# Privacy Issues in Computer-Mediated Communication

**Daniel Salber**

*LGI-IMAG, University of Grenoble*

*BP 53*

*38041 Grenoble Cedex 9*

*FRANCE*

*E-mail: daniel.salber@imag.fr*

## Introduction

For the last few years, the use of computers has been expanding from traditional computing tasks to communication tasks. The advent of sophisticated audio and video capabilities, the rapid development of fast and cheap computer networks make it possible to turn the computer into a powerful communication tool. This new communication tool is far superior to paper or even the telephone: it's fast, ubiquitous (with the recent developments of personal digital assistants), and makes the long-rumoured videophone a reality. However, these new communication techniques also bring up serious ethical issues. Some of these issues were already present in text-based computer-mediated communication such as e-mail and have been adressed by various means. But the use of audio and video tends to exacerbate these problems or bring up new ones. This paper focuses on privacy issues that arise when designing or using advanced computer-mediated communication facilities: we first assess some of these issues and then propose a property of communication systems that guarantees system support for privacy.

## Privacy in computer-mediated communication systems

Desktop videoconferencing is now commercially available. It is mostly used for formal and focused conversations, much like traditional meetings. Research done on MediaSpace systems shows possible future directions for the use of audio video communication tools. MediaSpace systems, pioneered by Xerox at PARC and EuroPARC, along with the University of Toronto, are computer-controlled audio video settings that allow people within a workgroup to communicate. A MediaSpace usually relies on a local audio video network and is similar to a local area network for file sharing: it is always available and its use is free.

These systems have been used by researchers to investigate novel uses of audio video communication. But they have also used different approaches for privacy protection. For instance, EuroPARC's RAVE [Gaver 1992] and Toronto's CAVECAT [Mantei 1991] MediaSpaces offer a *glance* connection in addition to traditional videophone connections: the *glance* connection is a very short one-way video-only connection. It allows the caller to litterally glance at the callee. The system provides users with a feedback mechanism, for example in the form of an audio message: whenever a user is glanced at, s/he hears the sound of an opening door, followed by the spoken name of the glancing user, then the sound of a closing door.

The system also provides users with access control: in the RAVE system, a user can allow or forbid glance access to any user in the group. Access control here is *prescriptive*: it is enforced by the system according to settings determined by the user. There is no way for an unauthorized user to perform a glance connection. In the CAVECAT system on another hand, access control is *indicative*: each user can set his/her level of availability. It is then shown to other users as a door icon: the door can be open, ajar, closed or barred. But this setting is just a social cue and its meaning is not known to the system. Even if a user has set a low availability level (door closed or barred), incoming connections to this user are possible.

These two different approaches to access control illustrate a well-known concept in multi-user interaction: the dichotomy between technical and social control. In computer-mediated communication systems (and in CSCW systems as well), control of interactions between users can rely on social rules or can be delegated to the system. In both these approaches, how can we assess that users privacy is or isn't at risk? As [Gaver 1992] emphasizes, MediaSpace systems so far are used by researchers who know each other well and trust each other. One could wonder about the use of the same system in a "real-world" setting. Even if, as argued by [Bruckman 1994], we prefer to "try social solutions first, and if they fail, fall back to technical solutions", we feel the need to define properties of a system that would help guarantee privacy.

# A property for privacy protection

Based on the assessment of existing MediaSpace installations, as well as on our experience with VideoPort, our own MediaSpace system [Salber 1994] , we propose a property as a first approach to privacy protection in computer-mediated communication. Properties are provable and verifiable characteristics of interactive systems. They help assess design options in the design process of a system. Although a consistent set of properties has been devised for single-user interactive systems [Abowd 1992] there are few properties that specifically address multi-user or computer-mediated communication systems and none that address privacy. We show how to refine the observability property to take privacy into account.

The *observability* property for single-user systems asserts that states of the system that are relevant to the interaction between the user and the system must be made perceivable to the user. In other words, the system shouldn't leave the user "in the dark". This property can be adapted to ensure privacy in computer-mediated communication. However, in computer-mediated communication systems, the system is no more well-defined as in single-user systems. For a given user, should we consider the system as the one running on the local workstation of the user, or as the whole set of connected workstations? Actually, considering the local system is not enough since information such as the availability of the user may be gathered on a remote server. Considering the whole system may be too much: making any user aware of system states of other workstations could mean other risks to privacy: any user could be aware of connections between third parties.

Instead of referring to states of the system, we feel more relevant to refer to information that is made available about a user. This information can be seen as “being published” by a user. It can consist of user-defined settings (such as availability), or live audio and video of the user (when engaged in a connection) or even be provided by the system (such as login time). In any case, the user must have the choice to publish this information or not and he must also be made aware by the system that this information is accessible to other users. The user must also be able to know who accesses this information. Thus, we can refine the observability property for computer-mediated communication systems as: the user must be able to choose what information about her/himself is made available to others; the system must make perceivable to the user what information about her/himself is available to other users. Access to this information by other users must be made perceivable to the user.

The RAVE and CAVECAT systems almost conform to this property: the system makes perceivable to users what is available to other users (e.g., a user’s own availability level is always displayed on the user’s own screen), and with audio feedback, incoming glance connections are made perceivable. But the user doesn’t have the choice of what will be made available to other users: for example, a glance connection always provides the caller with a video image. There is no system support to let the callee block video and provide an audio glance or a text message instead. One can also note that the Unix `finger` command, which serves a similar goal as the glance connection and has similar potential privacy risks, fully conforms to this property: the user decides what will be available through `finger`, he can know what is actually available (by doing a `finger` on her/his own account), and he can also know if s/he’s has been fingered. On another hand, the CU-SeeMe videoconferencing system [Cornell University 1995] doesn’t conform to our property: users in a videoconference may not know that a new user has arrived and is able to see them, except if they have chosen the “Show All Participants” option.

# Conclusion

Computer-mediated communication use relies on both technical means and social rules. Social rules may be constrained by technical means that enforce a given policy of use. Privacy is one such example: to allow wide acceptance and use of computer-mediated communication systems, these systems must guarantee privacy protection. With this aim in mind, we have proposed an extension of the observability property. This new property must be assessed with regard to various settings. We find it valuable for MediaSpace-like systems that have a limited number of identified users. Other settings with e.g., wider networks or anonymous users, such as the MediaSpace/World-Wide Web interface [LRI 1994] could possibly question this property. Finally, assessment of this property with various groups of users and input from social sciences researchers would certainly be valuable.

# Acknowledgements

Our thanks go to members of the GDR-PRC GT-SCOOP research group for interesting and fruitful discussions. We also thank the ESPRIT BRA 7040 AMODEUS project.

# References

[Abowd 1992] G. D. Abowd, J. Coutaz and L. Nigay. *Structuring the Space of Interactive System Properties*. IFIP Conference on Engineering for Human-Computer Interaction, Ellivuori, Finland, 1992.

[Bruckman 1994] A. Bruckman. *CHI'94 Panel on Approaches to Managing Deviant Behavior in Virtual Communities* 1994.

[Cornell University 1995] Cornell University. *CU-SeeMe* 1995.

[Gaver 1992] W. Gaver, T. Moran, A. MacLean, L. Lövstrand, P. Dourish, K. Carter and W. Buxton. *Realizing a Video Environment: EuroPARC's RAVE System*. CHI'92 Conference on Human Factors in Computing Systems, Monterey, CA, 1992.

[LRI 1994] LRI. *MediaSpace-WWW interface (http://www-ihm.lri.fr)* 1994.

[Mantei 1991] M. Mantei, R. M. Backer, A. Sellen, W. Buxton, T. Milligan and B. Wellman. *Experiences in the use of a Media Space*. CHI'91 Conference on Human Factors in Computing Systems, New Orleans, 1991.

[Salber 1994] D. Salber and J. Coutaz. *Fenêtres sur groupe: des mediaspaces pour collaborer et communiquer*. Conference L'interface des mondes réels et virtuels '94, Montpellier, France, 1994.