PRIVACY CONSIDERATIONS IN CSCW: REPORT ON THE CSCW'92 WORKSHOP

ANDREW CLEMENT

A central feature of CSCW applications is the electronic capture and dissemination of detailed personal information. Whether using e-mail, computer conferencing facilities, group decision support systems, media spaces, active badges, or other computerized means for aiding collective work activities, fine-grained information about individual's performance and behaviour is made available to others. This poses important questions about how the people involved may control information about themselves —information which can play an important role in fundamental notions of personal and collective dignity, identity, and autonomy.

Privacy issues are therefore intrinsic to CSCW applications and must be considered an essential part of their design and implementation. However, there has been relatively little attention to these issues in the CSCW context. Is is therefore appropriate that privacy discussions were a prominent part of the activities at the CSCW'92 Conference in Toronto. At previous conferences there had been panel sessions on narrower privacy-related topics and heated exchanges in some papers sessions, but here for the first time was the opportunity for involving a significant number of people in examining in depth a full range of CSCW privacy concerns. The principal forums for these discussions were a small all-day workshop and a plenary panel session attended by a large portion of the 650 conference attendees.

This article reports mainly on the workshop activities while the next article by Jonathan Allen discusses the subsequent privacy panel. A fuller report, including scenario analyses, privacy panel questions and answers, and a bibliography, can be found in the August 1993 SIGOIS Bulletin's special issue dealing with the privacy discussions at CSCW'92. It also contains Rob Kling's "partisan" report as the panel chair, in which he shows how privacy issues in CSCW relate to privacy issues in other areas.

I organized the workshop in recognition of the inherent challenge that CSCW applications pose for personal workplace privacy. I saw the workshop as a way of encouraging discussion among researchers and practitioners about the privacy implications of CSCW technologies, identifying the major issues involved, and developing a framework for guiding CSCW developers and implementors in creating applications that were sensitive to privacy concerns. Announcements of workshop asked anyone interested in participating to submit a short position paper together with a scenario describing a realistic episode in the use of CSCW applications in which privacy issues played a prominent part. All those who did submit were invited to attend, and on Saturday morning, October 30, 1992, 16 participants, including the 4 members of the forthcoming privacy panel, met to begin the all day session. These participants brought an impressive breadth of experience. There were academics who had written extensively on privacy and the workplace implications of computerization, graduate students doing their theses on privacy-related topics, industrial researchers creating basic CSCW technologies, applications developers producing marketable products, and more. All were actively concerned about privacy issues in their work, but had very different interests and views. Many had direct personal experiences that they were able to share with the group. Between them they had brought 26 scenarios, reflecting a wide range of CSCW applications, settings and issues (four of these scenarios can be found below). The stage was set for an stimulating discussion.

Following the usual round of self-introductions in which participations identified some of their primary concerns, the group turned to the central activity of the session—the analysis of scenarios. These had been circulated beforehand to all participants, along with the position statements and a framework for scenario analysis (see below). The discussion of the widely reported Epsom America case, which involved the interception of electronic mail (see below), provided a warm up for the more intense small group discussions of a few chosen scenarios. After lunch, the workshop reconvened to hear the results of the separate discussions and to consider any broader conclusions that could be drawn.

Many of the workshop's participants found it helpful to apply key ideas from certain literatures about computerization to CSCW situations. These literatures include: (1) the body of studies about the computerized control and monitoring systems in more traditional workplaces and (2) the body of studies and legal practices about surveillance, social control, privacy, and fair information practices in personal records systems.

Workshop participants felt that CSCW often raised old issues, such as who has a right to see "private" mail in new electronic venues where norms were much less well established. In some of these cases, procedures that were developed for personal records systems, such as for credit reporting, might be usefully extended to CSCW. Such procedures include due process (e.g., that those who use e-mail systems know what sorts of people may read their private mail, under what conditions, and that they would be informed in advance about such reading, and should have a voice in arguing against such reading by others who were not on the distribution list for a message). In other cases, CSCW applications like audio-video monitoring in medical care created new kinds of records which opened new questions about confidentiality and the balance of rights between doctors and their patients. In both kinds of cases, fair information practices would be valuable for regulating the use of systems and information. While they are mainly social arrangements, and hence cannot be wholly embodied in software or hardware, some fair information practices may be facilitated by special system features.

There was considerable debate among workshop participants about fundamental matters such as the nature of people's rights to privacy in workplaces (and if there are any absolute rights). These debates take on different meanings in workplaces and other social settings, such as "personal" records or mollify. The debates in the workshop paralleled many of the long-standing debates about rights to privacy and their "tradeoffs" with other important values which have been articulated in the rich literature about computerization and privacy in record systems. Workshop participants also debated the extent to which the effective functioning of workgroups required various kinds of individual and group privacy.

Participants generally found discussing scenarios to be an interesting and productive way to deal with these privacy issues. Some thought them "disturbing", and sufficient cause for concern that "privacy impact statements" be prepared in cases of major interventions. One participant felt that the "moral climate" was being eroded in organizations where the greatly enhanced potential for surveillance was becoming accepted as commonplace. This could lead down a "slippery slope" in which individuals increasingly engage in "reflexive self-monitoring" to comply with prevailing social norms. Even the construction of individual and group identities would be challenged in such environments. There were others who argued that the threats were much less serious than this. One technology advocate noted that the debate had been distorted by too much emphasis on the negative aspects, and that the potential to enhance privacy by means of such devices as Active Badges was thereby being over looked.

One of the sharpest differences of opinion came in the discussion of a set of "value statements" about privacy and CSCW (see below). I initially offered these to the workshop as the basis for a possible resolution to be presented in the upcoming panel session. It was immediately clear that some would not be comfortable with any form of collective public statement. What was more surprising, to me at least, was that even the notion of a general statement about privacy values would be problematic. One participant pointed out that with the wealth of experience in data protection available, surely we could agree on a minimal statement about the need to have workplace committees responsible for dealing with privacy concerns. But even this was too much for some. The main concern expressed was that particular situations varied so much that any universalistic prescriptions were doomed. Much more research would be needed before any conclusions could be drawn. This seems to me unduly cautious. While certainly there are important local variations and the need for continued research, we do know enough to start the process of formulating broad values and design precepts which can be adapted for particular situations and refined from experience.

In the end, no agreements were reached. However, my sense is that the participants left feeling that we had discussed important issues and were enlightened by the experience. The workshop was a good step, but obviously there is much work left to do.

The significance of the privacy discussions at CSCW'92 lies not in any resolution of issues, but in the opportunity they provided to bring important issues out into the open. Given the varied interests at stake, the diversity of backgrounds, the complexity of issues and the rapid pace of technological development, it is not surprising that there were no signs of consensus being achieved. However, several observations can be made about the discussions which may help in making further progress. The first is that similar concerns about the possible threats to people's control over information about themselves arise in many different settings—Who knows what about me? How is the information going to be used? Where is the boundary to be drawn between "public" and "private"? Can one be drawn? How should the competing information access interests be traded off between employees and employers and with the organization as a whole? What constitutes informed consent in tightly integrated workplaces? A related observation is that these fundamental issues are not confined to

CSCW and have indeed been with us for some time. CSCW applications mainly just show them off in a new light, perhaps also blinding us to the underlying commonalities and to the rich experiences we can draw upon to address them. While it is discouraging that more reference to earlier debates about computers and privacy was not made in the discussions, this does suggest that greater education about current data protection provisions could be quite fruitful. In particular, principles of Fair Information Practise, listed later in this issue, offer a useful starting point.

If CSCW does bring in a novel aspect to the debates around privacy, it is in its strong focus on group activities. Policies for the proper handling of personal information becoming increasingly necessary for local work settings as well as in wider organizational contexts. Both the informational transactions between individuals and their immediate work groups and between these groups and the larger organization need sensitive handling. Concerns in this area are likely to grow with the rapid spread of techniques which intensify workplace data capture and transmission practices. Hopefully the privacy discussions at CSCW‘92 reflected in these pages will inform this development in ways that promote full respect for the privacy rights of the people involved.

VALUE STATEMENTS ABOUT CSCW AND PRIVACY

Workshop participants found these statements provocative and they helped stimulate interesting discussion and debate about the nature of good professional practice in this area:

1. Individuals and groups have a fundamental right to privacy and control over information about themselves in using computer systems to support their work.

2. CSCW applications inherently pose privacy implications for the individuals and groups that use them.

3. Designers and implementors of CSCW applications bear an ethical responsibility to contribute to social and human well-being in their professional work.

4. Investigation of and education about the privacy implications of CSCW applications should be recognized as priorities in CSCW development.

5. Respect for privacy, and in particular the principles of informational self-determination, should be an important consideration in the design, implementation and use of CSCW applications.

FRAMEWORK FOR SCENARIO ANALYSIS:

General aspects

Organizational setting,
principal actors,
focal technologies,
tasks

Type of information involved
transactional versus content
performance versus behavioural
Relationships
peer versus hierarchical
Generality
"paradigmatic" versus marginal

Privacy issues raised
What "type" of privacy?
intrusion versus exposure
personal versus group
aesthetic vs. strategic

Has privacy been violated?

How & why violated?

Trade-offs and priorities.

Possible remedial principles to follow:

- Informational self-determination—the right of individuals (and groups) to decide when and under what circumstances their personal information may be processed
- Fair information practice (see below)
- Personal/group "ownership" of resources or information (these need not necessarily be regarded as owned exclusively by the employer)
- Feedback (knowing what information about oneself is accessible to whom)
- Equality/Reciprocity (What You May See Of Me Is What I May See Of You "WYMSOMIWIMSOY"?)
- Participation (Users active involved in making on design and implementation choices)
- Bounding personal or group space (defining privacy zone intermediate between the personally private and the public)

Possible realms for action:

These principles may be applied to both the social and the technical realms:

- Social: e.g. etiquette, organizational policy, legislation,...
- Technical: e.g. interface, functional features, infrastructural options
- Social/technical: e.g. development of social conventions around particular technological mechanisms

Possible actors:
managers, developers, users, educators, social advocates, professional bodies, legislators, ...

CODE OF FAIR INFORMATION PRACTICES

To promote information privacy

The principles of Fair Information Practise provide useful guidelines for handling personal information across a range of CSCW settings. While they are well established in the data protection field, and indeed underlie most of the directly relevant legislation, they appear not to be well known among computing professionals. There are many versions of the principles, but they all have in common the intention to enable people to exercise "informational self-determination" the right to determine when and under what circumstances their personal data may be processed. The list provided below is a particularly concise formulation and was prepared by Computer Professionals for Social Responsibility (C.P.S.R.) and Privacy International. It appears in Jan Holvast's "Ethics of Computing: Information Technology and Responsibility", an IFIP TC9 report presented at the IFIP World Computer Congress in Madrid, September, 1992. Another formulation, which is incorporated in the influential OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data can be found in Marc Rotenberg's "Communications Privacy: Implications for Network Design", *Communications of the ACM*, Vol. 4, No. 8, August 1993, pp. 61-68. For a fuller discussion of data protection principles and how they have worked in practise, see David Flaherty's, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, Chapel Hill, 1989.

Stop Data Misuse
Personal information obtained for one purpose should not be used for another purpose without informed consent.

Encourage Data Minimization
Collect only the information necessary for a particular purpose. Dispose of personally identifiable information where possible.

Promote Data Integrity
Ensure the accuracy, reliability, completeness, and timeliness of personal information.

Allow Data Inspection
Notify record subjects about record keeping practices and data use. Allow individuals to inspect and correct personal information. Do not create secret record-keeping systems.

Establish Privacy Policies
Establish and enforce an information privacy policy. Make the policy publicly available.

ILLUSTRATIVE SCENARIOS

The workshop participants and their scenario titles were:

1. Jonathan Allen, UC Irvine, "Integrated manufacturing production reporting"
2. JoAnn Brooks, SunSoft (ex), "Indexing E-mail files"
3. Andrew Clement, University of Toronto, "E-mail court case (New York Times)", "Women's E-mail discussion group (Zuboff)"
4. Kelly Gotlieb, University of Toronto, "Automatic vehicle location reporting"
5. Beverly Harrison, University of Toronto, "Multimedia operating room broadcast", "One-way A/V connections in an engineering office", "Video 'glance' protocols"
6. Andrew Hopper, Olivetti Research, "Real-time remote 'fingering' of active badge data" (panelist)
7. James Katz, Bellcore, "Automatic Number Identification (ANI) Management" (panelist)
8. Rob Kling, UC Irvine, (panelist)
9. Jo Ann Oravec, University of Wisconsin, "Active badge highlighting intra-team discrepancies", "Team leader 'doctors' multimedia commentary", "Covert management profiling of team GDSS behaviour", "Finger pointing via GDSS reconstruction", "Multimedia caricaturing"
10. Russell Owen, University of Toronto, "Privacy expectations in collaborative writing workshop"
11. Amy Pearl, Sun Microsystems, "Sharing artifacts in geographically distributed work groups"
12. Judith Perrolle, Northeastern University, (panelist)
13. Heinrich Schwarz, HPLabs/UC Berkeley, "Video/audio broadcast of neurosurgical operations"
14. Abi Sellen, Rank Xerox EuroPARC, "Open A/V shared office - unexpected over-hearing", "Video in commons broadcasts 'private' trouser repair", "Open A/V shared office - borrowing as intrusion", "Open A/V shared office - expectations of response"
15. Sylvia Wilbur, University of London, "Unwelcome background exposure in a media space"
16. Mary-Ellen Zurko, MIT/DEC, "Anonymity in computer conferencing"

The following are four of the 26 scenarios contributed by workshop participants. Other scenarios, along with analyses, can be found in the August 1993 issue of the *SIGOIS Bulletin.*

Scenario 1: E-mail court case—Epson America

'When Alana Shoars arrived for work at Epson America one morning in January 1990, she discovered her supervisor reading and printing out electronic mail messages between other employees. As electronic mail administrator, Ms. Shoars was appalled. When she had trained employees to use the computerized system, Ms. Shoars told them their mail was private. Now a company manager was violating that trust.

When she questioned the practice, Ms. Shoars said, she was told to mind her own business. A day later, she said she was fired for insubordination. She has since filed a $1 million wrongful termination suit.

... she still bristles about Epson: "You don't read other people's mail, just as you don't listen to their phone conversations. Right is right, and wrong is wrong."

Michael Simmons, chief information officer at the Bank of Boston, disagrees completely, "If the corporation owns the equipment and pays for the network, that asset belongs to the company and it has a right to look and see if people are using it for purposes other than running the business," he said.' (excerpt from Rifkin, NYTimes, Dec. 8, 1991, contributed by Andrew Clement, Univ. of Toronto)

Scenario 2: Real-time fingering of active badge data

Active Badges are an infrared based technology for tracking people and objects in organisations. They have been developed at Olivetti Research in Cambridge and have been in use for a number of years. They have proved extremely useful—indeed addictive--and are at present in use by a group of about 150 people across two sites. No longer are phone calls made to people who are not available, nor does one try and find colleagues who are not there. By passing the wearers' circumstances to others the system makes it possible for users to be more polite to each other. The formal rules are that no storage of the information is allowed and that there is symmetry of use (if I see you, you see me). The success of the Badge System has encouraged us to extend our work on location systems which make information available to applications.

The Active Badge information is available on the Internet using a modified finger command. This has had the benefit that users trying to contact each other across continents can do so easily. From time to time the phone rings and at the other end there is somebody thousands of miles away who says "I see your meeting has finished and I wanted to call you about some subject". It is possible to track the sites from which the finger command is being run. By word of mouth, the availability of the system has spread and there are now many sites which look at individuals' movements for no apparent reason. Is this one-sided peeping a potential breach of privacy? (contributed by Andy Hopper, Olivetti Research)

Scenario 3: Active badge highlighting intra-team discrepancies

This scenario is set in an organizational context in which Active Badges are utilized. Much of the work in this organization is conducted in teams. In one of the teams, a member was formally warned by his supervisor that he should not spend so much time visiting the offices of lower-level employees in person; two of these employees were mentioned by name in the conversation. He was told by the supervisor that "effective" team members request that their subordinates come to them if face-to-face contact is indeed required.

The individual being chastised for his office behavior asserted that he indeed was highly productive despite his perambulatory habits. His manager countered that she knew that several other individuals in the team were far more productive, primarily because they stayed in their own offices at least 20 percent more than he did. The manager added that the two lower-level employees (mentioned previously) were seldom visited by the more effective team members. After the perambulatory individual discussed the situation with his peers in the team, several of them protested to the manager that she was employing personally-identifiable information pertaining to their own work habits in the evaluation of a co-worker without their knowledge or consent. (contributed by Jo Ann Oravec, Univ. of Wisconsin)

Scenario 4: Covert management profiling of team GDSS behaviour

This scenario is set in a large R&D establishment, with a good number of teams. Most of the teams utilize electronic meeting rooms (such as IBM GroupSystems) as well as a variety of group decision support systems (GDSS).

Profiles of many of the groups' decision-making characteristics in these electronic meeting room and GDSS environments were regularly composed and analyzed by management higher-ups. Decisions were made as to team membership, leadership, and other important group-level aspects largely on the basis of whether or not a member was considered a "benefit" or a "detriment" to the team in light of these group profiles. The profiles were not shared with the teams—they were considered "group" profiles, not individual profiles. The reasons given for the transfers of individuals among teams often included the phrase "team-group incompatibility" but otherwise gave few clues as to what was happening.

An individual involved in a transfer from one team to another inadvertently found out about management's use of the profiles in making critical decisions about group membership. This individual complained to some of the managers who utilized these techniques, arguing that the group as a whole should be informed about the construction of the profiles and their use by management. The managers replied that neither the privacy of the groups involved nor that of any single individual was being violated, since the profiles were of "aggregate group behavior" and were developed in the light of various widely-accepted social science techniques and methodologies. (contributed by Jo Ann Oravec, Univ. of Wisconsin)

SHORT BIBLIOGRAPHY PERTINENT TO CSCW & PRIVACY

Rob Kling [UC-Irvine]

1. Association of Computing Machinery. 1993. "ACM Code of Ethics and Professional Conduct." *Communications of the ACM.* 36(2)(Feb.):99-103.

2. Attewell, Paul. "Big Brother and the Sweatshop: Computer Surveillance in the Automated Office" in Dunlop and Kling 1991.

3. Bullen, Christine and John Bennett. 1991. Groupware in Practice: An Interpretation of Work Experience" in Dunlop and Kling 1991.

4. Congress of the United States. 1986. *Electronic Communications Privacy Act of 1986.* 100 STAT. 1848. Public Law 99-508. Text available by gopher from the Electronic Frontier Foundation at gopher.eff.org.

5. Dunlop, Charles and Rob Kling (Ed). 1991. *Computerization and Controversy: Value Conflicts and Social Choices.* Boston: Academic Press.

6. Harper, Richard H.R. "Looking at Ourselves: An Examination of the Social Organization of Two Research Laboratories" *Proc. CSCW '92*: 330-337.

7. Iacono, Suzanne and Rob Kling "Computing as an Occasion for Social Control" *Journal of Social Issues*, 40(3) (1984):77-96.

8. Jackall, Robert (1988). *Moral Mazes: The World of Corporate Managers.* New York, Oxford University Press.

9. Kling, Rob. 1991. "Cooperation, Coordination and Control in Computer-Supported Work." *Communications of the ACM* 34(12)(December):83-88.

10. Kling, Rob and Charles Dunlop. 1993. "Controversies About Computerization and the Character of White Collar Worklife." *The Information Society* 9(1) (Jan-Feb):1-29.

11. Kling, Rob. "Organizational Analysis in Computer Science." *The Information Society* 9(2) (Mar-May, 1993):71-87

12. Kling, Rob. "Fair Information Practices with Computer Supported Cooperative Work." *SIGOIS Bulletin* (July 1993):28-31.

13. Marx, Gary. "The Case of the Omniscient Organization," *Harvard Business Review*, March-April, 1990.

14. Orlikowski, Wanda. 1991. "Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology." *Accounting, Management and Information Technology* 1(1):9-42.

15. Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society*, U.S. Government Printing Office, Washington D.C. (briefly excerpted in Dunlop and Kling, 1991.)

16. Riddle, Michael H. 1988. "The Electronic Communications Privacy Act of 1986: A Layman's View." Available by gopher from the Electronic Frontier Foundation at gopher.-eff.org.