing ubiquitous computing technology at EuroPARC. In doing so we hope to identify how it needs to be enhanced or extended.

Discussion and conclusions

In this paper we have focused on technical, rather than social or policy solutions for protecting privacy in ubiquitous computing environments. We have argued that this is an important design focus, and offered a framework as guidance. That being said, it is interesting that the framework has also highlighted ways in which cultural norms and practices affect and sometimes ameliorate privacy concerns.

In spite of shortcomings which our framework highlights, RAVE is, in general, very acceptable to lab members. In part, this is because feedback and control of information capture are well attended to overall in its design, enabling people to orient themselves appropriately to the technology. Further, lab members know roughly how it works, and trust the benign culture which governs its use. Visitors have no such knowledge or trust, and one can imagine that, other contexts, a RAVE

images of who is currently connected to the camera onto the wall. However, this would be *expensive*, and possibly *intrusive* to those who connect to a public area.

Audio feedback: In private offices audio feedback alerts occupants to onset and termination of short term glance connections. Such feedback about video connections to the Commons would be *inappropriately timed*, since they are normally of the long term background variety which outlast most visits to the room.

Q: What feedback is provided about the purposes of using information about me?

No Existing Solution

There is no technical feedback about the intentions of those who access the video signal. However, lab members are reasonably confident that their privacy is not threatened by others' uses of information, probably because, in a public area, they already behave in what they consider to be a publicly presentable and acceptable fashion.

Proposed Solution:

We cannot provide technological feedback about people's intentions. These may only be deduced from feedback about capture, access and utilisation of information, together with knowledge of the culture, context and individuals concerned.

Q: What control is there over when and when not to give out what information?

Existing Solutions:

Moving off camera: People can move on or off camera; there is a "video-free zone" in the commons for those who want to relax in private. This kind of solution is very *easy to learn*.

Covering the camera: If certain activities, such as the potentially embarrassing "weekly step-aerobics work-out," are taking place in the commons, the camera lens is covered. This is an extremely *trustworthy* solution.

Behaving appropriately: If people have to walk in front of the camera, they can orient themselves appropriately to it given the *meaningful* feedback they obtain from the confidence monitor (for example, they will probably not get too close or stare into it for fear of appearing foolish).

Control over what happens to information, who can access it and for what purposes it is used?

We do not propose to give individuals any additional technical control over the capture, construction and access of the Commons video signal because it is a *public* rather than a private information source. Technical control over purposes for which information can be used, however, is impractical with any information source, whether public or private. At EuroPARC, social control is effectively exercised. The culture of acceptable use which has evolved with RAVE dictates that certain practices are frowned upon.

Lab members are always expected to warn others that constructions and access other the normal background connection, glance and Portholes services, are occurring. For example, Vepys video diary experiments, in which subjects have their picture taken wherever they go, are announced to all lab members and the subjects wear labels to warn of potential recording of camera images in areas they enter.

however it is less *meaningful* because it doesn't tell you whether the camera is on, or if you are in its view.

Alternative Solution:

Movement Sensors: A solution which might supplement the use of confidence monitors would be to try using infra-red devices to alert people, either with an audio or visual signal, when they move into the field of view of a camera. These would provide *appropriately timed* feedback about onset of capture of video information, however they would not be *meaningful* without some other form of feedback.

Q: What feedback is there about what happens to information about me inside the system?

No Existing Solution:

The confidence monitor does not inform visitors and newcomers to the lab that the video signal is sent to a switch. This can potentially direct the signal to any number of nodes, recording devices or ubiquitous computing services in the lab. Unfortunately Toby cannot tell you whether recording or some other construction of video data is taking place. In fact the EuroPARC policy is that recording never takes place without warnings to lab members.

Proposed Solutions:

LED display: A simple design solution would be to have an LED status display by the camera, connected to the media space switch and other devices responsible for collecting, recording and distributing the video signal. This is a *low cost* proposal to give *appropriately timed* feedback about when and which services are actively collecting information. Unfortunately it might not be sufficiently *perceptible*.

Audio and video feedback: We could provide audio feedback to indicate connections and image framegrabbing but it could be *obtrusive* and *annoying* to provide repeated audio feedback to a public area at a sufficient volume to be heard all round the room. An alternative would be to superimpose the flashing word "Recording" on the screen of the confidence monitor. This would have to be refined to find a solution which draws attention whilst being *unobtrusive*.

Q: What feedback is given about who has access to information about me and what information they see?

Existing Solutions:

Textual information: In order to warn people that they might be "watched", Toby wears a sweatshirt with the message "I may be a dummy but I'm watching you!" printed on it. Together with the fact that Toby is holding a camera, the *meaning* of this is fairly clear in a general sense, but not specific enough about who is doing the watching and when.

Proposed Solutions:

Viewer display: One option is to display a list of names or pictures on the wall to indicate who can watch a public area. If we want to update the information we could adapt Portholes, an "awareness sever" which distributes images to EuroPARC and PARC media space users (Dourish & Bly, 1992). In order to be *perceptible* to passers by, the display would have to be larger than a normal monitor. We could project

Meaningfulness: Feedback and control must incorporate meaningful representations of information captured and meaningful actions to control it, not just raw data and unfamiliar actions. They should be sensitive to the context of data capture and also to the contexts in which information is presented and control exercised.

Learnability: Proposed designs should not require a complex model of how the system works. They should exploit or be sensitive to natural, existing psychological and social mechanisms that allow people to perceive and control how they present themselves and their availability for potential interactions.

Low cost: Naturally, we wish to keep costs of design solutions down.

The first seven criteria are especially relevant to protection of privacy. The final four are more general design concerns. Some of these criteria have to be traded off against one another in the search for design solutions.

Applying the framework: Feedback and control for video data from a public area

We have begun to apply our framework to RAVE to reveal aspects of its design which can be refined. For the sake of brevity, we focus on just one aspect of this media space which involves a video connection from the Commons, a public reading and meeting area at EuroPARC.

In RAVE, people can access the camera in the Commons either in the form of short glance or indefinite, background, video-only connections. The video data can sent to devices such as a framegrabber which takes digitised video snaps. These can be used by various services such as Vepys, a video diary which takes still images of people via media space cameras, every so often, wherever they are, and stores the series of images as a browsable record of their day-to-day activity (Eldridge, 1992).

Providing feedback and control mechanisms over video data taken from this public area is a challenging problem but it is an important one, since the Commons is an area where many visitors to EuroPARC spend their time.

Our framework prompts us to ask the following questions for which we describe existing or potential design solutions (relevant criteria appear in italics):

Q: What feedback is there about when and what information about me gets into the system?

Existing Solutions:

Confidence monitor: A monitor is positioned next to the camera to inform passers by when they are within range, and what they look like. This solution fulfils the design criteria of being *trustworthy, meaningful* and *appropriately timed*.

Mannequin (the Toby): In order to alert people to the presence of the camera, a mannequin affectionately named Toby is positioned holding the camera. Toby draws people's attention because he looks like another person in the room. Originally the camera was in his head, but this concealed it and some visitors thought it was deliberately being hidden. Now Toby holds the camera on his shoulder. This feedback is *less obtrusive* than the confidence monitor (which can be distracting),

questions, are explicitly represented together with proposed solutions and their assessments (for more details see MacLean et al., 1991; Bellotti, 1993).

The issues in the cells within the framework are not necessarily independent of one another. For instance, in order to be fully informed about the purpose of information usage, one must know something about each of the other behaviours. Likewise, in order to appreciate access, one must know about capture and construction. Understanding construction requires knowing something about capture. Hence there is a dependency relationship for design of feedback between these behaviours. Control over each of them may, however, be relatively independently designed.

For those concerned about privacy, and the potential for subversion in particular, control over, and thus feedback about, capture is clearly the most important. Given appropriate feedback about what is being captured, users can orient themselves appropriately to the technology for collaboration or communication purposes and exercise appropriate control over their behaviour or what is captured in the knowledge of possible construction, access and purposes of information use.

Evaluating solutions

Our framework emphasises design to a set of criteria, which may be extended through experience and evaluation. Whilst questions about what feedback and control to provide set the design agenda, criteria represent additional and sometimes competing concerns which help us to assess and distinguish potential design solutions. The set of criteria acts as a checklist helping to encourage systematic evaluation of solutions. They have been identified from our experiences with the design and use of a range of ubiquitous computing services. Particularly important in our current set are the following eleven criteria.

Trustworthiness: Systems must be technically reliable and instill confidence in users. In order to satisfy this criterion, they must be understandable by their users. The consequences of actions must be confined to situations which can be apprehended in the context in which they take place and thus appropriately controlled.

Appropriate timing: Feedback should be provided at a time when control is most likely to be required and effective.

Perceptibility: Feedback should be noticeable.

Unobtrusiveness: Feedback should not distract or annoy. It should also be selective and relevant and should not overload the recipient with information.

Minimal intrusiveness: Feedback should not involve information which compromises the privacy of others.

Fail-safety: In cases where users omit to take explicit action to protect their privacy, the system should minimise information capture, construction and access.

Flexibility: What counts as private varies according to context and interpersonal relationships. Thus mechanisms of control over user and system behaviours may need to be tailorable to some extent by the individuals concerned.

Low effort: Design solutions must be lightweight to use, requiring as few actions and as little effort on the part of the user as possible.

	Feedback About	Control Over
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Figure 1. A framework for designing for feedback and control in ubiquitous computing environments: Each cell contains a description of the ideal state of affairs with respect to feedback or control of each of four types of behaviour.

Accessibility: Is information public, available to particular groups, certain persons only, or just to oneself? What applications, processes, and so on utilise personal data.

Purpose: To what uses is information put? How might it be used in the future? The intentions of those who wish to use data may not be made explicit. It may only be possible to infer what these are from knowledge of the person, the context, patterns of access and construction.

We now consider each of these four classes of concerns in relation to the following two questions:

What is the appropriate feedback?

What is the appropriate control?

We thus have eight design questions which form the basis for a design framework (Figure 1) with which we can analyse existing designs and explore new ones, with respect to a range of privacy issues. This framework is a domain specific example of the QOC approach to design rationale in which design issues, couched as

It must be pointed out that the technology itself is not inherently problematic. Resources used in face-to-face situations can be exploited, simulated, or substituted through design. For example media space systems can embody the principle “If I see your face, you see mine,” which is natural in face-to-face situations (e.g., VideoTunnels; Buxton & Moran, 1989) or they can supply means to convey availability (e.g., Louie et al., 1992). Dissociation problems in CSCW systems have been reduced by means of conveying gestures, or even body posture (e.g. Minneman & Bly, 1991; Tang & Minneman, 1991).

Our ongoing research assumes that problems of interaction, communication and privacy in ubiquitous computing systems, can be reduced through technological design refinements and innovations. Disembodiment and dissociation may be reduced through the provision of enriched feedback about the state of the technology and information being projected about users. Users must also have practical mechanisms of control over that personal information. We now present a framework for systematically addressing these issues. Although it may have general use for designing CSCW technology to support social interaction and communication, we focus in particular on how it helps us confront privacy as a central design concern.

A design framework

Based on our experience with privacy issues in RAVE and other similar systems, we have developed a simple design framework aimed at counteracting the kinds of problems we have outlined.

Addressing the problems

Much of the mutual awareness, which we normally take for granted may be reduced or lost in mediated interpersonal interactions. We may no longer know what information we are conveying, what it looks like and how permanent it is, who it is conveyed to, or what the intentions of those using that information might be. In order to counteract problems associated with this loss, our framework proposes that systems must be explicitly designed to provide feedback and control for at least the following potential user and system behaviours:

Capture: What kind of information is being picked up? Candidates include voices, actual speech, moving video or framegrabbed images (close up or not), personal identity, work activity and its products such as keypresses, applications used, files accessed, messages and documents.

Construction: What happens to information? Is it encrypted or processed at some point or combined with other information and, if so, how? Is it stored? In what form? Privacy concerns in ubiquitous computing environments are exacerbated by the fact that potential records of our activity may be kept and possibly manipulated, and used at a later date and out of their original context. This leads to numerous potential ethical problems (Mackay, 1991).

In CSCW and ubiquitous computing environments disembodiment means that these resources may be attenuated. So you may not be able to present yourself as effectively to others as you can in a face-to-face setting. For example, in an AV connection, you may only be a face on a monitor (Gaver, 1992) with your voice coming out of a loudspeaker, the volume of which you may not be aware or able to control. You may only appear as a name (McCarthy et al., 1991) or a name associated with a room displayed on a screen (e.g., Harper et al., 1992). At worst (e.g., in a RAVE background connection) you may have no perceptible presence at all. On the other hand, disembodiment also means that you may be unaware of when you are convey information to others because of a lack of feedback from the technology.

Dissociation occurs in CSCW applications when only the results of actions are shared, but the actions themselves are invisible. In other words when you cannot easily determine who is doing, or did, what (e.g., ShrEdit, a shared editor with no telepointers; McGuffin & Olson, 1992).

Gaining information: In face-to-face situations, cues given by others influence your judgements about whether to attempt conversation, what to say and how to act.

In media spaces, there is usually no way to gauge how available someone else is before connecting to them (Louie et al., in press). Once connected, awareness of the person at the other end of the link or their actions is likely to be limited to the fixed and narrow field of view of a camera, and whatever a microphone picks up (Gaver, 1992). That person also has a reduced, disembodied presence. In turn, you are likely to receive fewer cues when someone is observing you, or your work.

Breakdown of social and behavioural norms and practices

The effects of disembodiment and dissociation manifest themselves in a variety of breakdowns in behavioural and social norms and practices. For example, breakdowns associated with disembodiment include a tendency for users to engage in unintentional, prolonged observation of others over AV links (Heath & Luff, 1991). Users may intrude when they make AV connections, because they cannot discern how available others are (Louie et al., in press). Furthermore, the intuitive principle that if I can't see you then you can't see me, does not necessarily apply to computer mediated situations where one person may be able to observe others' activities without themselves being observed.

A major problem related to dissociation is one's inability to respond effectively to a perceived action because one does not know who is responsible for it. A familiar example of this problem exists with telephones where it is impossible to identify nuisance callers before picking up the receiver.

Problems of disembodiment and dissociation receive far less attention in the literature than insidious exploitation of technology. This is unfortunate as they are also problems for social interaction and communication mediated by technology and likely to be much more pervasive, particularly because they often relate to purely unintentional invasions of privacy. Furthermore, by addressing these problems through careful design, we may reduce the potential impact of system abuse.

glances, audio feedback (Gaver, 1991) alerts users to onset and termination of a connection and can even announce who is making it. For the two-way office connections, reciprocity acts as a form of feedback about the connection (if I see you, you see me) and, in the case of an attempted v-phone connection, an audio “ringing” signal is given and the caller’s name is displayed on the workstation, whereupon the recipient can decide whether to accept or reject the connection. Office-shares, being very long term, do not require such a protocol.

Public areas have cameras which can be accessed by a glance or a “background” connection which is indefinite, one-way and video-only. We provide feedback about the presence of a camera in a public place in the form of a video monitor beside the camera which displays its view.

Control and feedback also figure strongly in the design of RAVE’s architecture. Connection capability lists and an access control model define who can connect to whom and provide long term, static control over accessibility. Providing distinct connection types can also allow users to exercise discriminating dynamic control over their accessibility as in the v-phone call (for a fuller description of these features see Dourish, 1993). Our concern, however, is with the moment-to-moment continuous control that people exercise over how they present themselves in public as respectable, social beings (Goffman, 1963). In the next section we indicate why people, especially newcomers and visitors to places with media spaces and other kinds of ubiquitous computing technology, can feel uneasy about their ability to monitor and control their self presentation and consequently their privacy.

Disembodiment and dissociation

A number of problems with RAVE relate to the extended duration of v-phone calls and office-shares. Users tend to forget about their existence and associated implications. Even seasoned users can get confused about the nature of their connections. For example, if a colleague with whom you have an office-share switches off their camera or moves out of shot, it is easy to forget that they can still see you.

Problems in public areas include the fact that monitors next to cameras only suggest (and then only to those familiar with a media space) that a video image may be being broadcast to many people, via background connections. They cannot inform people when or to whom the image is being sent. For most EuroPARC “regulars” this is not a major concern, but for newcomers to the building, it may be.

The underlying causes of such problems lie in the fact that the technology results in *disembodiment* from the context into and from which one projects information (Heath & Luff, 1991) and *dissociation* from one’s actions. These phenomena interfere with conveying information about oneself or gaining information about others.

Conveying information: In the presence of others you convey information in many ways. These include position, posture, facial expression, speech, voice level and intonation, and direction of gaze. Such cues influence the behaviour of others. For example, they can determine whether or not others will try to initiate communication with you.

ing without leaving one's office. Various kinds of flexible video-only and AV connections between nodes are set up and broken by central switching devices which are controlled from individual workstations.

Whilst media space technology improves the accessibility of people to one another, some may feel that their privacy is compromised. The very ubiquity of such systems means that many of the concerns with existing workstation-based information systems are aggravated. A much wider variety of information can now be captured. People are much less likely to be "off-line" (inaccessible) at any given moment. Further, the design of many of these systems is such that it may not be clear when one is off- or on-line and open to scrutiny (Mantei et al., 1991; Gaver, 1992). People also express concern about their own intrusiveness to others when they try to make contact without being able to determine others' availability (Cool et al., 1992). Concerns about such problems have strongly influenced the installation and ongoing design of RAVE, as well as the way in which people use it.

Feedback and control in RAVE

At EuroPARC people generally do not worry much about privacy. They feel that the benefits of RAVE outweigh their concerns. This is because the design has evolved together with a culture of trust and acceptable practices relating to its use. Individual freedom was fostered to use, customise, or ignore the technology. Design was informed by studies of how collaborative work is socially organised and how such technology impacts it (e.g. Heath & Luff, 1991; 1992). Users' views and reactions were obtained via questionnaires and interviews. The varied individual feelings about privacy were accommodated by ensuring that users could decide how accessible they were to others via the media space (Dourish, 1991; Gaver et al., 1992; Dourish, 1993).

In designing for privacy in RAVE, two important principles have emerged (Gaver et al, 1992). These are *control* and *feedback*, which we define as follows:

Control: Empowering people to stipulate what information they project and who can get hold of it.

Feedback: Informing people when and what information about them is being captured and to whom the information is being made available.

RAVE users can control who may connect to them and what kind of connections each person is allowed make. If they omit to do so, automatic defaults are set to reject connections. User control via the workstation is supported by "Godard", the software infrastructure which provides the primary interface to the complex AV signal-switching and feedback mechanisms (Dourish,1991). These mechanisms comprise the kinds of connections which can be made between people, to different public areas, and to media services (e.g., video-players).

Feedback depends on the type of RAVE connection being made. Three kinds of interpersonal connection are "glance", "v-phone call" and "office-share". Glance connections are one-way, video-only connections of a few seconds' duration. V-phone and office-share connections are longer two-way AV connections. For

with one such environment. However, our framework may also be related to the design of CSCW systems and distributed computing environments in general.

In the following sections we first introduce the context and nature of the technology which is the focus of our interest, we then go on to outline our design framework and provide a brief example of its application.

Maintaining privacy in a media space

The need to understand and protect personal privacy in sophisticated information systems is becoming critical as computing power moves out of the box-on-the-desk into the world at large. We are entering the age of *ubiquitous computing* (e.g., Weiser, 1991; Lamming & Newman, 1991; Hindus & Schmandt, 1992) in which our environment comes to contain computing technology in a variety of forms.

Increasingly, we are seeing such systems incorporate sensors such as microphones, cameras and signal receivers for wireless communication. These sensors have the potential to transmit information such as speech, video images, or signals from portable computing devices, active badges (Want et al., 1992), electronic whiteboards (Pederson et al., 1993), and so on. These devices can be networked so that multimedia information can be stored, accessed, processed and distributed in a variety of ways. Services include audio-video (AV) interconnections, information retrieval, diary systems, document tracking and so on (e.g., Lamming & Newman, 1991; Gaver, 1992; Eldridge et al., 1992).

Ubiquitous computing usually implies embedding the technology unobtrusively within all manner of everyday objects which can potentially transmit and receive information from any other object. The aims are not only to reduce its visibility, but also to empower its users with more flexible and portable applications to support the capture, communication, recall, organisation and reuse of diverse information. The irony is that its unobtrusiveness both belies and contributes to its potential for supporting potentially invasive applications.

In light of these developments, it is dangerously complacent to assume that social and organisational controls over accessibility of personal information are sufficient, or that intrusions into privacy will ultimately become acceptable when traded against potential benefits. Such a position could leave individual users with a heavy burden of responsibility to ensure that they do not, even inadvertently, intrude on others. It also leaves them with limited control over their own privacy.

"Media spaces" (Stults, 1988) are a recent development in ubiquitous computing technology, involving audio, video and computer networking. They are the focus of an increasing amount of research and industrial interest into support for distributed collaborative work (e.g., Root, 1988; Mantei et al., 1991; Gaver et al., 1992; Fish et al., 1992). EuroPARC's RAVE environment is just one of several media spaces which have been set up in various research laboratories around the world.

In RAVE, cameras, monitors, microphones and speakers are placed in every office, to provide everyone with their own personal RAVE *node*. This allows one to communicate and work with others and to be aware of what is going on in the build-

Deliberate or poorly considered design resulting in invasive applications and sophisticated subversion of supposedly secure systems are discouraged by cultural censure and law (although these forces trail behind the advances in sophistication of the technology). However, software must still be secure in order to reduce the risks of covert abuse of personal data and this is an important area of research. There are already a number of useful software protection models and standards which are designed to reduce the risks (see e.g., Lampson et al., 1981; and Mullender, 1989).

The second class of problem is related to very different concerns about a fast growing, less well understood set of issues. These arise from user-interface design features which interfere with social behaviour. These features may foster unethical use of the technology but, more significantly, they are also much more conducive to inadvertent intrusions on privacy (Heath & Luff, 1991).

Mediated interactions between people via technology are prone to breakdowns due to inadequate feedback about what information one is broadcasting and an inability to control one's accessibility to others. This disrupts the social norms and practices governing communication and acceptable behaviour. Our concern in this paper is tackle the latter kind of problem in the context of systems design.

In attempting to design systems which reduce perceived invasions of privacy, it would be useful to have a practical working definition of the concept. Unfortunately, although privacy is widely considered to be an important right, it is difficult to define this notion in more than an intuitive fashion (Anderson, 1991). Attitudes to what is and what is not private data vary between people in different contexts and roles (Harper et al., 1992). Codes of practice and the law offer inadequate guidance on what actually counts as violation of privacy in technologically sophisticated environments (Clarke, 1988) and it may take lengthy court proceedings to determine what the case may be (Privacy Protection Study Commission, 1991).

Any realistic definition of privacy cannot be static. With the introduction of new technology, patterns of use and social norms develop around it and what is deemed "acceptable" behaviour is subject to change. Naturally evolving social practices may interact with organisational policies for correct usage (Harper et al., 1992). In addition, people are more prepared to accept potentially invasive technology if they consider that its benefits outweigh potential risks (e.g., Ladd, 1991; Richards, 1991). In recognition of these facts we take privacy to be a personal notion shaped by culturally determined expectations and perceptions about one's environment.

The social practices and policies that determine any *rights* an individual has to privacy interact with the technical and interface design aspects of the technology they use. Technology is not neutral when it comes to privacy. It can increase or reduce the extent to which people have control over personal data. Our concern is to ensure that privacy should be a central design issue in its own right.

We present a framework for addressing the design of *control* and *feedback* of information captured by multimedia, ubiquitous computing environments. These two issues are fundamental to successful communication and collaboration amongst users as well as to maintaining privacy. We ground our examples largely in the domain of networked audio-video environments and in particular in experiences

Design for Privacy in Ubiquitous Computing Environments

Victoria Bellotti* and Abigail Sellen*†
* Rank Xerox EuroPARC, Cambridge, UK
bellotti@europarc.xerox.com; sellen@europarc.xerox.com

†MRC Applied Psychology Unit, Cambridge, UK

Abstract: Current developments in information technology are leading to increasing capture and storage of information about people and their activities. This raises serious issues about the preservation of privacy. In this paper we examine why these issues are particularly important in the introduction of ubiquitous computing technology into the working environment. Certain problems with privacy are closely related to the ways in which the technology attenuates natural mechanisms of feedback and control over information released. We describe a framework for design for privacy in ubiquitous computing environments and conclude with an example of its application.

Introduction

Information technology can store, transmit and manipulate vast quantities and varieties of information. Whilst this is critical to government, public services, business and many individuals, it may also facilitate unobtrusive access, manipulation and presentation of personal data (Parker et al., 1990; Dunlop & Kling, 1991).

The term "Big Brother" in the context of computing technology, seems to imply two classes of problem. The first is due to the fact that computer technology may be put to insidious or unethical uses (e.g., Clarke, 1988). All information systems, and particularly distributed systems, are potentially vulnerable to covert subversion (Lampson et al., 1981) and, although it can be made extremely difficult to tamper with data in computing systems, protection mechanisms "are often only secure *in principle*. They are seldom secure *in practice*." (Mullender, 1989).

Lamming, M. and Newman W. (1991): "Activity-Based Information Retrieval Technology in Support of Personal Memory", EuroPARC Technical Report, EPC-91-103.1, 1991.

Lampson, B., Paul, M. and Siegert, H. (1981): *Distributed Systems - Architecture and Implementation*. Springer Verlag, 1981.

Louie, G., Mantei, M. and Sellen, A. (in press) "Making Contact in a Multi-Media Environment", to appear in *Behaviour and Interaction Technology*.

Mackay, W. (1991): "Ethical Issues in the Use of Video: Is it Time to Establish Guidelines?" SIGCHI Discussion Forum in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 403-405.

MacLean, A., Young, R., Bellotti, V. and Moran, T. (1991): "Questions, Options, and Criteria: Elements of a Design Rationale for user interfaces", *Human Computer Interaction*, vol 6 (3&4), pp. 201-250.

Mantei, M., Becker, R., Sellen. A., Buxton, W., Milligan, T. and Wellman, B. (1991): "Experiences in the Use of a Media Space" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 203-208.

McCarthy, J., Miles, V. and Monk, A. (1991): "An Experimental Study of Common Ground in Text-Based Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 209-215.

McGuffin, L. and Olson, G. (1992): "ShrEdit: A Shared Electronic Workspace", CSMIL Technical Report, Cognitive Science and Machine Intelligence Laboratory, University of Michigan, 1992.

Minneman, S. and Bly, S. (1991): "Managing à Trois: A Study of a Multi-User Drawing Tool in Distributed Design Work", in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April- May 1991, pp. 217-224.

Mullender, S. (1989) "Protection", in S. Mullender (ed.) *Distributed Systems*. Addison Wesley, 1989.

Parker, D., Swope, S. and Baker, B. (1990): *Ethical Conflicts in Information and Computer Science, Technology, and Business*, QED, Information Sciences Inc. Wellesley, MA, 1990.

Pedersen, E., McCall, K., Moran, T. and Halasz, F. (1993): "Tivoli: An Electronic Whiteboard for Informal Workgroup Meetings", in *Proc. INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Privacy Protection Study Commission (1991): "Excerpts from Personal Privacy in an Information Society" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 453-468.

Richards, E. (1991): "Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy", in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 436-438.

Root, R. (1988) "Design of a Multi-Media Vehicle for Social Browsing" in *Proc. ACM Conference on Computer Supported Cooperative Work, CSCW'88*, Portland Oregon, September 26-29, 1988, pp. 25-38.

Stults, R. (1988): "The Experimental Use of Video to Support Design Activities", Xerox PARC Technical Report SSL-89-19, Palo Alto, California, 1988.

Tang, J. and Minneman, S. (1991): "VideoWhiteboard: Video Shadows to Support Remote Collaboration" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 315-322.

Want, R., Hopper, A., Falcco, V. and Gibbons, J.(1992): "The Active Badge Location System", *ACM Transactions on Office Information Systems*, January, 1992, 10(1), pp. 91-102.

Weiser, M. (1991): "The Computer for the 21st Century", *Scientific American*, September, 1991, pp. 94-104.

References

Anderson, R. (1991): *The Ethics of Research into Invasive Technologies*. Technical Report, EPC-91-107, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Bellotti, V. (1993): "Integrating Theoreticians' and Practitioners' Perspectives with Design Rationale" in *Proceedings of INTERCHI'93, Conference on Human Factors in Computing Systems*, Amsterdam, The Netherlands, April, 1993.

Buxton, W. and Moran, T. (1990): "EuroPARC's Integrated Interactive Intermedia Facility (IIIF): Early Experiences". *IFIP Conference on Multi-User Interfaces and Applications*, Herakleion, Crete, September 1990.

Clarke, R. (1988): "Information Technology and Dataveillance", *Communications of the ACM*, 31, 5, 1988, pp. 498-512.

Cool, C., Fish, R., Kraut, R. and Lowery, C. (1992): "Iterative Design of Video Communication Systems" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 25-32.

Dourish, P. (1991): "Godard: A Flexible Architecture for A/V Services in a Media Space" Technical Report EPC-91-134, Rank Xerox EuroPARC, Cambridge, UK, 1991.

Dourish, P. and Bly, S. (1992): "Portholes: Supporting Awareness in Distributed Work Groups" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'92*, Monterey, California, May 1992. pp. 541-547.

Dourish, P. (1993): "Culture and Control in a Media Space", in *Proc. European Conference on Computer-Supported Cooperative Work ECSCW'93*, Milano, Italy, September, 1993.

Dunlop, C. and Kling, R. (1991): *Computerization and Controversy: Value Conflicts and Social Choices*. Academic Press, Inc., 1991.

Eldridge, M., Lamming, M. and Flynn, M. (1992): "Does a Video Diary Help Recall?" in *People and Computers VII, Proceedings of the HCI'92 Conference*, York, UK, September, 1992, pp. 257-269.

Fish, R., Kraut, R. and Root, R. (1992): "Evaluating Video as a Technology for Informal Communication" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May, 1992, pp. 37-47.

Gaver, W. (1991): "Sound Support for Collaboration" in *Proc. European Conference on Computer-Supported Cooperative Work, ECSCW'91*, Amsterdam, The Netherlands, September, 1991, pp. 293-308.

Gaver, B., Moran, T., MacLean, A., Lövstrand, L., Dourish, P., Carter K. and Buxton, B. (1992): "Realising a Video Environment: EuroPARC's RAVE System" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI '92*, Monterey, California, May 1992, pp. 27-35.

Gaver, B. (1992): "The Affordance of Media Spaces for Collaboration" in *Proc. CSCW'92. ACM Conference on Computer-Supported Cooperative Work*, Toronto, Canada, October-November, 1992, pp. 17-24.

Goffman, E., *Behaviour in Public Places*. The Free Press, 1963.

Harper, R., Lamming, M. and Newman, W. (1992): "Locating Systems at Work: Implications for the Development of Active Badge Applications", *Interacting with Computers*, 4, 3, 1992, pp.343-363.

Heath, C. and Luff, P. (1991): "Disembodied Conduct: Communication through Video in a Multi-Media Office Environment" in *Proc. ACM Conference on Human Factors in Computing Systems, CHI'91*, New Orleans, Louisiana, April-May 1991, pp. 99-103.

Heath, C. and Luff, P. (1992): "Collaboration and Control: Crisis Management and Multimedia Technology in London Underground Line Control Rooms", *Computer Supported Cooperative Work (CSCW)*, 1, 1992, 69-94.

Hindus, D. and Schmandt, C. (1992): "Ubiquitous Audio: Capturing Spontaneous Collaboration" in *Proc. ACM Conference on Computer-Supported Cooperative Work, CSCW'92*, Toronto, Canada, October-November, 1992, pp. 210-217.

Ladd, J. (1991): "Computers and Moral Responsibility: A Framework for Ethical Analysis" in C. Dunlop & R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, Academic Press Inc., 1991, pp. 664-675.

style media space could seem very sinister indeed. It is thus quite understandable that many visitors to the lab experience some trepidation.

RAVE is a research tool and is also itself the object of research, like all of the ubiquitous computing systems at EuroPARC. It is not intended to be a model for a commercial, standard media space. Rather, it is an instance of a facility which has evolved inextricably with a culture of use and is only thus acceptable to members of that culture. The problems highlighted by our framework could, however, point to design refinements which might be essential in other contexts.

Another issue which the framework helps to elucidate, is the delicate balance that exists between awareness and privacy. Providing too much awareness of other people's activity and availability may be seen as intrusive. However, too little awareness may result in inadvertent invasions of privacy such as when people cannot tell how receptive another person is to being disturbed. The aim then is to provide awareness without crossing the line into intrusiveness.

A related issue is that data which could be feedback to one person may feature someone else's personal information which they might not want to make available. For example, our proposal to display large Portholes images of people currently connected to the Commons camera may make them feel as if they are on display. This suggests that designs which solve some privacy problems may cause others. Our framework must therefore be applied not only to the systems in place, but also to the privacy solutions themselves.

It is often the case that design decisions involve trade-offs and compromises. Designing to protect privacy is extreme in this respect. There is no guarantee that features put in place to protect privacy will confer the benefits that the designer intends. We therefore aim to prototype some the design refinements we have suggested and evaluate these in use at EuroPARC in the near future.

The framework described in this paper aims to provide a systematic basis for tackling a range of user-interface design problems. The problems we have been dealing with are those that interfere with interactions between people and the exchange of personal information and that are likely to arise with CSCW systems and, in particular, media space and other ubiquitous computing systems. Perhaps more important, we have made the case that *privacy is a user-interface design issue*, and one which we hope will become an increasingly integral part of the design process of information technology in general.

Acknowledgements

We wish to thank Mike Molloy and Paul Dourish for their support in implementing some of our design ideas. We also thank Bob Anderson, Sara Bly, Graham Button, Matthew Chalmers, Paul Dourish, Bill Gaver, Steve Harrison, Mik Lamming, Paul Luff, Wendy Mackay, Allan MacLean, Scott Minneman, William Newman and Peter Robinson for interesting discussions and helpful comments on drafts of this paper.

Anyone who objects to this can either avoid the label wearers or ask the researchers concerned to make sure that they are not recorded.

Use of the framework

In the example, our framework serves three important purposes.

- It helps to clarify the existing state of affairs with respect to privacy problems, and social norms and practices currently in place.
- By clarifying the problems, it helps to point to possible design solutions and explore a range of possibilities.
- It is used to assess the solutions in terms of how they might reduce the existing problems as well as how they might cause new ones.

With regard to this last issue, it is important to point out that, while the framework and design criteria help us evaluate proposed solutions prospectively, it is only by implementing these solutions that we can truly judge their usefulness. A case in point is the software infrastructure, Godard, whose privacy feature allows users to select who is allowed to connect to them. Consistent with the criterion of being failsafe, the default is that lab newcomers are automatically denied access until each person in the lab explicitly allows them access. Unfortunately, because lab members generally forget to change their settings, newcomers find that they are unable to connect to anyone. As a result, they have been known to give up trying and thus never get in the habit of using RAVE. There are simple solutions to this problem, like automatically notifying people to whom an unsuccessful attempt to connect has been made. However, many problems are not foreseen and thus evaluation through use must always be part of the design cycle.

In addition, the framework itself needs to be evaluated and refined. To do this we will be applying it to a range of existing ubiquitous computing technology at EuroPARC. In doing so we hope to identify how it needs to be enhanced or extended.

Discussion and conclusions

In this paper we have focused on technical, rather than social or policy solutions for protecting privacy in ubiquitous computing environments. We have argued that this is an important design focus, and offered a framework as guidance. That being said, it is interesting that the framework has also highlighted ways in which cultural norms and practices affect and sometimes ameliorate privacy concerns.

In spite of shortcomings which our framework highlights, RAVE is, in general, very acceptable to lab members. In part, this is because feedback and control of information capture are well attended to overall in its design, enabling people to orient themselves appropriately to the technology. Further, lab members know roughly how it works, and trust the benign culture which governs its use. Visitors have no such knowledge or trust, and one can imagine that, other contexts, a RAVE

images of who is currently connected to the camera onto the wall. However, this would be *expensive*, and possibly *intrusive* to those who connect to a public area.

Audio feedback: In private offices audio feedback alerts occupants to onset and termination of short term glance connections. Such feedback about video connections to the Commons would be *inappropriately timed*, since they are normally of the long term background variety which outlast most visits to the room.

Q: What feedback is provided about the purposes of using information about me?

No Existing Solution

There is no technical feedback about the intentions of those who access the video signal. However, lab members are reasonably confident that their privacy is not threatened by others' uses of information, probably because, in a public area, they already behave in what they consider to be a publicly presentable and acceptable fashion.

Proposed Solution:

We cannot provide technological feedback about people's intentions. These may only be deduced from feedback about capture, access and utilisation of information, together with knowledge of the culture, context and individuals concerned.

Q: What control is there over when and when not to give out what information?

Existing Solutions:

Moving off camera: People can move on or off camera; there is a "video-free zone" in the commons for those who want to relax in private. This kind of solution is very *easy to learn*.

Covering the camera: If certain activities, such as the potentially embarrassing "weekly step-aerobics work-out," are taking place in the commons, the camera lens is covered. This is an extremely *trustworthy* solution.

Behaving appropriately: If people have to walk in front of the camera, they can orient themselves appropriately to it given the *meaningful* feedback they obtain from the confidence monitor (for example, they will probably not get too close or stare into it for fear of appearing foolish).

Control over what happens to information, who can access it and for what purposes it is used?

We do not propose to give individuals any additional technical control over the capture, construction and access of the Commons video signal because it is a *public* rather than a private information source. Technical control over purposes for which information can be used, however, is impractical with any information source, whether public or private. At EuroPARC, social control is effectively exercised. The culture of acceptable use which has evolved with RAVE dictates that certain practices are frowned upon.

Lab members are always expected to warn others that constructions and access other the normal background connection, glance and Portholes services, are occurring. For example, Vepys video diary experiments, in which subjects have their picture taken wherever they go, are announced to all lab members and the subjects wear labels to warn of potential recording of camera images in areas they enter.

however it is less *meaningful* because it doesn't tell you whether the camera is on, or if you are in its view.

Alternative Solution:

Movement Sensors: A solution which might supplement the use of confidence monitors would be to try using infra-red devices to alert people, either with an audio or visual signal, when they move into the field of view of a camera. These would provide *appropriately timed* feedback about onset of capture of video information, however they would not be *meaningful* without some other form of feedback.

Q: What feedback is there about what happens to information about me inside the system?

No Existing Solution:

The confidence monitor does not inform visitors and newcomers to the lab that the video signal is sent to a switch. This can potentially direct the signal to any number of nodes, recording devices or ubiquitous computing services in the lab. Unfortunately Toby cannot tell you whether recording or some other construction of video data is taking place. In fact the EuroPARC policy is that recording never takes place without warnings to lab members.

Proposed Solutions:

LED display: A simple design solution would be to have an LED status display by the camera, connected to the media space switch and other devices responsible for collecting, recording and distributing the video signal. This is a *low cost* proposal to give *appropriately timed* feedback about when and which services are actively collecting information. Unfortunately it might not be sufficiently *perceptible*.

Audio and video feedback: We could provide audio feedback to indicate connections and image framegrabbing but it could be *obtrusive* and *annoying* to provide repeated audio feedback to a public area at a sufficient volume to be heard all round the room. An alternative would be to superimpose the flashing word "Recording" on the screen of the confidence monitor. This would have to be refined to find a solution which draws attention whilst being *unobtrusive*.

Q: What feedback is given about who has access to information about me and what information they see?

Existing Solutions:

Textual information: In order to warn people that they might be "watched", Toby wears a sweatshirt with the message "I may be a dummy but I'm watching you!" printed on it. Together with the fact that Toby is holding a camera, the *meaning* of this is fairly clear in a general sense, but not specific enough about who is doing the watching and when.

Proposed Solutions:

Viewer display: One option is to display a list of names or pictures on the wall to indicate who can watch a public area. If we want to update the information we could adapt Portholes, an "awareness sever" which distributes images to EuroPARC and PARC media space users (Dourish & Bly, 1992). In order to be *perceptible* to passers by, the display would have to be larger than a normal monitor. We could project

Meaningfulness: Feedback and control must incorporate meaningful representations of information captured and meaningful actions to control it, not just raw data and unfamiliar actions. They should be sensitive to the context of data capture and also to the contexts in which information is presented and control exercised.

Learnability: Proposed designs should not require a complex model of how the system works. They should exploit or be sensitive to natural, existing psychological and social mechanisms that allow people to perceive and control how they present themselves and their availability for potential interactions.

Low cost: Naturally, we wish to keep costs of design solutions down.

The first seven criteria are especially relevant to protection of privacy. The final four are more general design concerns. Some of these criteria have to be traded off against one another in the search for design solutions.

Applying the framework: Feedback and control for video data from a public area

We have begun to apply our framework to RAVE to reveal aspects of its design which can be refined. For the sake of brevity, we focus on just one aspect of this media space which involves a video connection from the Commons, a public reading and meeting area at EuroPARC.

In RAVE, people can access the camera in the Commons either in the form of short glance or indefinite, background, video-only connections. The video data can sent to devices such as a framegrabber which takes digitised video snaps. These can be used by various services such as Vepys, a video diary which takes still images of people via media space cameras, every so often, wherever they are, and stores the series of images as a browsable record of their day-to-day activity (Eldridge, 1992).

Providing feedback and control mechanisms over video data taken from this public area is a challenging problem but it is an important one, since the Commons is an area where many visitors to EuroPARC spend their time.

Our framework prompts us to ask the following questions for which we describe existing or potential design solutions (relevant criteria appear in italics):

Q: What feedback is there about when and what information about me gets into the system?

Existing Solutions:

Confidence monitor: A monitor is positioned next to the camera to inform passers by when they are within range, and what they look like. This solution fulfils the design criteria of being *trustworthy, meaningful* and *appropriately timed*.

Mannequin (the Toby): In order to alert people to the presence of the camera, a mannequin affectionately named Toby is positioned holding the camera. Toby draws people's attention because he looks like another person in the room. Originally the camera was in his head, but this concealed it and some visitors thought it was deliberately being hidden. Now Toby holds the camera on his shoulder. This feedback is *less obtrusive* than the confidence monitor (which can be distracting),

questions, are explicitly represented together with proposed solutions and their assessments (for more details see MacLean et al., 1991; Bellotti, 1993).

The issues in the cells within the framework are not necessarily independent of one another. For instance, in order to be fully informed about the purpose of information usage, one must know something about each of the other behaviours. Likewise, in order to appreciate access, one must know about capture and construction. Understanding construction requires knowing something about capture. Hence there is a dependency relationship for design of feedback between these behaviours. Control over each of them may, however, be relatively independently designed.

For those concerned about privacy, and the potential for subversion in particular, control over, and thus feedback about, capture is clearly the most important. Given appropriate feedback about what is being captured, users can orient themselves appropriately to the technology for collaboration or communication purposes and exercise appropriate control over their behaviour or what is captured in the knowledge of possible construction, access and purposes of information use.

Evaluating solutions

Our framework emphasises design to a set of criteria, which may be extended through experience and evaluation. Whilst questions about what feedback and control to provide set the design agenda, criteria represent additional and sometimes competing concerns which help us to assess and distinguish potential design solutions. The set of criteria acts as a checklist helping to encourage systematic evaluation of solutions. They have been identified from our experiences with the design and use of a range of ubiquitous computing services. Particularly important in our current set are the following eleven criteria.

Trustworthiness: Systems must be technically reliable and instill confidence in users. In order to satisfy this criterion, they must be understandable by their users. The consequences of actions must be confined to situations which can be apprehended in the context in which they take place and thus appropriately controlled.

Appropriate timing: Feedback should be provided at a time when control is most likely to be required and effective.

Perceptibility: Feedback should be noticeable.

Unobtrusiveness: Feedback should not distract or annoy. It should also be selective and relevant and should not overload the recipient with information.

Minimal intrusiveness: Feedback should not involve information which compromises the privacy of others.

Fail-safety: In cases where users omit to take explicit action to protect their privacy, the system should minimise information capture, construction and access.

Flexibility: What counts as private varies according to context and interpersonal relationships. Thus mechanisms of control over user and system behaviours may need to be tailorable to some extent by the individuals concerned.

Low effort: Design solutions must be lightweight to use, requiring as few actions and as little effort on the part of the user as possible.

	Feedback About	Control Over
Capture	When and what information about me gets into the system.	When and when not to give out what information. I can enforce my own preferences for system behaviours with respect to each type of information I convey.
Construction	What happens to information about me once it gets inside the system.	What happens to information about me. I can set automatic default behaviours and permissions.
Accessibility	Which people and what software (e.g., daemons or servers) have access to information about me and what information they see or use.	Who and what has access to what information about me. I can set automatic default behaviours and permissions.
Purposes	What people want information about me for. Since this is outside of the system, it may only be possible to infer purpose from construction and access behaviours.	It is infeasible for me to have technical control over purposes. With appropriate feedback, however, I can exercise social control to restrict intrusion, unethical, and illegal usage.

Figure 1. A framework for designing for feedback and control in ubiquitous computing environments: Each cell contains a description of the ideal state of affairs with respect to feedback or control of each of four types of behaviour.

Accessibility: Is information public, available to particular groups, certain persons only, or just to oneself? What applications, processes, and so on utilise personal data.

Purpose: To what uses is information put? How might it be used in the future? The intentions of those who wish to use data may not be made explicit. It may only be possible to infer what these are from knowledge of the person, the context, patterns of access and construction.

We now consider each of these four classes of concerns in relation to the following two questions:

What is the appropriate feedback?

What is the appropriate control?

We thus have eight design questions which form the basis for a design framework (Figure 1) with which we can analyse existing designs and explore new ones, with respect to a range of privacy issues. This framework is a domain specific example of the QOC approach to design rationale in which design issues, couched as

It must be pointed out that the technology itself is not inherently problematic. Resources used in face-to-face situations can be exploited, simulated, or substituted through design. For example media space systems can embody the principle "If I see your face, you see mine," which is natural in face-to-face situations (e.g., VideoTunnels; Buxton & Moran, 1989) or they can supply means to convey availability (e.g., Louie et al., 1992). Dissociation problems in CSCW systems have been reduced by means of conveying gestures, or even body posture (e.g. Minneman & Bly, 1991; Tang & Minneman, 1991).

Our ongoing research assumes that problems of interaction, communication and privacy in ubiquitous computing systems, can be reduced through technological design refinements and innovations. Disembodiment and dissociation may be reduced through the provision of enriched feedback about the state of the technology and information being projected about users. Users must also have practical mechanisms of control over that personal information. We now present a framework for systematically addressing these issues. Although it may have general use for designing CSCW technology to support social interaction and communication, we focus in particular on how it helps us confront privacy as a central design concern.

A design framework

Based on our experience with privacy issues in RAVE and other similar systems, we have developed a simple design framework aimed at counteracting the kinds of problems we have outlined.

Addressing the problems

Much of the mutual awareness, which we normally take for granted may be reduced or lost in mediated interpersonal interactions. We may no longer know what information we are conveying, what it looks like and how permanent it is, who it is conveyed to, or what the intentions of those using that information might be. In order to counteract problems associated with this loss, our framework proposes that systems must be explicitly designed to provide feedback and control for at least the following potential user and system behaviours:

Capture: What kind of information is being picked up? Candidates include voices, actual speech, moving video or framegrabbed images (close up or not), personal identity, work activity and its products such as keypresses, applications used, files accessed, messages and documents.

Construction: What happens to information? Is it encrypted or processed at some point or combined with other information and, if so, how? Is it stored? In what form? Privacy concerns in ubiquitous computing environments are exacerbated by the fact that potential records of our activity may be kept and possibly manipulated, and used at a later date and out of their original context. This leads to numerous potential ethical problems (Mackay, 1991).

In CSCW and ubiquitous computing environments disembodiment means that these resources may be attenuated. So you may not be able to present yourself as effectively to others as you can in a face-to-face setting. For example, in an AV connection, you may only be a face on a monitor (Gaver, 1992) with your voice coming out of a loudspeaker, the volume of which you may not be aware or able to control. You may only appear as a name (McCarthy et al., 1991) or a name associated with a room displayed on a screen (e.g., Harper et al., 1992). At worst (e.g., in a RAVE background connection) you may have no perceptible presence at all. On the other hand, disembodiment also means that you may be unaware of when you are convey information to others because of a lack of feedback from the technology.

Dissociation occurs in CSCW applications when only the results of actions are shared, but the actions themselves are invisible. In other words when you cannot easily determine who is doing, or did, what (e.g., ShrEdit, a shared editor with no telepointers; McGuffin & Olson, 1992).

Gaining information: In face-to-face situations, cues given by others influence your judgements about whether to attempt conversation, what to say and how to act.

In media spaces, there is usually no way to gauge how available someone else is before connecting to them (Louie et al., in press). Once connected, awareness of the person at the other end of the link or their actions is likely to be limited to the fixed and narrow field of view of a camera, and whatever a microphone picks up (Gaver, 1992). That person also has a reduced, disembodied presence. In turn, you are likely to receive fewer cues when someone is observing you, or your work.

Breakdown of social and behavioural norms and practices

The effects of disembodiment and dissociation manifest themselves in a variety of breakdowns in behavioural and social norms and practices. For example, breakdowns associated with disembodiment include a tendency for users to engage in unintentional, prolonged observation of others over AV links (Heath & Luff, 1991). Users may intrude when they make AV connections, because they cannot discern how available others are (Louie et al., in press). Furthermore, the intuitive principle that if I can't see you then you can't see me, does not necessarily apply to computer mediated situations where one person may be able to observe others' activities without themselves being observed.

A major problem related to dissociation is one's inability to respond effectively to a perceived action because one does not know who is responsible for it. A familiar example of this problem exists with telephones where it is impossible to identify nuisance callers before picking up the receiver.

Problems of disembodiment and dissociation receive far less attention in the literature than insidious exploitation of technology. This is unfortunate as they are also problems for social interaction and communication mediated by technology and likely to be much more pervasive, particularly because they often relate to purely unintentional invasions of privacy. Furthermore, by addressing these problems through careful design, we may reduce the potential impact of system abuse.

glances, audio feedback (Gaver, 1991) alerts users to onset and termination of a connection and can even announce who is making it. For the two-way office connections, reciprocity acts as a form of feedback about the connection (if I see you, you see me) and, in the case of an attempted v-phone connection, an audio "ringing" signal is given and the caller's name is displayed on the workstation, whereupon the recipient can decide whether to accept or reject the connection. Office-shares, being very long term, do not require such a protocol.

Public areas have cameras which can be accessed by a glance or a "background" connection which is indefinite, one-way and video-only. We provide feedback about the presence of a camera in a public place in the form of a video monitor beside the camera which displays its view.

Control and feedback also figure strongly in the design of RAVE's architecture. Connection capability lists and an access control model define who can connect to whom and provide long term, static control over accessibility. Providing distinct connection types can also allow users to exercise discriminating dynamic control over their accessibility as in the v-phone call (for a fuller description of these features see Dourish, 1993). Our concern, however, is with the moment-to-moment continuous control that people exercise over how they present themselves in public as respectable, social beings (Goffman, 1963). In the next section we indicate why people, especially newcomers and visitors to places with media spaces and other kinds of ubiquitous computing technology, can feel uneasy about their ability to monitor and control their self presentation and consequently their privacy.

Disembodiment and dissociation

A number of problems with RAVE relate to the extended duration of v-phone calls and office-shares. Users tend to forget about their existence and associated implications. Even seasoned users can get confused about the nature of their connections. For example, if a colleague with whom you have an office-share switches off their camera or moves out of shot, it is easy to forget that they can still see you.

Problems in public areas include the fact that monitors next to cameras only suggest (and then only to those familiar with a media space) that a video image may be being broadcast to many people, via background connections. They cannot inform people when or to whom the image is being sent. For most EuroPARC "regulars" this is not a major concern, but for newcomers to the building, it may be.

The underlying causes of such problems lie in the fact that the technology results in *disembodiment* from the context into and from which one projects information (Heath & Luff, 1991) and *dissociation* from one's actions. These phenomena interfere with conveying information about oneself or gaining information about others.

Conveying information: In the presence of others you convey information in many ways. These include position, posture, facial expression, speech, voice level and intonation, and direction of gaze. Such cues influence the behaviour of others. For example, they can determine whether or not others will try to initiate communication with you.

ing without leaving one's office. Various kinds of flexible video-only and AV connections between nodes are set up and broken by central switching devices which are controlled from individual workstations.

Whilst media space technology improves the accessibility of people to one another, some may feel that their privacy is compromised. The very ubiquity of such systems means that many of the concerns with existing workstation-based information systems are aggravated. A much wider variety of information can now be captured. People are much less likely to be "off-line" (inaccessible) at any given moment. Further, the design of many of these systems is such that it may not be clear when one is off- or on-line and open to scrutiny (Mantei et al., 1991; Gaver, 1992). People also express concern about their own intrusiveness to others when they try to make contact without being able to determine others' availability (Cool et al., 1992). Concerns about such problems have strongly influenced the installation and ongoing design of RAVE, as well as the way in which people use it.

Feedback and control in RAVE

At EuroPARC people generally do not worry much about privacy. They feel that the benefits of RAVE outweigh their concerns. This is because the design has evolved together with a culture of trust and acceptable practices relating to its use. Individual freedom was fostered to use, customise, or ignore the technology. Design was informed by studies of how collaborative work is socially organised and how such technology impacts it (e.g. Heath & Luff, 1991; 1992). Users' views and reactions were obtained via questionnaires and interviews. The varied individual feelings about privacy were accommodated by ensuring that users could decide how accessible they were to others via the media space (Dourish, 1991; Gaver et al., 1992; Dourish, 1993).

In designing for privacy in RAVE, two important principles have emerged (Gaver et al, 1992). These are *control* and *feedback*, which we define as follows:
Control: Empowering people to stipulate what information they project and who can get hold of it.
Feedback: Informing people when and what information about them is being captured and to whom the information is being made available.

RAVE users can control who may connect to them and what kind of connections each person is allowed make. If they omit to do so, automatic defaults are set to reject connections. User control via the workstation is supported by "Godard", the software infrastructure which provides the primary interface to the complex AV signal-switching and feedback mechanisms (Dourish,1991). These mechanisms comprise the kinds of connections which can be made between people, to different public areas, and to media services (e.g., video-players).

Feedback depends on the type of RAVE connection being made. Three kinds of interpersonal connection are "glance", "v-phone call" and "office-share". Glance connections are one-way, video-only connections of a few seconds' duration. V-phone and office-share connections are longer two-way AV connections. For

with one such environment. However, our framework may also be related to the design of CSCW systems and distributed computing environments in general.

In the following sections we first introduce the context and nature of the technology which is the focus of our interest, we then go on to outline our design framework and provide a brief example of its application.

Maintaining privacy in a media space

The need to understand and protect personal privacy in sophisticated information systems is becoming critical as computing power moves out of the box-on-the-desk into the world at large. We are entering the age of *ubiquitous computing* (e.g., Weiser, 1991; Lamming & Newman, 1991; Hindus & Schmandt, 1992) in which our environment comes to contain computing technology in a variety of forms.

Increasingly, we are seeing such systems incorporate sensors such as microphones, cameras and signal receivers for wireless communication. These sensors have the potential to transmit information such as speech, video images, or signals from portable computing devices, active badges (Want et al., 1992), electronic whiteboards (Pederson et al., 1993), and so on. These devices can be networked so that multimedia information can be stored, accessed, processed and distributed in a variety of ways. Services include audio-video (AV) interconnections, information retrieval, diary systems, document tracking and so on (e.g., Lamming & Newman, 1991; Gaver, 1992; Eldridge et al., 1992).

Ubiquitous computing usually implies embedding the technology unobtrusively within all manner of everyday objects which can potentially transmit and receive information from any other object. The aims are not only to reduce its visibility, but also to empower its users with more flexible and portable applications to support the capture, communication, recall, organisation and reuse of diverse information. The irony is that its unobtrusiveness both belies and contributes to its potential for supporting potentially invasive applications.

In light of these developments, it is dangerously complacent to assume that social and organisational controls over accessibility of personal information are sufficient, or that intrusions into privacy will ultimately become acceptable when traded against potential benefits. Such a position could leave individual users with a heavy burden of responsibility to ensure that they do not, even inadvertently, intrude on others. It also leaves them with limited control over their own privacy.

“Media spaces” (Stults, 1988) are a recent development in ubiquitous computing technology, involving audio, video and computer networking. They are the focus of an increasing amount of research and industrial interest into support for distributed collaborative work (e.g., Root, 1988; Mantei et al., 1991; Gaver et al., 1992; Fish et al., 1992). EuroPARC’s RAVE environment is just one of several media spaces which have been set up in various research laboratories around the world.

In RAVE, cameras, monitors, microphones and speakers are placed in every office, to provide everyone with their own personal RAVE *node*. This allows one to communicate and work with others and to be aware of what is going on in the build-

Deliberate or poorly considered design resulting in invasive applications and sophisticated subversion of supposedly secure systems are discouraged by cultural censure and law (although these forces trail behind the advances in sophistication of the technology). However, software must still be secure in order to reduce the risks of covert abuse of personal data and this is an important area of research. There are already a number of useful software protection models and standards which are designed to reduce the risks (see e.g., Lampson et al., 1981; and Mullender, 1989).

The second class of problem is related to very different concerns about a fast growing, less well understood set of issues. These arise from user-interface design features which interfere with social behaviour. These features may foster unethical use of the technology but, more significantly, they are also much more conducive to inadvertent intrusions on privacy (Heath & Luff, 1991).

Mediated interactions between people via technology are prone to breakdowns due to inadequate feedback about what information one is broadcasting and an inability to control one's accessibility to others. This disrupts the social norms and practices governing communication and acceptable behaviour. Our concern in this paper is tackle the latter kind of problem in the context of systems design.

In attempting to design systems which reduce perceived invasions of privacy, it would be useful to have a practical working definition of the concept. Unfortunately, although privacy is widely considered to be an important right, it is difficult to define this notion in more than an intuitive fashion (Anderson, 1991). Attitudes to what is and what is not private data vary between people in different contexts and roles (Harper et al., 1992). Codes of practice and the law offer inadequate guidance on what actually counts as violation of privacy in technologically sophisticated environments (Clarke, 1988) and it may take lengthy court proceedings to determine what the case may be (Privacy Protection Study Commission, 1991).

Any realistic definition of privacy cannot be static. With the introduction of new technology, patterns of use and social norms develop around it and what is deemed "acceptable" behaviour is subject to change. Naturally evolving social practices may interact with organisational policies for correct usage (Harper et al., 1992). In addition, people are more prepared to accept potentially invasive technology if they consider that its benefits outweigh potential risks (e.g., Ladd, 1991; Richards, 1991). In recognition of these facts we take privacy to be a personal notion shaped by culturally determined expectations and perceptions about one's environment.

The social practices and policies that determine any *rights* an individual has to privacy interact with the technical and interface design aspects of the technology they use. Technology is not neutral when it comes to privacy. It can increase or reduce the extent to which people have control over personal data. Our concern is to ensure that privacy should be a central design issue in its own right.

We present a framework for addressing the design of *control* and *feedback* of information captured by multimedia, ubiquitous computing environments. These two issues are fundamental to successful communication and collaboration amongst users as well as to maintaining privacy. We ground our examples largely in the domain of networked audio-video environments and in particular in experiences

Design for Privacy in Ubiquitous Computing Environments

Victoria Bellotti* and Abigail Sellen*†
* Rank Xerox EuroPARC, Cambridge, UK
bellotti@europarc.xerox.com; sellen@europarc.xerox.com

†MRC Applied Psychology Unit, Cambridge, UK

Abstract: Current developments in information technology are leading to increasing capture and storage of information about people and their activities. This raises serious issues about the preservation of privacy. In this paper we examine why these issues are particularly important in the introduction of ubiquitous computing technology into the working environment. Certain problems with privacy are closely related to the ways in which the technology attenuates natural mechanisms of feedback and control over information released. We describe a framework for design for privacy in ubiquitous computing environments and conclude with an example of its application.

Introduction

Information technology can store, transmit and manipulate vast quantities and varieties of information. Whilst this is critical to government, public services, business and many individuals, it may also facilitate unobtrusive access, manipulation and presentation of personal data (Parker et al., 1990; Dunlop & Kling, 1991).

The term "Big Brother" in the context of computing technology, seems to imply two classes of problem. The first is due to the fact that computer technology may be put to insidious or unethical uses (e.g., Clarke, 1988). All information systems, and particularly distributed systems, are potentially vulnerable to covert subversion (Lampson et al., 1981) and, although it can be made extremely difficult to tamper with data in computing systems, protection mechanisms "are often only secure *in principle*. They are seldom secure *in practice*." (Mullender, 1989).