PRIVACY ISSUES IN UBIQUITOUS MULTIMEDIA ENVIRONMENTS: Wake sleeping dogs, or let them lie?

Anne Adams **&** **Martina Angela Sasse**

Department of Computer Science
University College London, Gower Street
London, WC1E 6BT
England

A.Adams@cs.ucl.ac.uk A.Sasse@cs.ucl.ac.uk

ABSTRACT Many users are not aware of the potential privacy implications of ubiquitous multimedia applications. Decision-makers are often reluctant to raise users' awareness, since this may open a *"can of worms"* and deter potential users. We conducted an opportunistic study after videoconferencing developers placed a camera in the common room of their university department, broadcasting the video on the Internet. The email debate following the common room users "discovery" of the camera's existence was analyzed as well as 47 anonymous questionnaire responses. Three distinct types of responses were identified, varying with the *media type* (audio *vs.* video) transmitted and *scope of distribution* (local *vs.* global). The groups also differ in their perception of the common room *situation* (public *vs*. private) and the degree of *control* exerted by observers and those observed. We conclude that privacy implications of ubiquitous multimedia applications must be made explicit. Users who discover privacy implication retrospectively are likely to respond in an emotive manner, reject the technology, and lose trust in those responsible for it.

KEYWORDS Internet, Multimedia Applications, Privacy, Trust, Ubiquitous Computing, Grounded Theory

1. INTRODUCTION

1.1 Background

With the rapid advance of network and compression technology, ubiquitous multimedia is fast becoming a reality (Crowcroft et al., in press). Applications of this technology include broadcasting of multimedia data on a global scale (e.g. putting lectures and seminars on the Internet) and continuous recording of such data (e.g. video diaries). Remote access is an inherent feature of ubiquitous multimedia applications: data captured locally by microphones, cameras and sensors can be accessed through the network. Many users will welcome the chance to remotely check their windows at home if a storm breaks while they are at work, or to survey the contents of their fridge before going to the supermarket on their way home. The same users would not, however, allow anybody to view live video from their home, or to monitor their food preferences, since such data are regarded as private. Clearly, the increase in multimedia data, and functionality for accessing and using them, carries risks for users as well as benefits (Bellotti, 1997; Neumann, 1995; Smith, 1993).

Privacy is a basic human requirement. The U.S. supreme court ruled that privacy is a more fundamental right than any of those stated in the Bill of Rights (Schoeman, 1992). Providing adequate protection of people's privacy is complicated by the

phenomenon's socio-psychological nature – what is regarded as private varies across individuals, organizations and cultures. This is especially true in ubiquitous multimedia environments, which can involve many individuals, domains and cultures. There is, therefore, an obvious need for a HCI model of salient factors, which allow prediction of perceived privacy invasions. The main problem with establishing such a model in is that privacy factors vary according to users' perceptions, which are manipulated by an array of personal trade-offs (Davies, 1997). It is, therefore, necessary to consider social norms that guide our interactions, and how ubiquitous multimedia environments distort these norms and relevant privacy factors.

1.2 Social Norms

There is evidence that users equate computer-mediated interaction with interaction in the real world. Users' perception of social factors, such as privacy, is, therefore, vital to the successful and effective introduction of technology. Social norms (such as politeness and decency) guide social interactions and determine socially rich responses - irrespective of whether a system was designed to cater for them (Laurel, 1993; Reeves & Nass, 1996). Based on existing knowledge, users construct social representations that allow them to recognize and contextualize social stimuli. These representations originate from social interaction and help us construct an understanding of the social world, enabling interaction between groups sharing the representations (Augoustinos & Walker, 1995). Social situations provide cues that allow people to make assessments of those situations. Harrison & Dourish (1996) argue that it is a *sense of place* that guides social interactions and our perceptions of privacy, rather than the *physical* characteristics of a space. This is because social norms guide our perceptions of spaces allowing us to interpret them as places and adapt our behaviors accordingly. All parties within the same culture understand what is - and is not - acceptable in a given situation (i.e. it is acceptable to stare at a street performer but not at a passer-by). However, our perception of a situation also depends on how we see ourselves in that situation. Goffman (1969) pointed out that, when an individual takes part in an interaction, there is an intentional and unknowing perception of being involved in the situation. The presentation of the *self* within a perceived situation increases the risks attached with potential consequences extending from the personal to the social level. If an individual's perception of a situation turns out to be incorrect *after the event*, there are far-reaching consequences. Previously natural interactions suddenly seem inappropriate, making individuals feel awkward and flustered. The perception of the self and others is also likely to change. Ultimately, how we perceive ourselves depends on assumptions made about a situation that are based on social norms. If these assumptions are vastly inaccurate, there will be far-reaching repercussions.

1.3 Ubiquitous Multimedia Technology

Cowan (1983) argues that invasion of privacy is merely a by-product of the information society. Technology increases potential invasions of privacy because of the perceived *control* of certain applications. Karabenick & Knapp (1988) studied students who failed to identify concepts in a task, and were allowed to seek help from a computer or another person. The proportion of those seeking help from the computer was significantly greater than those turning to a person. Since a computer does not make psychological judgements about abilities, users' felt in control of the situation and trusted in the technology. Surveillance technology, on the other hand, has been used to curtail our freedom in a way so as to control and manipulate socially unacceptable behavior. Jeremy Bentham (1832) argued for control by surveillance, in the preface to his *Panopticon*, whereby every person in a building is watched from a central tower. Although people are not watched all the time, they maintain their standards of behavior for *fear of being watched*. Fear is maintained by examples being made of odd individuals, "*to keep the others on their toes"*. The *Panopticon's* modern-day equivalent, closed-circuit television (CCTV), is one of the fastest growing technologies. In the UK, for instance, coverage is such that there will soon be a national CCTV network. Although CCTV provides little or no means of control by those being observed many users accept the potential risks to their privacy (e.g. security staff using CCTV footage for their entertainment or profit) in a trade-off with perceived benefit (e.g. preventing crime). Such trade-offs are usually made within an environment where the perceived individual risks are low (*I am doing nothing wrong, so I am OK*) and/or the perceived benefits (e.g. personal safety) are high. If such a risk assessment (based on social cues) turns out to be inaccurate, the implications for privacy are far-reaching.

People need social cues about the type of situation in which they find themselves (e.g. public/private), and the types of appropriate behaviour with which they should respond (Goffman, 1969). We also use social cues to assess who we are interacting with and how we think others perceive us. Multimedia environments vary in the level of contextual cues provided that enable users to appropriately frame

their interactive behavior (Harrison & Dourish, 1996). Privacy problems often occur when people who *are observed* cannot *see how they are being viewed*, by whom (the information receiver), and for what purpose (Bellotti, 1997; Lee et al, 1997). Users may make assumptions about the information receiver (IR) viewing a picture of a certain size or quality, but technology may allow the receiver to configure and manipulate the image they receive. Interpersonal distance has, in the past, been found to dictate the intensity of a response: faces in a close-up are scrutinised more often than those in the background. Reeves & Nass (1996) argue that, because the size of a face is more than just a representation of an individual, it can influence psychological judgements of a person and thus become an invasive piece of information. Image quality and camera angles may result in a perception of the viewee by the viewer that the viewee regards as inaccurate. Users' assumptions about the IR can similarly be distorted by the technology. A system allowing the viewer to freeze the video (e.g. so that they appear to be avidly watching the screen, when they have actually gone to make themselves a cup of tea) could produce an inaccurate appraisal of their attention within the interaction. Another privacy issue associated with the IR is the viewee's assumption that there is only one viewer, when the information is actually accessible to many others. It has been argued that - if a system is embedded in the organisational culture - social controls will establish a culture of use which will restrict these activities (Dourish, 1993). Relying merely on social controls for safeguarding privacy is dangerous if assumptions based on social cues are distorted by the technology itself. The aim of the study reported here was to identify users' perceptions of ubiquitous multimedia, and its relationship to privacy factors. A specific model of the factors guiding users in their privacy assessments will then be developed.

1.4 Privacy Factors

To define privacy adequately, it is important to identify privacy *boundaries* which, if breached, are likely to cause resentment among users. If such boundaries can be identified and mapped, appropriate organizational behavior and security mechanisms could be formulated and integrated into organizational policy (Smith, 1993). Previous research has identified three main privacy factors: *information sensitivity*, *information receiver*, and *information usage*:

Information Sensitivity: Previous work on users' perception of authentication mechanisms (Adams et al., 1997; Adams & Sasse, in press) identified the concept of *information sensitivity*: users rate certain types of information as sensitive or private. This perception determines the amount of effort that users are prepared to expend on protecting that information. Discussions of privacy often ignore that the same information may be rated – and therefore treated - differently by different users. Another common misconception is that users make a simple binary *private/not private* distinction: users actually describe information sensitivity as a dimension with varying degrees of sensitivity.

Information Receiver (IR): Users' privacy can be invaded without them being aware of it (Bellotti, 1997). This leads to a further important distinction: whether it is *what is known* about a person that is invasive, or *who knows* it. To date, research on privacy has not clearly identified the role of the IR – who receives information that is rated as sensitive by a user. Users' perception of being *vulnerable to* - and *trusting* - the IR can enable or restrict self-expression and personal development within multimedia communications. Certain technology may apply well in an environment of trust but fail in an atmosphere of distrust (Harrison & Dourish, 1996; Bellotti, 1997).

Information Usage: Information about users can promote concerns about how and for what purposes it is used. (Dix, 1990). At the same time, privacy concerns can be reduced through trust, i.e. in an environment that have an '*acceptable use'* policy for potentially invasive applications and/or data (Bellotti & Sellen, 1993). It has been suggested that a lack of contextual elements in processing and use may be a key factor in potential invasions of privacy (Dix, 1990). These concerns can be addressed by providing users with mechanisms for control and feedback (Bellotti & Sellen, 1993). Such mechanisms, though, do not necessarily cover information which users initially perceived as innocuous but is potentially invasive when viewed out of context.

Finally, it must be identified whether users trade off perceived privacy risks against benefits (see section 1.3).

2. THE STUDY

2.1 Situation

Two videoconferencing developers (not the authors) placed a small camera in the staff common room of their university department. Their immediate colleagues knew about the camera, but the general staff of the department were not consulted. The camera captured a limited view of the common room, including the entrance, pigeonholes and some of the seating area. The camera view was transmitted

over the multicast backbone of the Internet[1] and thus could be viewed potentially by thousands of users anywhere in the world. The developers placed a notice explaining the purpose of the camera on the common room door. However, most common room users did not read the notice because the door was always open, obscuring the notice.

The purpose of the camera – to contribute to an existing *"Places around the World"* multicast session – was also announced in a casual message to a small email list of multicast tool developers. A week later, an email message about the availability of images from the common room was sent to a larger multimedia research list, and finally to the departmental mailing list. Three reasons were cited for placing the camera:

1. *"We can see from our desks what's going on in the common room, and decide whether to go there."*
2. *"To stop people taking coffee from other people's pigeonholes"* (followed by a ";-)" smilie).
3. *"This helps us gain experience with telepresence."*

An email debate ensued, in which several departmental members stated they were unhappy about the camera being in the common room. It was then suggested that the camera would be more beneficial in the photocopier room to check the accessibility of the copier. After a day's debate, the camera was moved to the photocopier room. Placed behind the copier, it transmitted a close-up view (at hip level) of photocopier users. There was a prominent notice on the photocopier room door and an announcement on the multimedia research list. The email debate continued, and further objections were raised, until the camera was finally removed.

The authors decided to seize the opportunity and distributed a 2-page anonymous[2] paper questionnaire, with both closed and open-ended questions[3], to all departmental members. The questionnaire asked how comfortable repondents were about:

(a) audio and visual transmission
(b) the situation (common *vs*. photocopier room)
(c) for different levels of transmission (department *vs.* university *vs.* world),
(d) the re-use of the information within a different context.

Grounded theory methods (Strauss & Corbin, 1990) were used to analyse the questionnaire responses and all relevant email messages.

2.2 Results

Pearson's correlation coefficient was used to analyze 47 questionnaire responses. The majority of respondents agreed on two points:

1. They were significantly less comfortable with *audio* rather than *video* data being transmitted - both generally and in the specific situation of the common room.
2. They were significantly less comfortable with the *re-use* of (recorded) video data as opposed to continuous transmission (see Table 1).

	No	**Mean**	**Sig**
General Visual & Audio	47	3.10 4.619	P < 0.005
Specific* Visual & Audio	47	3.17 4.643	P < 0.005
Specific* Visual & Reuse	47	3.17 4.24	P < 0.005

Table 1: Significant findings for all respondents
(*specific situation of the common room)

In a cluster analysis, 3 groups with significantly different *perception profiles* emerged (see Table 2 and Diagram 1).

	Grp 1	**Grp 2**	**Grp 3**
Group size	15	14	13
Significance levels			
Visual transmission General / Specific	**.029***	.655	.053
General Visual / Audio	**.005***	**.000***	**.000***
Specific Visual / Audio	.055	**.000 ***	**.000***
CS / UCL	.189	**.047***	1.000
CS / World DIS	.096	**.028***	.721

Table 2: Clustered groups comfort levels (*P<0.05)

Further qualitative analysis provided distinct profiles of each group (see Table 3 & 4). The qualitative issues were categorized according to the 3 privacy factors previously highlighted (see section 1.4). A clear difference was identified between

[1] See Macedonia & Brutzmann (1994) for an introduction to multicast conferencing technology and its applications.

[2] We did not ask for information which could potentially be used to identify respondents (e.g. multimedia expertise, gender).

[3] These sections allowed respondents to 'let off steam' - several pages were filled out by some respondents, providing a rich source of qualitative data.

respondents in Group 3's perspective of the situation and the other two groups.

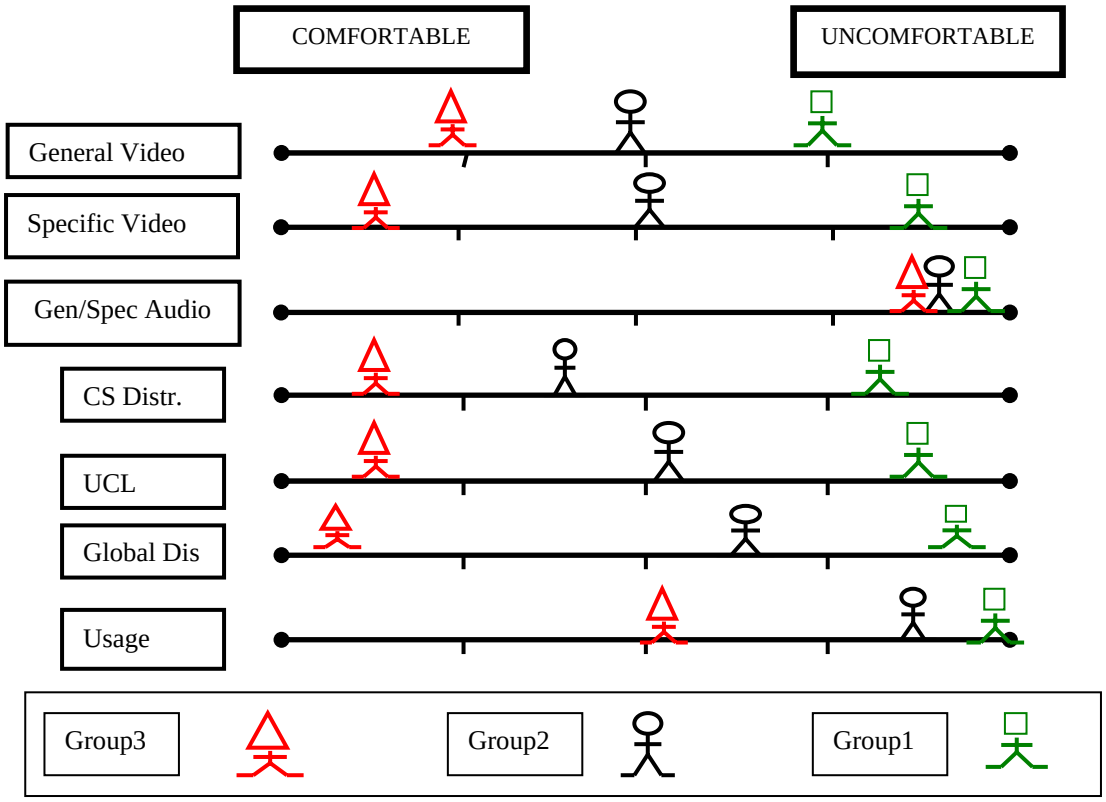

Diagram 1: Group profile for relevant privacy issues

	Grp 1	Grp 2	Grp 3
Information Receiver			
Observed Control	9	5	0
Observer Control	0	0	7
Information Sensitivity			
CR Private Situation	3	4	1
CR Public Situation	0	0	4
Information Usage			
Benefits	0	6	7
Costs	14	8	0

Table 3: Sample of qualitative analysis by groups

Since questionnaire responses were collected anonymously, we were not able to identify Group 3 members. However, analysis of the email debate indicates that many of the respondents who placed the camera in the common room (multicast tool developers) exhibited Group 3 profiles (discussed in detail in 3.2).

	Groups 1 & 2	**Group 3**
Observed Control	"… how to become one of the peeping toms"	**No comments**
Observer Control	**No comments**	"Could also be used as a soap substitute"
Emotive response	"only for nosy computer scientists wishing to assess the usefulness of their technology."	**No comments**

Table 4: Sample of coded comments

The degree of invasiveness of the video was also identified as related to the quality and focus of the picture being transmitted.

3. DISCUSSION

3.1 Privacy model validated

One pivotal finding of this study is the impact that users' perception of *information sensitivity* has on their assessment of privacy invasions. All users were significantly less comfortable with *audio* – rather than visual data - being transmitted. Users perceive what they say to be potentially more sensitive than what they do - in general, and in the specific case of this study (where video only was transmitted). All respondents also expressed strong discomfort if the video data transmitted were to be recorded and re-used (*information usage*) out of context (Dix, 1990). This highlights the flexible nature of *information sensitivity* - data initially considered to be non-invasive may be perceived as invasive when used out of context. Contrary to our expectations, the majority of respondents did not perceive the *information receiver* as an important factor effecting *information sensitivity* - except for Group 2, who was significantly more uncomfortable with distribution of the visual data beyond the department. Ultimately, the two groups that did not perceive the *information receiver* as a factor, either perceived the data as highly sensitive and thus invasive regardless of who viewed it (Group 1) or very low in sensitivity and non-invasive whoever saw it (Group 3).

3.2 Individual differences or social norms

The study revealed different perceptions of the *situation* and relevant privacy implications. Although this divide may not represent a split prior to perceived privacy invasions, it could be concluded that the divisions are due to individual differences in privacy needs. There have been arguments presented regarding the individual differences in privacy responses. Underwood & Moore (1981) argued that some peoples' behaviour varies according to the situation, whereas others' does not. Those with a high degree of "private self-consciousness"[4] carefully monitor their own behaviour (even when not being observed) and show consistent behaviour from situation to situation.

There are arguments, however, that organisational culture and social control can be traded-off against users' individual differences in privacy concerns (Dourish, 1993). Bellotti & Sellen's (1993) research identified that a reduction in users' concern about privacy was related to a general environment of trust, and the development of acceptable practices governing the use of the application. This brings to the forefront issues of trust, legitimate use and confidence in the information receivers. Ultimately trust - or lack of it - in *information receivers* and *information usage* is an important variable amongst all users, which can determine the information sensitivity. Our results show clear divisions in levels of trust in the technology. Whilst Group 3 expressed a high degree of trust (high usage benefits and no cost) in multicast conferencing, respondents in Groups 1 and 2 (68% of the respondents) expressed a lack of trust in the system (high usage costs). A key factor for Groups 1 and 2 appears to be the perception of being observed in a *private* situation (the common room) – a violation of a social norm. Group 3 in contrast perceived the common room to be a *public* situation with reduced social norms on observing people. This finding emphasises the importance of the perceived distinction between private and public, and the expected social norms in each situation, when defining *information sensitivity* (Schoeman, 1992). It could be argued that Group 3's perception of the common room as public is connected to their view of *observing*[5] rather than *being observed* in this situation (Group 1 & 2's assessment). It is interesting that those who originally placed the camera (technical experts in network multimedia) showed Group 3 profiles in the email discussion. A sense of being in *control* of the technology could therefore be linked to a distorted perception (from the majority) of the situation. These differences in perceptions may have already existed within the department. However, the technology introduction brought these differences to the fore, resulting in tension and an emotive debate which ended with a formal departmental decision to remove the technology. This is a lesson for other organisations: to assess how the relationships between organisational *control* and *trust* will affect users' privacy. Trust is undermined if users are not allowed to judge trade-offs for themselves or feel part of the proposed solution. Guidelines and boundaries (rather than restrictive controls) for use of the technology is required to encourage and nurture trust.

3.3 Technologies distorting social norms

To understand the power of ubiquitous multimedia applications, we must understand the social and

[4] This relates to Schoeman's (1992) idea of certain behaviours being mediated by social norms.

[5] These respondents also frequently used the common room and commented on this factor.

psychological factors governing its use. Most people are social creatures who are naturally interested in the world and people around them. The key question is whether that interest is socially acceptable and where the dividing line between benign and intrusive lies. *Being watched* is not a problem *per se* – it depends on our awareness of *how, when and by whom.* The type (e.g. camera angle), quality (e.g. resolution) and continuity (still images or continuous film) of video images can make them more or less invasive. It is not only important to an individual that they are identifiable in certain situations, but also how they are perceived. Filmmakers have used camera angles (close-ups, long shots) distorted quality (frosted lenses, lighting from below) and film continuity (stills, slow motion) for decades to aid film viewers in a crafted perception (as busy, slovenly, evil or good) of characters (Reeves & Nass, 1996). Thus, the individual's need to control how others view them cannot be ignored. Several respondents objected to the second situation (in the photocopy room) because the camera showed the hip portion only - producing a potentially comical or embarrassing image. How we are viewed is also dependent on the situation in which we are observed. Harrison & Dourish (1996) pointed out the importance of our perception of *place* in social interactions. We expect different behavior in private and public situations. In this study we identified a division in the perceptions of the common room situation. An individual's failure to accurately identify a situation as private can have serious consequences. To assess a technology-mediated situation accurately, users require adequate feedback and control mechanisms (Bellotti, 1997). Users' assessment of a situation depends on the degree of *control* they retain over how they are viewed and by whom. Our study highlighted how the observer's *control* of the technology distorted their perception of the *place* being observed. To explain this complex phenomenon, consider the analogy of sitting in a café (semi-private) watching people in the street (public) - which is socially acceptable in most cultures. However, someone in the street (public) pulling up a chair and staring in at the diners of the café (semi-private) would be perceived as unacceptable. Relating this analogy to this study, we can understand that the common room users perceived the situation as their café (semi-private) looking out on the street and corridor (public), able to see who can see them. The common room observers, however, were sitting at their desk – equivalent to their café - (private) looking out on the common room (public), seeing people who cannot see them. The issue highlighted by this example is the perceived ownership and control of the "window". We know and accept the risk of being watched and scrutinized as we walk in the streets (public). However, in more private situations (e.g. a café or changing room), our acceptance of being watched is reduced. Ultimately, our behavior is guided by the situation. If we misjudge the situation then we are at more of a risk of socially embarrassing ourselves. Assessing that situation is, therefore, of immense importance in our social interactions. This may help to explain the emotive response that ensued from the camera installation: a perceived privacy invasion. The emotive response was caused by Group 1 & 2's perceived *lack of control* over the situation, whereas Group 3 could not understand what all the fuss was about. Emotive responses are produced as a defense mechanisms to a perceived threat, resulting from a lack of control over - potentially detrimental – representations of the self (Goffman, 1969; Schoeman, 1992). Once users experience a lack of control and respond emotively, a total rejection of the application and all similar technology is the likely consequence. In this study, those who felt the most discomfort subsequently rejected transmission of any audio and video data under any circumstances.

4 CONCLUSIONS

In any social interaction, implicit assumptions are made to ensure the success of the interaction. If those assumptions are incorrect, we are more likely to misjudge a situation and act inappropriately. Multimedia environments have the potential to distort the assumptions that guide our behavior (Reeves & Nass, 1996). The technology developers' (who placed the camera) surprise at the emotive reactions to the perceived privacy invasion shows they had made inaccurate assumptions and misinterpreted the situation. The key to their perception of the situation as *public* is their familiarity with the technology, and thus their sense of control over it. This is probably why, even though Group 3 used the common room, they still retained an over-riding perception of the situation as an observer – they viewed the situation "through the camera's eyes". The reasons for placing the camera, as detailed by the technology developers' in an email, were primarily those of the observers, and not of those being observed. The "security" motivation (catch those who take other people's coffee) behind the camera placement, shows how the camera instigators dangerously crossed the line between multi-media environments and CCTV. Crossing this line breaks many implicit assumptions underlying multimedia environments as a tool for increased co-operation, communication and thus freedom of information. Similarly, if CCTV broke the

assumptions[6] underlying their successful implementation, they would be in danger of producing an emotive backlash. The camera instigators also stated that the purpose for the technology was to increase telepresence and allow users to see what was going on in the common room. However, as the web-site was not initially advertised to the whole department, this again decreased a sense of control over the technology for those being observed, and produced an emotive rejection of it beyond the confines of the present situation. This is an important finding for anyone introducing ubiquitous multimedia technology in an organization. Because of the degree of personal infringement experienced and the resulting emotive response, it is vital that the situation and implicit assumptions are judged accurately prior to installation. Privacy problems need to be addressed before they arise - before users lose trust and become emotive. Once a problem becomes emotive it is far harder to solve. However, this danger arises from the organizational philosophy of '*if it isn't broken, don't fix it'*. When it comes to ubiquitous multimedia technology and privacy – such an approach is likely to lead to rejection of the technology, and loss of trust in the organisation that introduced it. Ultimately it **is** too dangerous to let those sleeping dogs lie.

ACKNOWLEDGMENTS

We gratefully acknowledge the help of staff in the Department of Computer Science at UCL. Anne Adams is funded by BT/ESRC CASE studentship S00429637018.

REFERENCES

Adams, A., Sasse, M. A. & Lunt, P. (1997): Making passwords secure and usable. In H. Thimbleby, B. O'Conaill & P. Thomas (eds.), "*People & Computers XII* - Proceedings of HCI'97, pp. 1-19. London: Springer.

Adams, A. & Sasse, M. A (in press): The User Is Not The Enemy. To appear in *Communications of ACM*.

Augoustinos, M. & Walker, I. (1995): *Social Cognition*. London: Sage Publications.

Bellotti, V. & Sellen, A. (1993): Designing for privacy in ubiquitous computing environments. In G. de Michelis, C. Simone & K. Schmidt (Eds.): *Proceedings of ECSCW'93, pp.* 77-92. Kluwer (Academic Press).

Bellotti, V. (1997): Design for privacy in multimedia computing and communications environments. In P. E. Agre, & M. Rotenberg (Eds.): *Technology and Privacy the New Landscape*. Cambridge, Mass: MIT Press.

Bentham J (1832) "Panopticon" in Entham, J. (1995) "The panopticon writings". London: Verso.

Cowan, R. S. (1983): *More work for mother: the ironies of household technology from the open hearth to the microwave*. New York: Basic Books.

Crowcroft, J., Handley, M. & Wakeman, I. (in press): *Internetworking Multimedia*. London: UCL Press.

Davies, S (1997): Re-engineering the right to privacy. In P. E. Agre & M. Rotenberg (Eds.): *Technology and Privacy the New Landscape*, pp. 143-165 Cambridge, Mass MIT Press.

Dix, A. (1990): Information processing, context and privacy. In *Proceedings of INTERACT'90*, pp. 15-20. Amsterdam: North-Holland.

Dourish, P (1993): Culture and Control in a Media Space. In G. de Michelis, C. Simone & K. Schmidt (Eds.): *Proceedings of ECSCW'93*, pp. 125-137. Kluwer (Academic Press).

Goffman, E (1969*): The presentation of self in everyday life*. London: Penguin.

Harrison, R. & Dourish, P (1996): Re-Place-ing Space: The Roles of Place and Space in Collaborative Systems. In *Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW'96),* pp. 67-76. New York: ACM Press.

Karabenick, S.A; Knapp, J.R (1988): Effects of computer privacy on help-seeking. *In Journal of applied social psychology*. 18 (6), pp. 461-472.

Laurel, B. (1993): Computers As Theatre. New York: Addison Wesley..

Lee, A. Girgensohn, A. & Schlueter, K. (1997): NYNEX Portholes: Initial user reactions and redesign implications. In *Proceedings of Group'97*, pp. 385-394. ACM Press

Macedonia, M. R. & Brutzman, D. P. (1994): Mbone Provides Audio and Video Across the Internet. *IEEE Computer*, 27 (4), pp.30-36.

Neumann, P. G (1995) *Computer related risks*. New York: Addison-Wesley.

Reeves, B. & Nass, C. (1996): The media equation: How people treat computes, television and new media like real people and places. Stanford, CA: CSLI Press.

Schoeman, F. D. (1992): Privacy and Social Freedom. Cambridge: Cambridge University Press.

Smith, J. (1993): Privacy policies and practices: inside the organizational maze. *Communications of the ACM***,** 36 (12), pp. 105-122.

Strauss. A. & Corbin, J. (1990): *Basics of Qualitative Research: Grounded Theory Procedures and*

[6] If CCTV in a department store is used by management to assess staff performance, or by marketing to profile customers, this would violate passer-by assumptions of both the perceived information receiver (security personnel) and usage (security) factors.

Techniques. Newbury Park: Sage.
Underwood, B. & Moore, B. S (1981): Sources of behavioural consistency. *Journal of Personality and Social Psychology*, 40, pp. 780-785.