Privacy in Collaborative Multimedia Environments

Jeremy Pitt

Intelligent and Interactive Systems, Department of Electrical & Electronic Engineering
Imperial College of Science, Technology & Medicine, Exhibition Road, London, SW7 2BT, UK
Tel: +44 (0)20 7594 6318 Email: j.pitt@ic.ac.uk URL: http://www.iis.ee.ic.ac.uk/jeremy

Angela Sasse

Multimedia and Usability, 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

EXTENDED ABSTRACT

Topics Addressed. *2: Watermarking, Rights Management; 5: Distributed Intelligence; 6: Models for Commerce and Industry; 9: Social Aspects of Media (Privacy).*

This research reported in this paper is motivated by the increased complexity, proliferation and commercial value of digital multimedia information. This has been fuelled by three emerging trends. Firstly, on the users' side, technological developments have facilitated creating personal multimedia and distributing this information (MIME enabled mailers, personal web pages, etc.). Secondly, on the broadcasters' side, further technological developments (e.g. IP multicast, MP3 audio, computing-telephony-TV convergence) and deregulation of markets have altered business strategies to focus on service-oriented operations. Thirdly, there is increasing awareness of the utility of information: for users, the potential buying power of their profiles; for content providers, the mass audience that can be reached – but which can be compromised by audio- and video-piracy and internet ubiquity.

These developments require that management of personal information needs to be tailored to individuals and adaptive over time, while management of multicast and broadcast information needs to be targeted to appropriate groups and responsive to needs. Both information types need protection from unauthorised or inappropriate access and use. This management of multimedia – personalised, adaptive, pro-active and selective – for the purposes of achieving privacy, security and identity can be achieved by agents and multi-agent systems. Many communications organizations have recognised that agent-based technology appears to offer a timely solution to the demonstrable multimedia application pull, e.g. for video-on-demand, Internet TV, etc.

However, the increasing availability and accessibility of multimedia data generated by such high-bandwidth multicast applications harbours new and increased risks as well as benefits for users (Bellotti, 1997). Users may be less conscious of the risk that these applications pose to their privacy than they are with more "upfront" surveillance devices (Davies, 1997), but when invasions of privacy do occur, users lose trust in the technology that afforded the invasion and reject it (Adams & Sasse, 1999a). Moreover, users have been shown to lose trust in the organisation that introduced or sponsored the technology (Adams & Sasse, 1999b). The damage caused by media reporting of security loopholes and 'denial of service' attacks, mean that a company which relies on customer trust must consider the overall, long-term damage from applications or services that do not adequately consider and protect users' privacy. Publicised invasions of privacy could trigger panic-driven large-scale opt-out by users, or calls for simplistic regulations which stop the distribution of such data altogether. There is a need for privacy mechanisms that protect privacy adequately while allowing the exchange of multimedia data that is mutually beneficial to both data originators and the data users (Brin, 1998).

Yet, there is currently no body of knowledge that designers of such applications, or organisations considering introduction of such technology, can draw on. There is a plethora of literature examining technical and legal aspects of privacy. The technical perspective, however, tends to focus on preventing unauthorized access to data through authentication and cryptography (e.g. Garfinkel & Spafford, 1996), or hiding users identity altogether behind anonymising mechanisms. The legal community and the regulatory bodies seem, as Raab & Bennett (1998) point out, more cognisant of the needs of *data users* (such as government and commercial organisations) than the needs of *data subjects*. There is much sociology and social psychology knowledge to inform our

understanding of the individual, society and privacy (*e.g.* Schoemann, 1992), but it does not address the specific issues of multimedia data and communication.

We therefore propose a hybrid approach which combines a user-centred privacy model witthe logical distribution of responsibility and control to agents representing individuals and organizations provides a 'higher level' approach to ensuring privacy by policy, which builds on conventional authentication techniques. In particular, the full paper describes an approach based on:

1. The implementation of a user-centred privacy model (Adams and Sasse, 1999a), which …
2. … enables users to specify usage policies and access rights to their multimedia data, according to the information receiver, sensitivity and usage, that …
3. … can be watermarked (in real-time for streamed multimedia), survive compression and lossy transmission, so that …
4. … it can be interpreted on a per user per multimedia object basis by agents operating in a general peer-to-peer computing infrastructure, which …
5. … is supporting collaborative multimedia environments that are based on new commercial models for audio and video transmission (Chiariglione, 1999).

We propose that this model will support the move towards what we call the *Information Trading Economy* of future distributed intelligent information systems (Pitt et al, to appear), rudimentary forms of which are Napster (http://www.napster.com) and Gnutella (http://gnutella.wego.com). We propose that information is a commodity, but in its electronic form, to maximise utility it will be traded not sold, and more likely to be pushed rather than pulled (i.e. users will trade profile information for content in 'client-server' transactions, and exchange content in 'peer-peer' transactions). In this case, content providers will provide a 'broadcaster' (i.e. portals with content in return for cash. However, a broadcaster will not actually broadcast but instead content can actively targeted at and tailored for a particular user, who will pay for it with their user profile. Consumers will access content (in exchange for profile information) and invoke some services that may be free at the point of access. Other services will be offered by third-party service providers who will pay for having services hosted, but will also charge. In this way, we can envisage that the possibly unlimited number of business models identified by Chiariglione (1999) for digital audio and video services can be realised (e.g. pay on receipt, pay on approval, pay per view, subscription, rental, rent-to-buy, etc.).

We conclude that this synthesis of: (1) privacy research from Human-Computer Interaction; (2) watermarking and coding techniques from multimedia communications; and (3) agent intelligence and peer-to-peer computing from Artificial Intelligence and Distributed Computing, when combined with new business models, provide the foundations for building a range of agent-mediated applications. The resulting synergy enables the potential for broadband communication to be exploited while the rights of the owners of the content can be protected.

REFERENCES

A. Adams & M. A. Sasse (1999a): Taming the Wolf in Sheep's Clothing: Privacy in multimedia communications. *Proceedings of ACM Multimedia'99*, Orlando, Florida.

A. Adams & M. A. Sasse (1999b): Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, Or Let Them Lie? In M. A. Sasse & C. Johnson [Eds.]: *Proceedings INTERACT '99*, Edinburgh, pp 214-221. IOS.

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

L. Chiariglione (1999): Beyond Digital Audio and Video. Presentation at Imperial College of Science, Technology & Medicine, 1999.

D. Brin (1998): The Transparent Society. Addison-Wesley.

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

S. Garfinkel & G. Spafford (1996): *Practical Unix and Internet Security*. 2nd edition. O'Reilly & Associates.

E. Mamdani, J.V. Pitt & K. Stathis (1999): Connected communities from the Standpoint of Multi-Agent Systems. *New Generation Computing*, 17(4), pp381–393.

J.V. Pitt, E. Mamdani & P. Charlton (1999): The Open Agent Society and Its Enemies. *Journal of Telematics and Informatics*, to appear (2001).

C. D. Raab & C. J. Bennett (1998): The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14, 263-274.

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