Multimedia Information Changes the Whole Privacy Ballgame

Anne Adams
Computer Science Dept
Middlesex University
Bounds Green, London. UK. N11 2NQ
A.Adams@mdx.ac.uk

Global multimedia communications is advancing the freedom of information and knowledge. However, as the amount and variety of multimedia data generated through these applications increases, so do risks associated with widespread accessibility and utilization of such data. Specifically, data may be used in a manner which users regard as an invasion of their privacy. The relationship between multimedia data and privacy invasion has not yet been clearly described. The main problem is that current approaches to privacy define characteristics of the data and thus information, rather than *how it is perceived* by the users (Davies, 1997). Three years of research within this field have, however, identified that previous approaches to privacy protection are not addressing the real problems in this field. Most multimedia invasions of privacy are not intentional or malicious; rather, the designers failed to anticipate how the data could be used, by whom, and how this might affect users (Adams, 1999a & b; 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. Trade-offs users make, thus rendering some privacy risks acceptable are also identified. The model can assist designers and organizations utilizing multimedia communications to assess privacy implications, and thus develop mechanisms for acceptable use of the technology.

1. The importance of users' perceptions

It has been argued that there are many inalienable privacy rights which should never be disregarded when developing systems (Davies, 1997). Similarly it is also maintained that privacy experts understand potential privacy risks at a greater depth than users (Bennett, 1997). Both these arguments have directed privacy research and identification of privacy requirements in system development towards appraisals by privacy advocates. The problem with *only* taking this approach is that any expert may have a distorted perception of a situation and potential privacy risks that do not reflect the perceptions of those whose privacy needs protecting. Inaccurate assumptions are a major cause of unintentional invasions of privacy (Adams, 1999b; Adams & Sasse, 1999a/b).

Previous research (Adams & Sasse, 1999a) has highlighted how system designers, policy makers and organizations can easily become isolated from users' perceptions of environments and privacy risks. Differing situation perceptions resulted in a serious invasion of privacy and a retrospective over-reactive departmental policy devised to calm the situation. In this scenario the technology instigators had considered the use of a web-camera in a specific situation as applicable. However, they were later identified as having mis-interpreted the situation as being public while the majority of users perceived it as a private / semi-private situation. Key to the camera implentors distorted assumptions was their familiarity with the environmental tools and thus their sense of control over the technology. These differences in perceptions may have already existed within the department in question. 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 organizations to assess how the relationship between organizational *control* and *trust* affects users' privacy. Trust is undermined if users are not allowed to judge trade-offs for themselves or feel part of the proposed solution.

Ultimately privacy, as with trust, is reliant on our perception of it. It is not necessarily important how private or safe we are (although this is a vital component) but whether we perceive ourselves to be safe and private. Over recent years the importance of the users perceptions has been identified with a move to increase perceptions of privacy. These 'semantic cueing mechanisms' (e.g trust badges, opting-in vs. opting-out), however, rely on accurate appraisals of users' perceptions of privacy. If policies are based on inaccurate users' privacy perceptions they will not address users' current and future fears and may complicate further issues. Therefore identifying users' perceptions of privacy is an important element in both distinguishing what needs to be protected and how best to protect it.

Empirical research into users' privacy perceptions is very limited. National opinion polls (off-line and on-line questionnaires) have sought to capture users' perceptions to help direct privacy protection advancements. However, the results from these surveys have done little more than identify the importance of computer privacy for users (Harris & Westin, 1998) and have substantiated privacy advocates perceptions of data usage. The cause of these limitations has its roots in the constraints of using a questionnaire approach with a complex, previously under-research phenomena such as computer privacy. Recent questionnaires have sought to delve more into the specifics of users' data / information perceptions (Cranor et al 1999). However, with the fast changing nature of computer technology potential privacy problems are often not recognized until they occur. Within the fast changing field of multimedia communications a need to keep ahead of potential privacy problems has led to an increase in privacy research based on anecdotal findings (Harrison & Dourish, 1996; Bellotti & Sellen, 1993; Mackay, 1994). This approach may uncover some important issues but without a holistic appraisal it may only highlight idiosyncratic problems particular to specific situations and organisational cultures (Dourish, 1993).

2. Multimedia data privacy implications are often overlooked

When starting my research into privacy in multimedia communications my first stop was to attend the computer freedom and privacy conference of 1997. I quickly realised that privacy was not approached with regard to this data type. In fact this was the first and only conference I have attended where sessions were not only video recorded but also copies were sold after the session without any clear prior notification of either actions to attendees. Organisers could have considered that as presenters were informed and accepted / rejected these conditions, that privacy protection has been conformed to. However there are three major problems with these frequently made assumptions. Firstly users rarely understand potential privacy risks that are heightened within multimedia data.

Previous research has identified that multimedia data has two privacy levels within it. The primary level[1] relates to the actual information being broadcast (topic of conversation etc.) whilst the

secondary level relays the social/psychological characteristics of the data being broadcast. These characteristics often define and personally represent the user in a particular way increasing potential invasiveness of this information. Privacy problems often arise when only the information's primary level is reviewed for potential privacy risks. With different types of data different amounts of secondary level information are relayed: -

text textual cues : the way things are presented, abusive language used etc.
audio verbal cues : tone of voice, accent / dialect
Video visual cues : dress & look of user, mannerisms of the user etc.

Multimedia information therefor increases the amount of secondary level information released (an email debate will not show how emotional and loud you got in a debate like a conference recording). Research into conference session recordings (Adams & Sasse, 1999b) has identified that those interviewed often rated the sensitivity of multimedia session data on the basis of its technical content (primary level). However, users noted that the recorded sessions were invasive if they were viewed, at their secondary level such as: -

i) As an educational tool in how not to present at a conference
ii) As a research resource to evaluate how people from different ethnic backgrounds act and react in an argument

A second issue relating to the acceptability of multimedia data capture and usage is that users' perceptions are often reliant on implicit assumptions. If these assumptions are not fully understood they can be broken, easily and unintentionally. Previous research (Adams & Sasse, 1999b) has highlighted that although conference presenters were initially happy with session recording this was based on implicit assumptions about the information sensitivity, who would receive it (information receiver) and what it would be used for (information usage). When conference organisers decided to broadcast sessions on an internal hotel television network they breached users assumptions. For most of those interviewed, the benefits of transmitting sessions for within-community members who cannot attend the conference outweighed potential risks associated with sessions being viewed by *outsiders*. However the same trade-off did not apply to the hotel transmission of sessions. It is important to understand privacy trade-offs so that the privacy effects of changing circumstances can be assessed prior to users loosing their trust in the organisation.

Finally, the data recorded in conference sessions is rarely isolated to presenters (or even those asking questions). In my findings (Adams & Sasse, 1999b) of conference remote viewing I identified an example where cameras frequently panned the conference session to give a feel of the surroundings. The cameramen had decided that hundreds of people were viewing the attendees so more people viewing them remotely would not be more invasive. However, the attendees in the real world situation could see who was watching them or not whereas when this situation was made virtual there was no awareness of who was watching. One attendee, who fell asleep in a multicast session, found this out to his cost when his employer (viewing remotely) later reprimanded him for sleeping while attending a conference they had paid to send him to. Attendees noted that recording sessions they attended without their awareness to be highly invasive. Others noted that recording sessions dissuaded them from asking questions in sessions.

3. Need for a multimedia communications privacy model

Without a clearly defined negative outcome from not ensuring users multimedia privacy there is little incentive for organizations with regard to these issues. Also, without detailed accounts of users' privacy boundaries and levels of multimedia data importance, there is little guidance on how to devise privacy protection mechanisms. Until a validated account of users' perceptions is identified and detailed with some accuracy there will be little movement by organizations in ensuring multimedia

communication privacy. There is, therefore, an obvious need to identify a model of salient factors that determines perceived privacy invasions.

3.1 Users' perception privacy model in multimedia communications

A model (Diagram 1) of **users' perceptions** within multimedia communications has been developed based on three years research (Adams, 1999a / b; Adams & Sasse, 1999a / b) using social science grounded theory methods (Strauss & Corbin, 1990). It is important to note that this model is an abstract representation of important factors which will change value with the context (e.g Context1: IU > IS or IR, Context2: IR > IU or IS). Similarly, each *factor* can change the importance of another factor (e.g. Context3: IU & thus IS > IR).

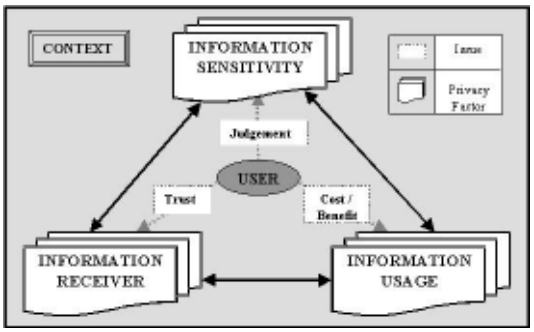

Diagram 1: Users' perceptions privacy model summary

This model presents the *User*[2] as the person who has data transmitted either directly (Primary information - their work achievements, consumption habits, medical records etc.) or indirectly (2nd information - their image, voice or writings) about themselves. 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). The model (diagram.1) has identified 3 major privacy factors (*Information Sensitivity*, *Receiver* & *Usage*) that are key to users' perceptions of privacy. Each of the privacy factors interacts with each other to form the users' overall perception of privacy. Within different scenario's one factor will be more important that the others although all factors will have a bearing of the overall privacy perception.

3.2 Factor summary

3.1.1 Information Sensitivity

Primary to this model is the privacy factor *Information Sensitivity* (IS) and the effect that the other privacy factors identified have on perceived sensitivity levels. It is important to understand that information sensitivity, as with privacy, relates to the users' perceptions of the data being transmitted thus interpreting the data as information. There are two further points to make about information sensitivity: firstly it is reliant on the users' judgements of the sensitivity levels of the information being broadcast and secondly that sensitivity levels are not binary (private / not private) but dimensional with degrees of sensitivity. See design recommendations in Table 1.

3.1.2 Information Receiver

The *Information Receiver* (IR) is the users' perception of the person (not necessarily the actual person) who receives and / or manipulates their data. A range of issues will influence the users' assessment of the information receiver, however *trust* (often based on relationships and information roles) is an important issue in the users information receiver perceptions. See design recommendations in Table 1.

3.1.3 Information Usage

Finally *Information Usage* (IU) relates to the user's perception of how and what their transmitted data is used for during data exchange and at a later date. The importance that the user attributes to the perceived usage is key in privacy risk / benefit trade-offs that are made. Ultimately privacy is set within its surroundings and therefore the user's perception of the context within which multimedia communications occur - specifically the technology, social groupings and national / international settings - are summarised in the model. See design recommendations in Table 1.

3.2 Conclusions

Ultimately there are many complex privacy problems that arise from multimedia data usage and yet there is little privacy research or protection within this field. From my privacy research there also appears to be a common misconception that, as multimedia data identifies the user, by accepting its usage, users accept a complete loss of privacy. However, all of my research has highlighted that this is not the case and that acceptable data capture is always reliant on users' implicit assumptions. This research has also identified that there are many solutions to potential privacy problems that can be dealt with by privacy mechanisms. However, there are some serious re-adjustments to the current approach to privacy that must be made before effective mechanisms within this domain can be devised.

The technical and military style bias towards security of many security departments has been commented on as a narrow perspective which has produced security mechanisms which are, in practice, less effective than they are generally assumed to be (Davis & Price, 1987; Hitchings, 1995). Previous research (Adams et al, 1997; Adams & Sasse, 1999c) has highlighted how this authoritarian approach has led to security departments' reluctance to communicate with users with regard to work practices and user requirements. This approach does not fit with modern distributed and networked organizations, which depend on communication and collaboration. However, because of the 'enemy within' security culture of many organisations, user feedback is hard to administer. (Adams et al, 1997; Adams & Sasse, 1999c). The present privacy paradigm of privacy protection being devised for the individual against a malicious invasion of privacy, highlights the adversarial nature of the security domain. However, most of my research has highlighted that socially unacceptable behaviours can be stumbled across by a lack of cues to the user and the information receiver isolating them from the social norms of acceptable behaviour for that specific situation. Often this is caused by poor interface design but also by misconceptions of user perceptions by organisations and system designers. As privacy perceptions are complicated and multimedia communications often defy real world assumptions there is a vital need to keep in tune with users' perceptions within these environments.

User feedback / control	
Usage awareness / feedback and control	(1) Identify user awareness of multimedia data capture, recording and later usage. (2)Inform users if they are unaware of these factors along with benefits and potential privacy threats so accurate trade-offs can be made. (3)Obtain user permission (where possible) to record. If impractical then provide feedback to users that they are being recorded. (4)If the data is to be edited or used for another purpose than those previously detailed to the user a further permission should be obtained or feedback on re-usage /editing provided.
Feedback on the information receiver	(1)Identify who the user believes the information receiver to be and how public they believe the situation is. (2)Notify the user immediately if data is transmitted (either currently or at a later date) to people that the user had not envisioned. (3)Provide feedback and control to the user (& IR) on the person(s) to whom the data is transmitted. Include (in an understandable way) the distance the receiver is from the user (physical & organisational) thus allowing users to accurately assess interaction privacy risks.
feedback on data received	Provide feedback to the user on what images & audio the information receiver will be intercepting (e.g. degree of distortion)
Users IR trust appraisal for data release:	Trust mechanisms, which help determine data transmission procedures, should not relate to trust as a linear factor (e.g. highly trusted people allowed access to highly sensitive information). Trust is a highly complex phenomena which relates to the sensitivity of the information and the information receiver's role in that information usage as well as the context of usage etc.
Information Receiver Feedback	
IR sensitivity feedback	(1)Identify what the users rate the information sensitivity levels at. (2)Provide feedback to the IR of users' perceived information sensitivity levels + acceptable / unacceptable information usage both currently and at a later date.
Data context for IR	(1)Provide context for the data (e.g transmission source, why and when transmitted). Time and date stamp recorded multimedia data so it can be viewed within a temporal context. (2)Edited data should be clearly marked with links to original full versions provided. For highly sensitive information digital watermarking and watercasting should be considered - copying and editing of multimedia data can then be traced. It would be ideal if this action was automated to save the user trawling through information trying to find if their data is on public display somewhere.

Diagram 4: A summary of multimedia design recommendations based on the privacy model

ACKNOWLEDGEMENTS

I gratefully acknowledge the help and support of my Ph.D. Supervisors Angela Sasse and Peter Lunt as well as other UCL colleagues. This project is funded by a British Telecom / ESRC CASE studentship S00429637018.

REFERENCES

Adams, A. (1999a) "Users' perception of privacy in multimedia communication" *in Proceedings (Extended Abstracts) of CHI' 99,* Pittsburgh.

Adams, A. (1999b) "The Implications of Users' Privacy Perception on Communication and Information Privacy Policies" *in Proceedings of Telecommunications Policy Research Conference, Washington DC.*

Adams, A., Sasse, M. A. & Lunt, P. (1997) "Making passwords secure and usable" *in* "*People & Computers XII* (proceedings of HCI'97)" Springer, pp. 1-19.

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

Adams, A. & Sasse, M. A (1999b) "Taming the wolf in sheep's clothing: privacy in multimedia communications" *in Proceedings of multimedia' 99,* Orlando.

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

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* , Kluwer (Academic Press), 77-92.

Bennett, C (1997) "Convergence revisited: towards a global policy for the protection of personal data" IN "*Technology and Privacy the New Landscape*" eds. Agre, P. E & Rotenberg, M. pp 99-123. MIT Press, Mass

Cranor, L. F., Reagle, J & Ackerman, M. S (1999) "Beyond concern: understanding net users' attitudes about online privacy" In Proceedings of the Telecommunications Policy Research Conference; http://www.research.att.com/library/trs/TRs/99/99.4/99.4/99.4/

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

Davis, D. & Price, W. (1987) "Security for Computer Networks". John Wiley & Sons, Chichester.

Dourish, P. (1993) 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.

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.

Hitchings, J. (1995) "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology". *Computers & Security*, 14, 377-383.

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

Harris, L. & Associates and Westin, A. F (1998) "E-commerce & Privacy: What Net Users Want. Hakensack, NJ; Privacy and American Business.

[1] 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, person finance information etc.

[2] The HCI equivalent is the system end-user whereas political scientists would say the data subject.