Privacy in multimedia communications: Protecting users, not just data

Anne Adams

Department of Computer Science, Middlesex University, Bounds Green Road, London, N11 2NQ, UK.
Tel: *+44 (0)20 8411 6946*
Email: *a.adams@mdx.ac.uk*
URL: *http://www.cs.mdx.ac.uk/staffpages/aadams/*

Martina Angela Sasse

Department of Computer Science, University College London, Gower Street, , London, WC1E 6BT, UK.
Tel: *+44 (0)20 7679 7212*
Email: *a.sasse@cs.ucl.ac.uk*
URL: *http://www.cs.ucl.ac.uk/staff/a.sasse/*

As the use of ubiquitous multimedia communication increases so do the privacy risks associated with widespread accessibility and utilization of data generated by such applications. Most invasions of privacy are not intentional but due to designers inability to anticipate how this data could be used, by whom, and how this might affect users. This paper addresses the problem by providing a model of user perceptions of privacy in multimedia environments. The model has been derived from an analysis of empirical studies conducted by the authors and other researchers and aids designers to determine which information users regard as private, and in which context. It also identifies trade-offs that users are willing to make rendering some privacy risks acceptable. To demonstrate how this model can be used to assess the privacy implications of multimedia communications in a specific context, an example of the models application for a specific usage scenario is provided.

Keywords: Privacy, Multimedia Communications, Grounded Theory, Trust, User-centred design

1. Introduction

The increasing uptake of multimedia communications technology brings risks as well as benefits. The relationship between technology and privacy is particularly complex, and often discussed in emotional - rather than rational - terms (Adams &

Sasse, 1999a;b). The discussion of privacy within the HCI community looks likely to continue throughout the new millennium. The CHI '99 panel *"Trust me, I'm accountable: trust and accountability online"* (Friedman & Thomas, 1999) provided a showcase of the difficulties faced by application designers and organizational users. Two positions emerged from the debate:

1) "As the new technology environments develop, users will adapt their privacy expectations and behaviours."

2) "*Privacy is a complex problem, but it will not go away. To design successful applications, we have to acknowledge the problem and start tackling it, proactively."*

The first type of response may remind veterans of the early days of HCI, when some in the computing industry argued that *"inaccessible user interfaces are not really a problem - people will get used to them, eventually."* The continued growth of HCI as a discipline shows how misguided that belief was. In our view, designers and organizations who subscribe to the view that *"users will eventually get used to"* having no privacy in computer environments, are similarly misguided.

1.1 Background

The problem with much of the published literature on privacy is that it concentrates on protecting certain types of *data* without establishing what *people* regard as private information (Davies, 1997). Expert opinion on what might be invasive is not a sufficient basis for designing acceptable multimedia communication technology, or effective policies for their usage. Professionals' perceptions of the data captured are not sufficient grounds for determining what will be acceptable to users. In our view, it is vital to identify user's perceptions to predict acts that will be regarded by them as invasive, and why (Adams & Sasse, 1999a;b).

Although previous research (Bellotti, 1996; Bellotti, & Sellen, 1993; Lee, Girgensohn, & Schlueter, 1997, Smith, & Hudson, 1995) has identified the need for user feedback on, and control of, potentially invasive information, we need to understand when and why users want to exercise this feedback and control. Most privacy research to date has focussed on policies and mechanisms around the concept of *personal information* - data that can be used to identify an individual (Davies, 1997). We argue that such a *data-centric* approach cannot work well in the domain of multimedia communications. The majority of data in this field allows identification of a person (e.g. video image, voice patterns). Labelling all audio and video data as *personal information* - and thus declaring it to be *off limits* - is hardly practical. To define privacy it is important to review an *individual* within society; for being private requires a public context (Wacks, 1989; Goffman, 1969; Agre, 1997). Thus, organizational *culture* (Smith,1993; Dourish,1993) and perceptions of the *situation* (Harrison, & Dourish,1996; Adams & Sasse, 1999a) will influence what users are prepared to reveal about themselves.

Ultimately, it is important to understand that most multimedia invasions of privacy are not intentional or malicious (Adams, 1999; Adams, 2001; Adams & Sasse,

1999a & b). Seeking to address this problem a model of the user perspective on privacy in multimedia environments has been identified. The model helps to determine which information users regard as private, from whom, and in which context. The model also highlights privacy risks users' trade-off against the potential *benefits* to be gained from using multimedia applications.

2 Research Approach

To generate the model of users' perceptions of privacy (see Figure 2), we drew on an established approach from social psychology. *Grounded Theory* is a structured approach to both qualitative and quantitative data which can be used to model highly complex and sensitive phenomena in a structured empirical yet ethical manner, making it ideal for identifying privacy perceptions (Strauss & Corbin, 1990; Stevenson, & Cooper, 1997). This *Grounded Theory* model was developed inductively from an integrated analysis of previous privacy literature and further studies of the phenomenon within multimedia communications (Adams, 2001). Rather than formulate a model and then attempt to prove it, the model was allowed to emerge through the analysis of qualitative and quantitative data collected by the authors and other privacy researchers. The *Grounded Theory* analysis has produced:

1) A privacy model of the factors involved in privacy invasions.
2) The privacy invasion cycle, which details how these factors lead to privacy invasions.

Designers and organizations wishing to implement multimedia communications should identify user assumptions (see Figure 1) for each privacy model factor and match them to what is actually occurring to identify areas where users' may perceive threats to their privacy. This process should take place prior to, or during, technology installation. The model can be used as a guide to identifying where potential privacy problems could occur for specific scenarios and where further investigation and consultation may be required. It should be noted that some model aspects require further research to detail pre-emptive solutions to the privacy invasion cycle.

3 Privacy Invasion Cycle

The central concept for the *privacy model* is privacy invasion and its story-line (the conceptualisation of a descriptive narrative for privacy invasion) is the *privacy invasion cycle*. The changing process detailed in the *privacy invasion cycle* (PIC) details users' strategies for managing and responding to privacy invasions. PIC (see Figure 1) reveals that most invasions of privacy occur when users realise that a mismatch has occurred between their perceptions and reality.

(1) TRUST: Users do not go into every situation ready to assess the privacy benefits and risks of that information exchange (Adams, 1999; Adams & Sasse, 1999a;b). The degree of trust[1] felt by the user in the *Information Receiver*, technology and technology instigators determines the degree of privacy evaluation required**.**

(2) ASSUMPTIONS: The trust felt by the user in that information exchange relies, however, on many implicit assumptions surrounding that interaction (Adams, 1999; 2001; Adams & Sasse, 1999a;b).

i) Users previous knowledge and experiences and their role in the interaction
ii) Perceived *Information Sensitivity* (IS).
iii) Perceived *Information Receiver* (IR).
iv) Perceived *Information Usage* (IU).
v) Perceived Context of interaction.

The technology mediating the multimedia interactions can make those assumptions inaccurate.

(3) REALISATION AND RESPONSE: When users realize that their assumptions were inaccurate, they experience an invasion of privacy. Their responses are likely to be emotive, resulting in a rejection of the specific system, decreased trust in the *Information Receiver* and the organization who implemented the technology (Adams & Sasse, 1999a;b).

(4) DECREASING CYCLE: The next time the user encounters what they perceive to be a similar scenario (i.e. similar *Information Receiver*, technology or organisation implementing the technology) their initial trust levels will be lowered, and distorted negative assumptions may prevail which, if confirmed, will decrease users' trust still further (Adams & Sasse, 1999a;b).

The PIC thus details high-level perceptions of privacy invasion and how these perceptions change over time. For designers and those deploying multimedia, however, a detailed account of the factors involved is required to identify potential solutions. The privacy model, therefore, reviews in more detail the factors relevant to PIC.

[1] Users' privacy perceptions often reflect their trust in the organization, technology and thus expectations for privacy protection, rather than perceived potential privacy risks and responses to those risks.

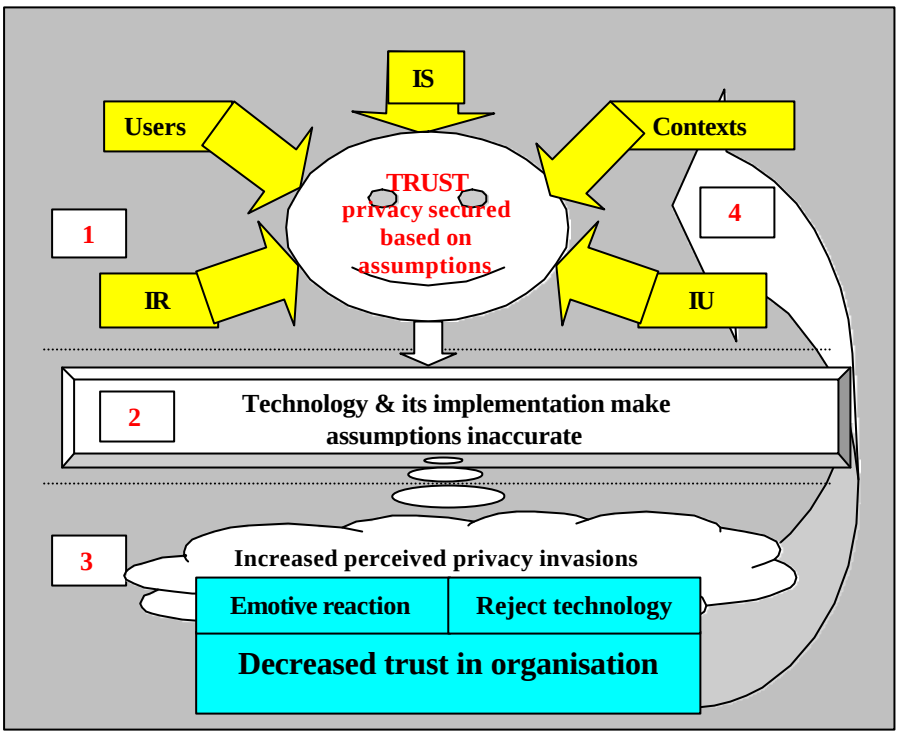

Figure 1. The privacy invasion cycle.

4 Multimedia Privacy Model

Like all mental models, users' privacy perceptions are not necessarily correct – they may be inaccurate, incomplete and biased – but they nevertheless determine user responses (Norman, 1986). It is therefore vital to establish the perceptions and assumptions with which users approach a specific technology in a particular context. This model (see Figure 2) has identified 3 major privacy factors (*Information Sensitivity, Receiver & Usage*) that interact to form the users' overall perception of privacy. There are also two further issues which are important but not specific to privacy (*User, Context*). The context of interaction also produces context issues which interact with and vary the importance of the privacy factors (e.g. Scenario1: IU > IS or IR, Scenario2: IR > IU or IS). Within specific scenarios trade-offs occur between the factors making some privacy risks acceptable to users based on their assumptions. This paper presents a summarised version of the model and relevant issues (Adams, 2001). Our aim is to provide designers and organizations with a better understanding of how users will perceive data generated or transmitted by multimedia communications technology, and the way it is used.

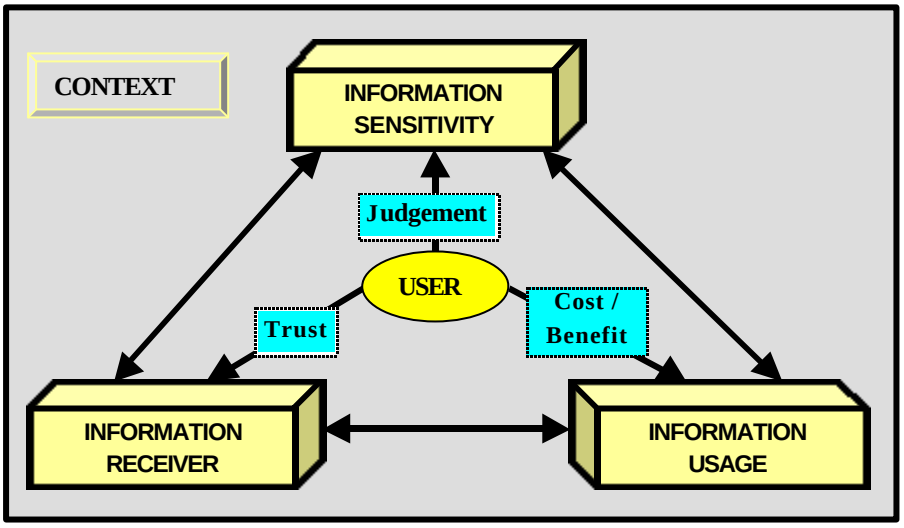

Figure 2. Privacy model factors and issues.

4.1 Privacy Factor: Information Sensitivity

The primary factor in this privacy model is *Information Sensitivity* (IS) (Goffman, 1969; Adams, 1999; Adams & Sasse, 1999a;b;c). *Information Sensitivity* relates to the users' perception of the data being transmitted and the information interpreted by the receiver. This model highlights that contrary to the *personal information* approach to privacy users make adjustable judgements about *Information Sensitivity* (Bennett, 1992; Agre, 1997). Users judgements assess *Information Sensitivity* via a flexible scale rather than making a simple binary private vs. not private distinction. Users' perception of the data transmitted, and how public or private the broadcast situation is, can also affect perceived sensitivity levels.

4.1.1 Primary and Secondary Level Information

A key factor in a user's perception of multimedia data is the degree to which it provides information that defines them personally. Most data can be used to infer at least two levels of information:

i. *Primary level*[2]: The core data being broadcast / the topic of discussion e.g. the medical facts discussed in a video-mediated doctor-patient consultation, or technical opinions of a speaker giving a remote lecture.

ii. *Secondary level*: other interpretative social / psychological characteristics of the user broadcasting the data e.g. the body language a doctor adopts when giving a pessimistic diagnosis to a patient, or the speech characteristics of the speaker giving a lecture.

[2] Highly sensitive primary information, which is personally defining, tends to relate to the traditional paradigm of *personal information*. Here the sensitive nature of the information is immediately apparent e.g. medical information, personal finance information etc.

We have found that many privacy invasions can be explained in terms of primary/secondary levels of information: most users fail to appreciate that the data in question can reveal more than primary level information. When they discover the data has a secondary level, which has been used in a way they did not anticipate, they feel that their privacy has been invaded. Consider the case of sales staff that discover the security cameras in their store were also used to evaluate their performance. The secondary level can also emerge over time: students participating in video-mediated tutorials (Adams, 1999) initially rated discussions of their coursework as 'impersonal' and regarded anyone using the data as a 'non-invasive' act. Towards the end of the course, however, the same students regarded the same data as potentially invasive, since someone reviewing several sessions could notice that a particular student was a *social loafer*, i.e. always badly prepared and contributing little to the discussion. Information can thus become invasive depending on what context the information was viewed in, how it was used and who viewed it.

Primary-level information may affect perceived sensitivity of secondary level information, and vice versa. Lacking knowledge of your field of expertise would be more personally detrimental than having an inadequate understanding of a general topic – e.g. the weather (unless you are a meteorologist). Similarly, being emotional (2^{nd} level) in a family argument (1^{st} level) will appear more appropriate than becoming emotive about the weather. Interactions can also occur between the *context* of data, the *Information Receiver*, and its *usage*. It is the increased potential for ubiquitous technology to vary these factors without the user's full awareness of the repercussions, which increases the likelihood of unacceptable privacy risks.

It is particularly important to review *Information Sensitivity* issues within multimedia communications technology. Firstly, multimedia generates a richer set of data, and this increases the amount of secondary information relayed. Examples include:

- Text with textual cues: information presentation, inappropriate use of language, etc.
- Audio with verbal cues: tone of voice, accent or dialect, gaps in conversation etc.
- Video with visual cues: dress and look of user, mannerisms, body language etc.

Secondly, the speed with which multimedia data can be distributed to a potentially vast audience further increases the risk associated with un-anticipated interpretations of such data.

4.1.2 Situation

How others view us depends on the situation in which we are observed. Harrison & Dourish (1996) point out the importance of our perception of "place" in social interactions. Certain behaviours may be socially acceptable in a *private* situation, but not in a *public* one - and *vice versa.* If a user misinterprets how public a

situation is, the result may be inappropriate behaviour, thus producing inappropriate expressions of themselves. Adams & Sasse (1999a) report an example where those installing a multimedia application judged the situation (staff common room) as public, and thus saw no problem with broadcasting images over the Internet. The users, however, regarded the situation as private or semi-private, and felt their privacy was being invaded through the installation of a camera. The result was an emotive rejection of the technology, and decreased *trust* in those who had introduced it. However, it is not just the distinction of *public* vs. *private* that is important, but the users' notion of *place* that is vital in perceptions of how private the information may be (Harrison & Dourish 1996). Some data may be considered unacceptable for transmission beyond a specific public setting. Adams & Sasse (1999b) reviewed perceptions of audio and video data being broadcast from a public conference. Even though transmitting images of speakers and those asking questions was deemed acceptable, broadcasting video of the audience was not. This issue was emphasized when embarrassing images of a member of the audience sleeping during a session were broadcast; his boss happened to watch the session and reprimanded him on his return. This highlights an interaction between *task* and *situation* factors. The situation for the conference attendee was only acceptably public to those visible to him, whilst the images were used for purposes other than those assumed of information exchange (similar to staff performance monitoring).

Mackay (1995) and Bellotti & Sellen (1993) suggest that people should be made aware that their images are being transmitted. Ultimately this model proposes that allowing users to weigh-up the information value (e.g. audience to obtain overall session perspective) against potential privacy risks involved (e.g. those not consciously on show being viewed) prior to transmission reduces the likelihood of these invasions occurring. It must be remembered that although technology deployers perceptions are important that they are likely to have different situation perceptions from those of users (Adams & Sasse 1999a).

4.2 Privacy Factor: Information Receiver[3]

The *Information Receiver* (IR) is the user's perception of the person (not necessarily actual person) who receives and or manipulates their data. A range of issues will influence users' assessment of the *Information Receiver* and potential trade-offs made, with trust (often based on relationships, information roles and group membership) playing the most important part (Adams 2001).

4.3 Privacy Factor: Information Usage

The model identifies that the final privacy factor *Information Usage* relates to users' perception of how their information is currently being used or at a later date.

[3] For a detailed full analysis of this complex factor see Adams, 2001.

Important usage issues (some of which this paper expands upon) relate to the users' perception of task, recording awareness, repeated viewing, context, editing and risk/benefit trade-offs.

4.3.1 Current information usage: Task

This model highlights the importance of *task* factors on users' perceptions of information and related privacy issues, as most multimedia privacy research has not reviewed these aspects. Davis (1997) asserts that the acceptability of CCTV for surveillance (security) in the UK is a manipulation of the concept of public interest. Adams & Sasse (1999a) report a case where the line between awareness and a surveillance technology were crossed according to users' perceptions. Crossing that line violated users' implicit assumptions underlying multimedia environments as a tool for increased co-operation, communication and thus freedom of information. This resulted in an emotive rejection of the technology, and a decrease in users' trust in the organization.

4.3.2 Later information usage: Recording, Repeated viewing & Editing

Users' anxieties about the use of technology are often said to come down to a fear of the potential *Information Usage*. Recording of multimedia data increases the likelihood of information losing important contextual factors, which can increase the potential for it to become invasive (Dix, 1990). Adams & Sasse (1999b) identified that data recorded without time and date stamps could be potentially invasive when viewed out of context. A professor, for example, presenting her findings via videoconferencing which is recorded and viewed 10 years later could be viewed as an out of date researcher if the information has not even been date stamped. Further contextual information could decrease potential misunderstandings for future *Information Receivers*.

Using recorded multimedia data with secondary level information (see section 2.2.1) also increases its sensitivity, as the potential to view the data repeatedly increases (Mackay, 1995; Bellotti, & Sellen, 1993; Adams & Sasse, 1999b). An embarrassing instance (emotional response in a debate, an indelicate physical action) within an interaction could be 'written off' as one of those humiliating moments best forgotten. However, a record of that event can be watched an infinite number of times by numerous people. It must be remembered that if the most guarded of politicians can make embarrassing mistakes on film what is the probability that the rest of us will.

Organizations often assume that a user providing personal data for accepted organizational practices (e.g. providing a service) accepts that this can be used in any way that fits within these parameters. This again makes the mistake of assuming that information remains at the same degree of sensitivity regardless of slight changes in its usage. Using recorded videoconferencing data to evaluate the technology may be acceptable; using the same data to evaluate the technology's effect on people of different ethnic backgrounds may not. Not only should casual

access to multimedia data be restricted (Mackay, 1995), but an understanding obtained of how changes in usage can affect sensitivity levels.

As the potential to manipulate and edit data increases, so do associated privacy risks. This becomes doubly important within multimedia communications, as the perception that "*a picture doesn't lie"'*, although inaccurate, still prevails (Mackay, 1995). Although taking a section (in its entirety) out of the whole may appear to be keeping it within its context, evidence shows that users perceive this as a major threat to privacy (Adams & Sasse, 1999b). However, it must be understood that the majority of findings of privacy invasion within multimedia communications result from unintentional acts rather than malicious intent.

4.4 User Issues

Within multimedia communications the term *user* traditionally refers to people both broadcasting and receiving information. However, it is as the former that we take privacy risks and as the latter that we encounter communication benefits that can be traded off against those risks. This model, therefore, highlights the importance of presenting the user as the person who has data transmitted either directly (primary information - their work achievements, consumption habits, medical records etc.) or indirectly (secondary information – personality, attentiveness, intelligence) about themselves. The model also identifies that for privacy purposes designers and technology deployers must understand that the user may well not be actively using the system and may actually be unaware that their data (their image, voice etc.) is being transmitted (Bellotti & Sellen, 1993; Adams & Sasse, 1999a;b). Ultimately, users' perceptions of the sensitivity of multimedia data will initially be biased by their knowledge of, and previous experience with, the technology and the data it generates. In particular, previous experiences - positive in terms of benefits, negative in terms of privacy invasions – will affect their judgements.

4.5 Context Issues

The context of interaction relates to user perceptions of the technology, social and organisational norms as well as national and international boundaries.

4.5.1 Technology

In the real world, people rely on social and physical cues to appropriately frame interactive behaviour (Goffman,1969). Within virtual interactions, contextual cues are often lacking or distorted, resulting in user isolation from reality. Most privacy research in HCI has concentrated on distorted perception of information caused by problems at the user interface level. Disembodiment from the context of the interaction and dissociation from one's actions are suggested to be key factors in user isolation. Bellotti & Sellen (1993) argue that users require feedback on, and control of, how they are presenting themselves in multimedia interactions. With

regard to perceptions of the information transmitted - and thus its sensitivity - accurate and appropriate feedback is of utmost importance. However, it is not just feedback and control on *when* information is being transmitted that is required, but *what* is being transmitted. Users often make assumptions about the *Information Receiver* (IR) – e.g. that they know how other participants in a videoconference see them - but such assumptions are often incorrect (Thomas, 1996). Interpersonal distance has, in the past, been found to dictate the intensity of a response: faces in a close-up, for instance, are scrutinized more often than those in the background (Thomas, 1996). Reeves and 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 become an invasive piece of information. Image quality and camera angles may result in a perception of the user, which they regard as inaccurate. It is important that users have feedback on how they are being presented to the IR. Lee, Girgensohn & Schlueter (1997) also highlight the importance of the users ability to control and manipulate the image transmitted.

Finally, what data is captured can affect how invasive the information is perceived to be. Audio in isolation is perceived as significantly more invasive than video only (Adams & Sasse, 1999a). A lack of feedback of who may be listening to the information can result in a rejection of the technology. Smith & Hudson (1995) highlighted how, in an awareness application reviewed, users' lack of IR feedback resulted in the audio channel being rejected for even low sensitivity information.

4.5.2 Social, Organizational and National contexts

There is limited relevant research, but organizational culture has been identified as an important factor (Dourish, 1993; Smith, 1993), whilst some social groups are noted as more at risk of privacy invasion that others (Raab & Bennett, 1998).

5 Multimedia Communication Scenario

To demonstrate how this model can be used to assess the privacy implications of multimedia communications technology in a specific context, a specific usage scenario is evaluated using the model. Although the model can be used as a design tool it is presented here as an evaluation tool for a current multimedia communication application scenario, which actually occurred.

A videoconference seminar was given from a speaker alone in a small London-based office to two audiences: one local (London) and one remote (Glasgow). Both audiences watched the seminar in seminar rooms projected onto a large screen. During the seminar the two audiences either heard audio from the presenter or from the video recording whilst the presenter had all the audio channels open. At the end of the seminar a question and answer session occurred during which all of the audio channels were open.

The audiences had varying degrees of experience with multimedia communication technology, ranging from novice to expert, whilst the presenter was experienced in

multimedia communications. Although the participants within each audience knew each other, they did not know the remote audience or the seminar presenter. Consequently, the seminar presenter knew none of the people watching.

All the screens (both audiences and the presenter) displayed 4 tiled windows of the London audience, Glasgow audience, presenter and Seminar slides / video. PowerPoint slides and a video recording of a previous seminar were used as part of the seminar. The slides were transmitted as a vic stream and the recording was also played out from a VCR through this stream (i.e. the image was switched from the slides to the clip, and then back again). The size of the windows displayed to the audiences (at Glasgow and London) were:

- Presenter — *Common Intermediate Format* (CIF)
- Other Audiences image — CIF
- Viewing their own image — *Thumbnail*
- Slides / video recording — Super CIF

The presenter saw their images on a desktop screen at window size Quarter CIF whilst the two audiences and the slides / video recording were thumbnail images.

5.1 Scenario Privacy Evaluation

This scenario is evaluated for each of the model factors and Issues (see Tables 1,2 & 3) to assess whether the privacy invasion cycle (PIC) could be evoked for some of the participants.

Information Sensitivity (IS)	**PIC user assumptions**	**PIC technology breaches**
IS judgements: System interaction levels distort perception of what is transmitted and its sensitivity	Users could assume the IR is local (IR location is not clearly stated) perceiving the situation as semi-private with local norms (e.g. language, behaviour)	The IR is actually located across the country and may have different perceived norms.
Public / private situation: Although the seminar local images & audio transmitted remotely. Presenter's isolation further distorts situation.		
Primary and secondary levels: Presenter had poor feedback of what the IR received. The degree of media transmitted increased the amount of 2nd information received.	The presenter may assume habits and mannerisms may not be noticeable from the small image feedback they saw.	The IR receives large images where actions are more dramatic and potentially embarrassing.

Table 1: Multimedia scenario evaluated for the *Information Sensitivity.*

Information Receiver (IR)	**PIC user assumptions**	**PIC technology breaches**
Trust levels: Established local audience trust levels for each other may have been at odds with trust in remote viewers.	Users may assume the only IRs are those visible on the screen with associated trust levels.	IRs not on the screen were able to view the session e.g. seminar technicians.
Information Usage (IU)	Users could assume images and audio are only viewed during the seminar.	Images and audio were in reality being recorded and could also be edited and re-used for different purposes at a later date
Current IU: Participants often attend seminars, not mediated by technology, which are not recorded or re-used.		
Later IU: Participants were not advised or given feedback about seminar recordings later IRs or editing.		

Table 2: Multimedia scenario evaluated for the *Information Receiver and Usage.*

User Issues	**PIC user assumptions**	**PIC technology breaches**
Mental models: Poor feedback on technical processes and data transmitted.	Low system interaction levels could produce user assumptions that they are only IRs with a mental model of the scenario as similar to television or cinema.	Video and audio data was captured with two way communication elements which should stimulate a mental model similar to that of the telephone
System interaction: System interaction levels (direct / indirect), varied throughout.		
Context Issues	Audience users could assume as they can only hear the presenter (not the other users) that all the users can only hear the presenter.	The technology transmits more than is relayed to the user. The presenter, can hear audio from both of the audiences
Technology: Poor interface feedback on what information was transmitted and in what context it was received.		
Social grouping / Organisational culture: seminar interaction occurred within a specific context (with associated norms) both in time and location.	Users may assume the context of interaction is understood by the IR (e.g. time of day, environmental conditions – cold, poor lighting etc).	Information broadcaster actions could be mis-interpreted (e.g. shivering, poor concentration) especially when recorded.

Table 3: Multimedia scenario evaluated for the *User and Context* issues.

5.2 Scenario Privacy Recommendations

The evaluated scenario detailed in 5.1 (see Tables 1,2 & 3) has been used as a basis for recommendations to decrease the potential for privacy invasions occurring. It is important to identify exactly what degree of *control* and *feedback* (Bellotti & Sellen, 1993) is required, by whom (*Information Broadcaster / Receiver*) and why.

5.2.1 Briefing Session

- System details: A briefing session should be provided detailing how the system works for novices to establish accurate mental models. They must not be allowed to establish the inaccurate 'television/cinema viewing only' mental model of the system.
- Interaction details: The briefing session should establish clearly how public or private the situation is. What may be clearly public to the designer or technology instigator can be just as clearly private to the user (Adams & Sasse, 1999a). The audience must clearly understand that although they are attending a seminar (with low system interaction levels) they can still be viewed and heard remotely. They must also understand;
    1. When they can be viewed and heard; and
    2. Who the *Information Receiver* is.
- Recording details: Clear notification must be given if the seminar is to be recorded stating who will be able to view or edit it at a later date. Participants should be informed that they can leave if they now wish to not take part.

5.2.2 Interface changes: Information Broadcaster

- Data transmission: Present noticeable feedback on what data (i.e. video, audio) a seminar attendee, or presenter, is broadcasting and receiving. Feedback should also be provided to the presenter of how they are being viewed by the audiences, including the image size.
- Interaction Feedback: Display obvious feedback of who is receiving the data and when. If the receivers are not part of the interaction they should also be detailed. Also show clearly and in an understandable way ('technically related distances' are not acceptable for novices) the *Information Receiver's* current location.
- Recording Feedback: Detail noticeable feedback to the information broadcaster of when transmitted data is also being recorded (e.g. a red light going on with the letters REC underneath)

5.2.3 Interface changes: Information Receiver

- Contextual feedback: It is important for information to be kept within its original context (Dix, 1990; Adams & Sasse, 1999b). People viewing the session remotely or at a later date must be provided with contextual information (e.g. where transmitted from, why, when - time/date stamp)

- Edited data: Edited versions should be clearly marked and links to original versions detailed (Adams & Sasse, 1999b).
- Information handling: Identify if the *Information Receiver* is using the information for the same task as that perceived by the *Information Broadcaster*. Highlight to both acceptable *Information Usage*, e.g. 'for seminar purposes only'

5.2.4 Policy procedures

- Recording permission: Users' permission to record sessions should be obtained where possible. If impractical then feedback to users who are recorded must be provided (see interface issues).
- Changed usage: If the information is to be used for another purpose other than those previously detailed to the user a further permission should be obtained.
- Editing: Any editing - even minor - to recorded multimedia information should have permission obtained from the user and be carefully reviewed for potential *Information Receiver*, *Sensitivity* and *Usage* privacy risks
- Continued privacy evaluation: Assess the usefulness of the information capture against potential risk of privacy invasion to the user. These assessments can save later costly user trade-offs and rejections of the technology e.g. 'I'm not taking part in or presenting a remote seminar'.

6 Discussion and Conclusions

This paper highlights limitations of the current personal information privacy paradigm for multimedia communications. The concept of *personal information* is often employed as an assessment of users' potential privacy worries. However, the majority of multimedia communication is personally identifiable (e.g. user's visual image, email address, name etc) and it would be impractical to treat it all as sensitive information. In contrast, some multimedia environments allow for complete anonymity, which produces the misguided impression that no sensitive information is released and therefore users' privacy is secured. Ultimately, users' privacy perceptions relate strongly to users' misconceptions due to inaccurate social and physical cues and not to a simplistic categorising of the data transmitted. The *privacy invasion cycle* highlights how these inaccurate assumptions can lead to privacy invasions.

This model has mapped all of the relevant elements of users' privacy perceptions so that further research may detail context specific variations. These variations relate, for example, to different domains, tasks, social norms, organisational culture and national & international norms. Indeed, the importance of culture within multimedia communications is an important factor that is woefully under-researched.

In conclusion, not only must we accept the importance of privacy within multimedia communications, but also the significance of users' privacy perceptions. Application designers and organisations considering using multimedia communications must realise that, even though privacy may initially not be an important concern for some users, they will react strongly when they see that it has been invaded (Adams, 2001; Adams & Sasse, 1999a,b). This model details what guides users' perceptions and a theory of the processes behind privacy invasions in order to aid in the development of multimedia applications acceptable to users. There is a need to counteract privacy problems before they arise thus solving them before people lose their trust and emotively reject the technology.

Acknowledgements

We gratefully acknowledge the help of staff in the Department of Computer Science at UCL. This research was originally funded by BT/ESRC CASE studentship S00429637018

References

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

Adams, A (2001) "Users' perceptions of privacy in multimedia communications" Unpublished PhD thesis, school of psychology, University College London.

Adams, A. & Sasse (1999a) "Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie?" In Proceedings of *INTERACT'99* (Edinburgh UK, Sept 1999) IOS Press, 214 - 221

Adams, A. & Sasse (1999b) "Taming the wolf in sheep's clothing: Privacy in multimedia communications" In Proceedings of *Multimedia'99* (Orlando FL, Nov 1999) ACM Press, 101 - 107

Adams, A. & Sasse, M. A. (1999c) "The user is not the enemy". *Communications of the ACM, 40 - 46 (Dec 1999)*

Agre, P.E.(1997) "Beyond the Mirror World: Privacy and the representational Practices of Computing" IN "*Technology and Privacy the New Landscape*" eds. Agre, P. E & Rotenberg, M. 29-62. MIT Press, Mass

Bellotti, V. (1996) "What You Don't Know Can Hurt You: Privacy in Collaborative Computing", *in* M. A. Sasse, R. J. Cunningham & R. L. Winder (eds.), "*People and Computers XI* (Proceedings of HCI'96)", Springer, 241 - 261.

Bellotti, V. & Sellen, A. (1993) Designing of privacy in Ubiquitous computing environments, *in* G. de Michelis, C. Simone & K. Schmidt (eds.), "Proceedings of ECSCW'93, the 3rd European Conference on Computer-Supported Co-operative Work", Kluwer (Academic Press), 77-92.

Bennett, C. (1992) "Regulating Privacy" Cornell University Press. London

Davies, S (1997) "Re-engineering the right to privacy" IN "*Technology and Privacy the New Landscape*" eds. Agre, P. E & Rotenberg, M. MIT Press, Mass, 143-166.

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

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.

Friedman, B; Thomas, J. C. (1999) "Trust me, I'm Accountable: Trust and Accountability Online" in Proceedings (extended abstracts) of *CHI' 99* (Pittsburgh PA, May 1999), ACM Press, 79-80

Goffman, E (1969) "The presentation of self in everyday life" Penguin press, London

Grayson, D. & Coventry, L. (1998) "The effects of visual proxemic information in video mediated communication". *SIGCHI* Bulletin, 30.

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 (CSCS'96),* ACM Press, 67-76.

Lee, A. Girgensohn, A. & Schlueter, K. (1997): "NYNEX Portholes: Initial user reactions and redesign implications." In S. C. Hayne & W. Prinz (eds.), *Proceedings of International ACM SIGGROUP Conference on Supporting Group Work*, GROUP'97, ACM Press, 385-394.

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

Norman, D. A (1986) "Cognitive Engineering" in Norman, D. A & Draper, S. W (1986) Eds. "User Centred System Design: New Perspectives on Human-Computer Interaction" Lawrence Erlbaum Associated, New Jersey.

Raab, C. D & Bennet, C. J (1998) "The Distribution of Privacy Risks: Who Needs Protection ?" *the Information Society* 14(4) 253-262

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.

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

Smith, I & Hudson, S. E (1995) "Low disturbance audio for awareness and privacy in media space applications" In Proceedings of *Multimedia'95* (San Francisco CA, Nov 1995) ACM Press91-97

Stevenson, C. & Cooper, N. (1997) "Qualitative and Quantitative research." *The Psychologist: Bulletin of the British Psychological Society*, April. 159-160

Strauss, A. & Corbin, J. (1990) "Basics of qualitative research: grounded theory procedures and techniques" Sage, Newbury Park.

Thomas, J. C. (1996) "The long term social implications of new information technology." In R. Dholakia, N. Mundorf, & N. Dholakia (eds.), New Infotainments Technologies in the Home: Demand Side Perspectives. Lawrence Erlbaum, Hillsdale, NJ, 1996

Wacks, R (1989), "Personal Information: Privacy and the Law" Oxford Press. Clarendon