Users' Perception of Privacy in Multimedia Communication

Anne Adams
Department of Computer Science
University College London
Gower Street, London, WC1E 6BT
+44 (0)171 419 3462
A.Adams@cs.ucl.ac.uk

ABSTRACT
Perceived infringements of privacy can cause breakdowns in technologically mediated interactions, leading to user rejection of the technology. This research aims to identify the impact that users' perception of privacy has on their attitudes to, and behavior within, multimedia communication environments. Using both qualitative and quantitative data from various multimedia communication settings, 3 major factors have been identified (*Information Sensitivity*, *Receiver* & *Usage*) and integrated into a framework. In addition, a mismatch between *perceived* and *actual* privacy risks has been identified, which increases perceived invasions of privacy and produces negative emotive responses.

Keywords
Privacy, Multimedia Communications, Grounded Theory

INTRODUCTION
Multimedia communication systems - such as videoconferencing - are becoming ubiquitous, and their use generates a wealth of multimedia data. Facilities for accessing and using such data increase associated privacy risks. However, to define privacy adequately, it must be understood that it is an inter-disciplinary phenomenon varying across *context of use*, users' *roles*, social and organizational *norms* [3,6]. The aim of this research is to identify limitations, which if breached, cause user resentment and rejection of such systems. Once these limitation are identified and mapped, appropriate organizational behavior and mechanisms can be integrated into organizational policies and strategies for securing privacy.

Information Sensitivity
Initial research [1,2] has shown that users' labeling of information as "sensitive" or "private" is vital to how that information is reviewed and maintained. Current research has also identified that in multimedia communications, there are two levels of information relayed. *Primary* information relating to the topic of discussion, whilst *secondary* information relays other interpretative social/psychological characteristics about the user via visual, auditory or textural mediums.

Information Receiver
Additional complexity arises from the fact that privacy can be invaded without users being aware of it [4]. This highlights an additional issue of whether it is *what is known* about a person that is invasive or *who knows* it. This research has clearly identified the role of the *information receiver* within the privacy framework. Privacy risks associated with the information receiver, such as *vulnerability* and *trust*, restrict self-expression and personal development.

Information Usage
Finally users' fears of technology are said to relate to the use to which information is ultimately put [3]. It has been suggested that a lack of contextual elements in processing and usage may be a key factor in privacy invasion [5]. One answer to these fears is to improve users' *control* and *feedback* in design considerations [3,4]. However, this approach does not regulate information that is initially perceived as innocuous, but is potentially invasive. This research has ascertained interactions between the perceived *information sensitivity* and its potential *receiver*, which make later usage acceptable or unacceptable.

RESEARCH APPROACH
The key privacy factors previously identified (*Information Sensitivity*, *Receiver & Usage*) were validated with users of 4 multimedia communication system:

- 9 Ph.D. students at universities in the UK appraised a prototype virtual reality system through a focus group. The system was introduced as a potential information exchange aid to participants whose multimedia communications knowledge varied from novices to experienced users. High system immersion levels were ascertained with conscious in-group surveillance knowledge.
- 35 undergraduate students at UCL used a videoconferencing system for interactive sessions with each other and a tutor throughout an 8-week network

communications course. A series of focus groups throughout the course assessed system privacy implications. Participants were initially novice users with high system immersion levels and conscious in-group surveillance knowledge.

- 46 UCL staff responded to a quantitative/qualitative questionnaire evaluating a video surveillance device positioned in a common room. Participants had low immersion levels in the system and most were without conscious surveillance knowledge or official consent to surveillance.
- 24 attendees at a conference that was multicast on the Mbone were interviewed in-depth. Participants were expert users with varied system immersion levels and conscious in-group surveillance knowledge.

Grounded theory methods were used to analyze the data collected and integrate the findings [7]. This will allow for the amalgamation of both rich qualitative and precise quantitative data.

RESULTS

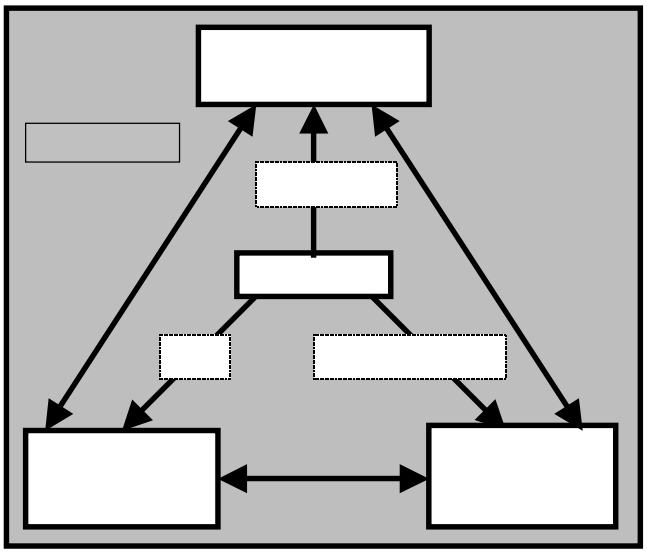
Information Sensitivity: Potential privacy invasions were found to be produced by unaccounted-for privacy risks associated with secondary information (see introduction). E.G discussions of technical coursework via videoconferencing initially perceived as impersonal and non-invasive were later realized to be potentially invasive via a users knowledge of the coursework (or lack of it).

Information Receiver: Interactions have been identified, between the type of information released and the privacy risks associated with the person receiving it. Some of the findings are counter-intuitive: someone who is personally well known to the user may incur higher privacy risks than a complete stranger. E.g. users may not mind someone a million miles away from you knowing details of their eating habits but a friend (who can make personal judgements that effect them) knowing the same information may be invasive.

Information Usage: The major issue to surface is the lack of awareness of potential privacy risks via later information usage. Once realized, however, users' reactions are emotive and intractable. However, when potential privacy risks and benefits are highlighted prior to disclosure a rationed trade-off is often made.

SUMMARY

- Perceived invasive behavior has been identified as related to the mismatch between users' perceptions of privacy risks and their realization of actual privacy risks. Privacy factor interactions have been found to be the result of cost-benefit evaluation determined by users' perception of risk assessments.
- A critical limit in privacy perceptions has been identified which, when exceeded, produces negative emotive user responses and a rejection of technology.



ACKNOWLEDGMENTS

I gratefully acknowledge my supervisor Angela Sasse, UCL colleagues and my sponsors at BT.

REFERENCES

1. Adams, A., Sasse, M. A. & Lunt, P. (1997) "Making passwords secure and usable" *in* H. Thimbleby, B. O'conaill & P. Thomas (eds.), "*People & Computers XII* (proceedings of HCI'97)" Springer, pp. 1-19.
2. Adams, A., Sasse, M. A. (In Press) "The user is not the enemy". *Communications of the ACM.*
3. 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), pp.77-92.
4. 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, pp. 241 - 261.
5. Dix, A. (1990) "Information processing, context and privacy" *Proceedings of INTERACT'90*, North-Holland. pp. 15-20
6. Schoeman, F. D. (1992) "Privacy and Social Freedom" Cambridge university press.
7. Strauss, A. & Corbin, J. (1990) "Basics of qualitative research: grounded theory procedures and techniques" Sage, Newbury Park.