Taming the Wolf in Sheep's Clothing: Privacy in Multimedia Communications

Anne Adams
Department of Computer Science
University College London
Gower Street, London, WC1E 6BT
+44 (0)20 7419 3462
A.Adams@cs.ucl.ac.uk

Martina Angela Sasse
Department of Computer Science
University College London
Gower Street, London, WC1E 6BT
+44 (0)20 7380 7212
A.Sasse@cs.ucl.ac.uk

ABSTRACT

When ubiquitous multimedia technology is introduced in an organization, the privacy implications of that technology are rarely addressed. Users usually extend the trust they have in an organization to the technology it employs. This paper reports results from interviews with 24 Internet Engineering Task Force (IETF) attendees whose presentations or contributions to IETF sessions were transmitted on the multicast backbone (Mbone). Due to a high level of trust in the organization, these users had few initial concerns about the privacy implications of this technology. However, interviewees' trust relied on inaccurate assumptions, since the interviews revealed a number of potential and actual invasions of privacy in transmission, recording and editing of multicast data. Previous research found that users who experience an unexpected invasion of their privacy are not only likely to reject the technology that afforded the invasion, but lose trust in the organization that introduced it [2,3]. We discuss a number of mechanisms and policies for protecting users' privacy in this particular application, and propose a strategy for introducing networked multimedia technology in general.

Keywords

Privacy, trust, multicasting, multimedia communications, grounded theory

1. INTRODUCTION

The number of networked multimedia applications has increased rapidly in recent years. The ability to multicast audio, video and other data on the Internet [11] offers an unprecedented opportunity to access conferences, lectures and other events anywhere in the world [19]. The increasing availability and accessibility of such multimedia data does, however, harbor increased risks as well as benefits [5,6]. The relationship between multimedia data and privacy invasion has not yet been clearly described. Existing legal definitions do not address the particular nature of multimedia data and communications - the main problem being that they aim to define characteristics of data and information, rather than *how it is perceived* by users [10].

Literature in Computer Human Interaction does discuss users' perceptions of privacy, but the recommendations found tend to be based on anecdotal findings [5,6,13,20], or aimed at specific applications [16]. The aim of this study was to identify expert users' perception of the privacy risks associated with Internet multicasting of events. Expert users were specifically chosen in contrast to previous studies of novice users' perceptions of multicasting, video conferencing and virtual reality [2,3] where users had varying levels of organizational trust.

1.1 IETF Session Multicasting

The Internet Engineering Task Force (IETF) is an open international community concerned with technical aspects of the Internet architecture and its operation, and is open to any interested individual. IETF standards are developed by working groups that communicate via email lists and meet three times a year. The first multicast transmission was from the IETF in 1992 [11]. The original idea was to construct a semi-permanent IP multicast test bed to carry the IETF transmissions and support continued experimentation between meetings. The multicasting of selected sessions is now an established and accepted part of the IETF meetings. Selected IETF sessions are multicast using multicast tools such as rat [15], Vic [17] and WB [18] to transmit audio, video and shared whiteboard data. Multicasting of the sessions allows those who cannot attend the IETF to follow these sessions remotely and ask questions. Several thousand sites all over the world have the connectivity and tools required to receive these transmissions.

The fact that a session is multicast is noted on the IETF agenda of the sessions. No announcement about multicasting is made at the session itself, but the presence of microphones (only used for multicasting purposes) and cameras provide a clear visual clue.

2. THE STUDY

All participants who had presented at or spoken out in a multicast session at the 41st IETF in Los Angeles were contacted by email and invited to participate in an interview (lasting approx. 30 minutes) during the 42nd IETF in Chicago. All interviewees were experts in computer networking. Even though the majority of interviewees had little experience of watching the IETF sessions remotely (because they usually attended the IETF in person), they had remotely watched other events using the same technology. Those interviewed were initially asked open-ended questions about their perceptions of multicasting and privacy followed by specific questions on their perceptions of the:

- Information Receiver: who would be viewing the multicast sessions.

- Information Sensitivity: how sensitive the multimedia session information being transmitted was.
- Information Usage: the re-use of recorded multicast sessions.

2.1 Results

The interview data was collection and analyzed using grounded theory methods widely employed in social sciences [14,24]. The majority (67%) of respondents raised issues relating to *information usage* as the main threat to their privacy, especially through unauthorized editing of recorded multicast data (see Figure 1, Table 1). The presentation of such data out of context can increase the potential misinterpretation of the information.

Figure 1 and Table 1 show the percentile of interviewees who raised a particular issue as an existing or potential threat to privacy. This summary does not, however, reflect how much of a threat any particular issue was seen to be. It is important to consider this because if users feel strongly about a particular issue, the chances of them rejecting the technology are high. In many situations, distributed collaborative systems have to be adopted by general consent; rejection of a technology by a minority of users can thus undermine the implementation and use of a technology. The detailed qualitative analysis of the responses revealed the relative importance of each issue. These results are described in detail for each cate[illegible] by examples of users' perceived privacy invasions.

	Issue title	Summarized description	% response
Transmission	Outsiders	Outsiders changing session dynamics	25%
	Remote Viewers	Misinterpreting sessions due to a lack of context	12.5%
	Non-Participants	Non-participants viewed (sleeping, leaving)	12.5%
	Emotive Sessions 1	Emotional sessions being broadcast	10%
Record	Out of Context 1	Record and reviewing without time-reference	10 %
	Emotive Sessions 2	Emotive session recording	12.5%
Edit	Out of Context 2	Out of context editing	67%
	Emotive Sessions 3	Emotive session editing potentially misrepresenting	25%

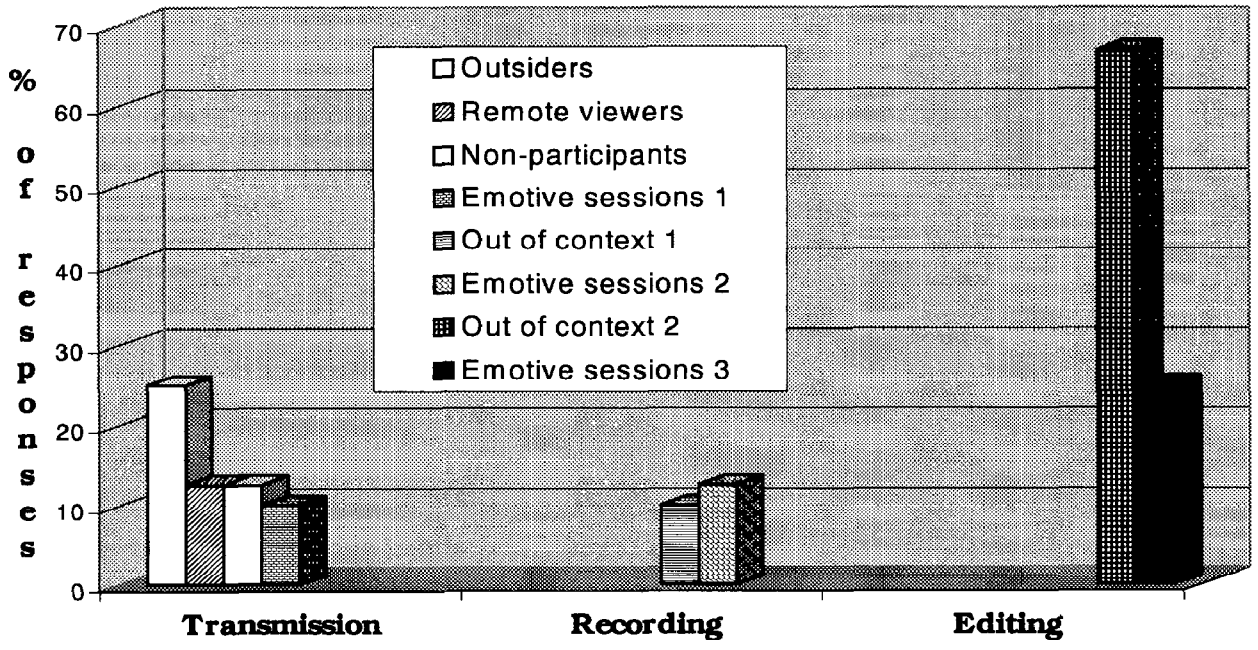

Figure 1: Users' Perceived Privacy Problems

Table 1: Categories of potential privacy issues

2.1.1 Transmission Issues

The transmission of non-participants' (people who were not actively participating in a session) images was not only mentioned by 12.5% of interviewees, but was also seen to be of great importance by those who mentioned it:

"That does feel like an intrusion on your privacy, to have them video taping you when your just sitting off in the corner - you know, having a conversation with somebody or falling asleep."

EXAMPLE: NON-PARTICIPANTS
"Apparently one time someone was tuning in and they saw one of my colleagues, one of my co-workers, falling asleep in one of the sessions - I fall asleep in lots of the sessions - but they [his bosses] took him to task for it, you know 'We saw you falling asleep, we didn't send you there to fall asleep!' you know."

The second transmission issue relates to *who receives* the transmitted multimedia data. A quarter of the respondents highlighted problems associated with *outsiders* (people not a part of the IETF technical community) viewing the sessions. Interviewees were, to some degree, concerned with the possibility that *outsiders* receiving the transmissions might change the dynamics of IETF session in two ways:

1. *"...it would inhibit some of the discussion."*
2. *"... it would encourage people to make statements with that broader audience in mind as opposed to just technical peers."*

EXAMPLE: OUTSIDERS
One interviewee recalled that the hotel in which a previous IETF had been held had transmitted sessions on its internal television network – this opened up the sessions to viewers who were not part of the IETF community, without speakers and contributors initially being aware of it.

The third transmission issue, raised by 10% of interviewees, was that arguments in sessions occasionally became *emotive* (heated), and that this could be potentially embarrassing for those involved:

> *"Presumably that would be the type of session that you'd be more likely to say something you didn't intend to have publicly known."*

A final – minor-issue - was that remote viewers might misunderstand some presentations. At the IETF, attendees often clarify points in a discussion with the speaker or contributor after the session ends – remote attendees find it hard to do this.

2.1.2 Recording Issues

The recording of sessions was not a major issue although some interviewees highlighted that a lack of recording context (time and place) increased the chances of misinterpreting the session. A key recording issue, however, was noted as the recording of sessions that had become *emotive* (see also previous section).

EXAMPLE: EMOTIVE SESSION RECORDING
"Only once when I slightly lost my temper and felt more like, you know, some people, they save it and watch it later on. It's the sort of thing that you wouldn't want to be captured for ever."

2.1.3 Editing Issues

The most important issue (both in terms of percentage of responses and strength of feelings) was related to the editing of recorded sessions. Like any soundbite, sections of a multicast session can be presented out of context. As one interviewee noted:

> *"It turns something into a pretty subjective interpretation of it."*

This issue increased in importance with the increased *perceived personal representativeness* of the multimedia information:

> *"I think that could be a problem if you're snarling at somebody and you miss all the reasons why you're snarling at them - so making you look unreasonable."*

EXAMPLE: EDITING OUT OF CONTEXT
"Somebody told me: 'Hey, I saw you the other day. I went to this workshop on multicast technology and you were talking,' and I said: 'I wasn't talking there.' They had shown like a demo of what a typical multicast session looked like, and it happened to be my presentation, and of course I hope they didn't show something like when I got a lot of questions or if there'd been a very heated discussion and I hadn't been doing very well at that discussion. I'd have found it a little bit embarrassing. They would show it to this group of people who have no idea what I'm talking about, what the subject is... In fact they probably wouldn't have listened to my whole presentation, they probably showed the last 5 minutes - a snippet - and they would have taken it completely out of context and of course that's not good."

3. TRUST AND THE INFORMATION RECEIVER

The results of this study corroborate previous findings. Most users of multimedia technology do not consciously assess the privacy implications of every situation they encounter – instead, *trust* governs the majority of users' privacy assessments [2,3,13]. Previous research, into password mechanisms, however [1,4] has shown that users need to be aware of *potential threats* to assess the true risks of any particular situation. Without this awareness, users' trust in the organisation will determine their perceptions of the situation and the positive or negative assumptions made:

1. Positive: users assume that the technology, introduced by an organization they trust, is trustworthy *('I've never heard of anything negative happening and I trust them so it must be okay')*. If users then find that this assumption is incorrect (i.e. find their privacy has been invaded), this results in a highly emotive rejection of the technology, and often also destroys the previously held trust.
2. Negative: users assume that the technology, introduced by an organization they distrust, is not trustworthy, causing an immediate rejection of the situation and the technology in question. *('I've never heard of anything negative happening*

therefore there must be a cover up of some terrible risks involved.')

The majority of interviewees showed a high level of trust in the organisation (IETF), and a desire to see the technology in question (IP multicast) succeed. Many interviewees, however, were not aware of the full privacy implications. As one respondent noted when talking about his own privacy concerns:

"But I have no clue that that has ever happened."

The results highlight that many of the respondents fears have already occurred and are likely to continue if they are not addressed (see previous section – 2.1).

Previous research [2,3,5,6] has shown that the information receiver is a vital part of users assessment of the privacy implications of information exchange. This highlights the issue of whether it is *what is known* about a person that is invasive, or *who knows* it. Most accounts of privacy have not clearly identified the role of the information receiver in the privacy equation. However, the users assessment of the information receiver will be influenced by:

1. the users experience of the information receiver;
2. a range of social and organizational norms;
3. the particular interaction setting (environment, task, system) [20,23].

Bellotti [6] details the importance of potential infringements of user perceived acceptable information receivers. It is surprising then that many interviewees noted that the information reciever was not an important issue for them *"...because the people that really matter are here, at the IETF."* The results of this study, however, show that there are important issues with regard to remote viewers, which are reliant upon the users implicit assumptions. Most interviewees assumed that the remote viewers were a small number of the same type of people that attended the IETF, and mainly academics (because these have easier access to the Mbone). When the issue of *outsiders* remotely viewing the sessions was discussed, several potential issues emerged:

1. Changing dynamics of the sessions: the presence of *outsiders* may make people less reluctant to speak out, or encouraging presenters to make more *"commercially acceptable"* and *"less technical"* statements.
2. Distorted impression: outsiders may gain a "distorted impression" of the sessions without the context required to understand statements made by speakers .

Throughout our life, we belong to a number of social groups with differing social norms. The privacy trade-offs we make rely on the social norms of the *group context* in which they are made. We are happy to reveal things to our family members that we would not want to reveal to our colleagues at work – and *vice versa*. For each group, there is an *outgroup* - those who are not members of that particular community. Acceptable practices are governed by the relevant community-determined social norms and social controls, which establish a culture of use for technologically-mediated communications [23,13].

For most interviewees, the benefits of multicasting sessions for within-community members who cannot attend the IETF outweighed the potential risks associated with sessions being viewed by *outsiders*. The same trade-off, however, did not apply to the hotel-internal transmission of IETF sessions. The benefits of attendees viewing sessions in their hotel room was not as great to the respondents (thus enough to outweigh the privacy negatives) as remote non-attendees viewing sessions. It is important to understand these privacy trade-offs so that the privacy effects of changing circumstances can be assessed prior to users loosing their trust in the organisation.

4. PRIVACY TRADE-OFFS

Relying merely on social controls for safeguarding privacy is dangerous [5]. Nevertheless, users do trade off privacy for perceived benefits in information usage. Identifying benefits of the technology, as well as privacy issues, is therefore vital. The *public forum* nature of the IETF was cited by many interviewees as a benefit that outweighed (for those presenting or contributing to a session) the majority of privacy risks associated with session multicasting. The same interviewees, however, were not necessarily prepared to accept the risks for *non-participant* attendees being shown on camera. The key issue here is that, at the sessions, attendees can see the people who can see them, and thus assess the associated privacy risks. If you know your boss is watching, you can make sure you look alert and interested. Remote viewers, however, are hidden, and so are the privacy risks. Some interviewees also argued that multicasting of this *public forum* retained the same risks as other forms of communication, such as email lists or bulletin boards. Textural media, however, usually provide some form of contextualisation - such as the date when a message was posted. This reduces the chance of a ten-year old comment being viewed as being made yesterday.

Bellotti & Sellen [5] argue that the ubiquity of unobtrusive technology increases the risk of privacy invasion. It is becoming very easy to generate and capture large amounts of data, but there are few corresponding mechanisms to provide users with control and feedback about its use. If such mechanisms were considered in the design and implementation of multimedia communications technology, the risk of privacy intrusions would be greatly reduced. However, though much of the data collected nowadays identifies individuals, the majority of people do not considered it as invasive. It is, therefore, users' *perception* of the information, which is of importance. Many contributions to the privacy debate often make a simple binary *private - not private* distinction, by devising privacy mechanisms for either all information or just 'personal information' without clearly defining what this term means to the user. In previous work on users' perception of authentication mechanisms [1,4], the concept of *information sensitivity* was identified. Users rated certain types of information in degrees of sensitivity. This perception, in turn, determined the amount of effort expended by them on reviewing and maintaining that information. Further research into users' perceptions of privacy have verified the importance of this privacy factor [2,3]

The study detailed in this paper also corroborates previous research which identified that information and thus its sensitivity can be interpreted at different levels [2,3]. *Primary* information relates to the topic of discussion, whilst *secondary* information relays other interpretative social or psychological characteristics about the user via auditory, visual or textural media. With increasing richness of data, there is an increase in secondary-level information (the way someone sounds, looks etc.). The majority of interviewees perceived the risk of having their privacy invaded, via the multicasting of sessions, as low because of its content *('We*

don't even want to listen to this – who else would?'). Privacy problems arise when only the information's primary level is reviewed for potential privacy risks. The interviewees were rating the sensitivity of IETF session data on the basis of its technical content (primary level). However, the recorded sessions could be viewed, at a secondary level, e.g:

i) illustrate mistakes commonly made in presentations;

ii) study the behavior of "techies";

iii) study how people from different ethnic backgrounds act and react in an argument.

At this secondary level, the data of technical debates could suddenly seem very personal, and its use perceived as highly intrusive. With the recording of this multicast information the associated privacy risks are higher than with, as one respondent pointed out, a documented record of events:-

> *"Although that kind of thing might not get reflected in the minutes as much - the level of emotion. I mean the argument might get reflected but the emotion won't be. How long did I yell - you know."*

The key factor here is the realisation that a misjudgement has been made. The information providers' assessment of the risk involved in the situation was inaccurate, and thus their control of the potentially invasive material has been lost [6]. Although misjudgements of the potential invasiveness of information can be made in normal situations, complex problems arise when technology inadvertently supports these misinterpretations. This highlights the importance of keeping data in its context [12].

How personally identifiable information is used (*information usage*) has always been of key importance to people with regard to privacy, and this is the main area where privacy is often dramatically noted as having been invaded (e.g. organisations discriminating against employees who they know have taken an HIV test). Users' fears about the use of technology are often said to come down to a fear of what information will be used for. It is not only how information is used, but the form it takes which may make it potentially invasive. A lack of contextual elements in information processing and usage is a key factor in privacy invasions [12]. This becomes doubly important in multimedia communication, as the perception of *'a picture doesn't lie'*, although inaccurate, still prevails to some extent [20]. Ultimately, most of the trade-offs that information providers make rely on trust relationships within the relevant communities. Many acceptable practices within multimedia communications rely on an equitable ratio of *perceived benefits, traded-off against the perceived risks.* It is not an equal balance between perceived benefits and costs that is vital in an acceptable trade-off, but changes to a perceived acceptable ratio [7]. Someone may be contributing more than others in a social interaction, but they find this acceptable unless this balance is changed - especially without their knowledge. Bellotti & Sellen's [5] research at EuroPARC found that privacy was not a major issue in the organizational multimedia communication application reviewed, as benefits were traded-off against potential concerns. Users low level of privacy concerns were due to the general environment of *trust,* and the development of acceptable practices relating to the application's usage. However, it must be understood that once this trust has been broken by a perceived privacy invasion, emotive responses and a potential rejection of the technology is likely to occur [2,3].

The results detailed in this paper show that the majority of interviewees saw the *context* of information as a major privacy problem which can be highlighted by one respondents' comments:-

> *"I don't mind editing in principle - just the way it seems to happen in practice that I seem to mind."*

When *low-sensitivity* information is taken out of context, it can sometimes become highly sensitive, personal representational information (at the secondary level) showing the user in a bad light. By editing sections of audio, video or a still image, someone can change how and what a person says, and even to whom they say it. However, as the majority or respondents had not personally felt this invasion of privacy occur, they are still open and responsive to actions being taken to address this potential problem.

5. CONCLUSIONS

Mayer et al. [21] identify a strong need for users' trust in organisations of the future, and emphasise the difficulty in maintaining these trust relationships. The study reported in this paper identified a high level of trust by the interviewees in the organisation in question. However research has shown [2,3] that if the privacy issues highlighted are not addressed before they become paramount, this may decrease the trust bond between the organisation and the information providers (in this case, presenters and contributors). The trade-off between perceived benefits and privacy risks made by information providers relies on assumptions that may be inaccurate. In order to retain system users' organisational trust levels, they must be informed of potential privacy risks (to make accurate risk assessments). In addition, the following issues should be addressed:

5.1 Information Receiver

- *Provide clear feedback* – on who is viewing sessions remotely or who may be viewing recordings in the future - thus relaying to the user potential risks of those outside the community viewing the sessions.
- *Assess risk of new media* - review whether the benefits of using a networked multimedia application outweigh potential privacy concerns. Changes in distribution procedures (e.g hotel TV distribution) will have an effect on who the potential information receiver is which, in turn, will effect the privacy trade-off made by the system user. A simple privacy risk assessment of the situation by the system administrators prior to any changes made could avoid potentially serious repercussions.

5.2 Information Sensitivity

- *Assess risk of camera shots* – are camera sweeps necessary? Which camera views are potentially sensitive or embarrassing? Previous research has suggested providing feedback to [5,6] or informed consent and permission from [20] those whose image is being broadcast or recorded. However, in many situations this course of action would be impractical (e.g providing all IETF attendees with feedback on all potential privacy risks from transmitting data). Ultimately, an initial appraisal of the importance and associated privacy risks of the information being captured is all that is required (e.g. how important is the information, how sensitive *could* the information be, do those being broadcast know the risks involved).

- *Contextualise multimedia data* - embed a visible date/time-stamp and name of the event in multicast video data [22]. The importance of contextualising video data has been commented on by several other authors [12,13,20]. We suggest that this simple, easily added feature could provide a first step towards preventing data being used out of context, intentionally or unintentionally.
- *Sensitivity feedback to the information receiver* – all actual invasions of privacy reported by the interviewees in our study were unintentional, i.e. the information receivers did not realize that their use of the data was an infringement of the information broadcasters' privacy. One way of raising information receivers' awareness of privacy issues would be through transmitting explicit statements of what constitutes "acceptable use" of the data – and what does not – at the beginning and end of a session. A second way would be by embedding permission-type tags in the transmitted data and displaying an alert when potentially unacceptable actions (e.g. such editing of an audio stream) are performed by the information receiver (see below).

5.3 Information Usage

- *Implement digital watermarking and watercasting* – incidents of copying and editing of multimedia data can be traced if transmitted data are marked using these techniques [9,8]. Copied multimedia data, once identified, could be traced back to its origins. Sessions could be transmitted with an embedded mark that allows broadcasters (e.g. the speaker or organizer of multicast sessions) to trace their multimedia data used publicly elsewhere (e.g. as part of a paper or lecture displayed on the Web). Rather than have users trawling the Internet to see if, where and how their multimedia data is used, a webcrawler-type search engine could perform this task and report this information to the user. Information receivers could also be informed, using a cryptographic hash function, of edited multimedia data against the broadcasters' wishes. It is important to note that these actions could help to provide feedback on unacceptable practices in multimedia usage behaviors thus developing social norms of expectable behaviors.
- *Keep an on-line session archive* - continuation of the IETF recorded archive (http://imj.gatech.edu/), which was mentioned by some interviewees as a useful reference source to counteract edited versions. However, a link from an edited version to the original was suggested as a useful addition. A visual watermarked link could provide feedback to information receivers that 1. this version has been edited and 2. there is a link back to the original unedited version.
- *Editing permission policy* – many respondents were only happy with the editing of recorded sessions if they first gave their permission. This requirement should be detailed on the IETF session archive page as well as being relayed to those viewing the sessions remotely.

Within the fast changing organizations of today it is vital that potential privacy issues are dealt with pro-actively before it becomes too late to rectify the damage done. Organisations that wish to utilize networked multimedia technology successfully should acknowledge the wolf beneath the sheep's clothing and take steps to tame it. If users discover it themselves by chance, their inclination may be to run, i.e. reject the technology.

6. ACKNOWLEDGMENTS

We gratefully acknowledge the help of our colleagues in the Computer Science Dept at UCL, specifically the technical advice from, and discussions with, Ian Brown and Jon Crowcroft. Anne Adams is funded by a BT/ESRC CASE studentship S00429637018.

7. REFERENCES

[1] Adams, A. & Sasse, M. A The user is not the enemy. Commun. ACM (in press)

[2] Adams, A. & Sasse Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie? In Proceedings of INTERACT'99 (Edinburgh UK, Sept 1999) (In Press)

[3] Adams, A. Users' perception of privacy in multimedia communication in Proceedings (extended abstracts) of CHI' 99 (Pittsburgh PA, May 1999), ACM Press, 53-54

[4] Adams, A., Sasse, M. A. & Lunt, P. Making passwords secure and usable *in* H. Thimbleby, B. O'Conaill & P. Thomas (eds.), Proceedings of HCI'97 (Bristol UK, Aug 1997). Springer, 1-19.

[5] Bellotti, V. & Sellen, A. Designing for privacy in ubiquitous computing environments *in* G. de Michelis, C. Simone & K. Schmidt (eds.), Proceedings of ECSCW'93, (Milano, Italy, Sept 1993), Kluwer (Academic Press), 77-92.

[6] Bellotti, V. Design for privacy in multimedia computing and communication environments *in* Agre, P. E & Rotenberg, M. (eds.) Technology and Privacy the New Landscape. MIT Press, Mass,1997.

[7] Brown, R. Social psychology (2nd ed.) Free Press, New York,1986.

[8] Brown, I., Perkins C. and Crowcroft J. Watercasting: Distributed Watermarking of Multicast Media. Submitted to Globecom '99, Rio de Janeiro, December 1999.

[9] Craver, S. Yeo, B. & Yeung, M. Technical trials and legal tribulations in Commun. ACM 41, 7, 45- 54, 1998.

[10] Davies, S. Re-engineering the right to privacy in Agre, P. E & Rotenberg, M. (eds.) Technology and Privacy the New Landscape. MIT Press, Mass, 1997.

[11] Deering, S. Host extensions for IP Multicasting. Request for Comments RFC 1112. Internet Engineering Task Force, 1989.

[12] Dix, A. Information processing, context and privacy in proceedings of INTERACT'90 (North-Holland, Sept, 1990) Kluwer (Academic Press), 15-20.

[13] Dourish, P. Culture and Control in a Media Space *in* G. de Michelis, C. Simone & K. Schmidt (eds.), in proceedings of ECSCW'93 , (Milano, Italy, Sept 1993), Kluwer (Academic Press). 125-137.

[14] Glaser, B. & Strauss, A. The discovery of grounded theory. Aldine, Chicago IL, 1967.

[15] Hardman, V., Sasse, M. A. & Kouvelas, I. Successful Multi-party Audio Communication over the Internet. Commun. ACM, 41, 5, 74-80, 1998.

[16] Lee, A. Gigensohn, A. & Schlueter, K. NYNEX Portholes: Initial user reactions and redesign implications, in proceedings of the International ACM SIGGROUP Conference on Supporting Group Work, GROUP'97 (Phoenix, AZ) ,New York, NY, 385-394.

[17] McCanne, S. & Jacobson, V. Vic: A flexible framework for packet video, Proceedings ACM Multimedia'95 (San Francisco CA, Nov, 1995) ACM Press, 511-522.

[18] McCanne, S., Jacobson, V. & Veterli, M. Receiver-driven layered multicast. Proceedings of ACM SIGCOMM'96 (Stanford University, California, August 26-30, 1996) ACM Press, 117-130.

[19] Macedonia, M. R. , Brutzman, D. P. Mbone Provides Audio and Video Across the Internet, *IEEE Computer*, 27 4, 30-36, April 1994.

[20] Mackay, W.E. Ethics, lies and videotape... in Proceedings of CHI '95 (Denver CO, May 1995), ACM Press, 138-145.

[21] Mayer, R. C., Davis, J. H. & Schoorman, D. F An integrating model of organisational trust. Academy of management review. 20, 3, 709-734, 1995.

[22] Memon, N & Wong, P, W Protecting digital media content Commun. ACM, 41,7, 41-43, 1998.

[23] Schoeman, F. D. Privacy and Social Freedom. Cambridge university press, Cambridge,1992.

[24] Strauss. A. & Corbin, J. Basics of Qualitative Research: Grounded Theory Procedures and Techniques. Sage, Newbury Park,1990.