Toward a Policy for Managing the Use of Computer Mediated Communication in the Workplace

Douglas J. Swanson

The University of Oklahoma

Editor's Note: Swanson is working toward his Ph.D. in Political Communication at O.U. He holds Bachelor's and Master's degrees in Communication from Eastern New Mexico University. He is currently an Instructor in Communication at Cameron University, Lawton, OK. Swanson is Vice President of a public relations consulting firm, The Swanson Group Inc. He may be reached at BITNET DSWANSON@UOKUCSVX or (405) 581-2473.

Paper was presented at the Fourth Annual Sooner Communications Conference, University of Oklahoma, Norman, Oklahoma, April 3, 1993.

Abstract

Toward a Policy for Managing the Use of Computer Mediated Communication in the Workplace

Douglas J. Swanson

Within the past decade, there has been tremendous growth in the number of businesses and not-for-profit organizations which have become equipped with computers and have empowered workers to communicate with them. This new on-the-job empowerment is known as Computer Mediated Communication (CMC). CMC's use has resulted in greater production and performance in the workplace. It has also resulted in an increased amount of tension observed between management and subordinates. This tension is evidenced through accounts of people's behavior in the workplace--specifically, accounts of members of management who perceive a lessening of their ability to control the actions of subordinates who use CMC to communicate on the job. These members of management have indicated a need for greater control over CMC, to help bring the CMC process and the subordinates who use it into the workplace hierarchial system. Subordinates, on the other hand, have reported that they enjoy the social and technical freedom they obtain for themselves through CMC--and that they want to preserve their ability to apply CMC skills and technology in the workplace as they see fit. Subordinates often report, however, that the management hierarchy stands in the way of this process by impeding access to CMC or limiting its content.

The observed organizational rift that results from these two drives in opposite directions may threaten organizational stability, and, in turn, may have the potential to reverse the productivity gains that CMC is typically introduced to foster.

The author hopes to shed some light on the situation by first summarizing CMC's impact on the organizational social and technical environment. He looks at issues of CMC content and access, to illustrate the current diversity of opinion about the assembly and legal ownership of CMC messages in the workplace. Varying opinions about access to, and editorial control over CMC messages are examined. The author looks at several business and educational organizations in which management and subordinates have encountered difficulty when attempting to define operational boundaries for the use of CMC.

As an initial step toward bridging the gap between the management and subordinate needs in the workplace, the author poses questions which may help in the development of policies which can bring about more effective organizational control of CMC. The questions urge consideration of a variety of operationalizations which will help balance the need of management to regulate CMC with the desire of subordinates to increase productivity and empowerment through CMC's use.

CMC Applications

There are tens of millions of personal computers in use today, along with thousands of varieties of software packages (Dertouzos, 1991). In the workplace, total dollar sales of computer systems as a share of durable-equipment purchases increased between 12% and 17% every year for the last decade, while the personal computer market grew at a 12% to 17% annual rate (Lewis, 1989). Corporate spending for computers "account[s] for more than 14% of the average capital budget" (Lewis, 1989, p. 69). The total value of computer hardware and software in use in the U.S. today is estimated at more than $500 billion (Dertouzos, 1991).

There has been a profusion of computer user networks established to link all these computers. One of the largest networks, Internet, operates in 26 nations, has more than 5,000 smaller networks feeding into it, "and supports several million users on more than 300,000 computers in several thousand organizations" (Cerf, 1991, p. 50).

In the U.S. alone, 60 million people have the ability to use their computers to communicate directly with other computer users--either at home or at work (Schwartz, 1991). This process is referred to as Computer Mediated Communication (CMC). CMC allows users to send and receive person-to-person messages to other individuals or groups of people (Kiesler, 1987; Hiltz & Turoff, 1978)--as opposed to the simple interaction with a predetermined computer program one might encounter when dealing with an automated bank teller machine or library electronic on-line catalogue. In CMC, the sending and receiving processes operate independently of each other and include "both routine transfer of data and nonroutine interpersonal communication" (Kiesler, Siegel, & McGuire, 1984, p. 1123). CMC helps eliminate the "elaborate, costly, and inefficient formal structure that often stands in the way of getting work done" (Zachmann, 1991, p. 96) because it allows participants to share information and bridge physical, cultural and social barriers in their organizations and others with which they work. It allows users to obtain "access to other people and what they have to

say" (Oldenburg, 1991, p. E5). It allows "the experience and expertise of employees [to] be mustered wherever it is needed" (Finholt & Sproull, 1990, p. 61-62). In short, CMC is a fast, text-based means of distributing information between people to "reduce coordination costs" (Malone & Rockhart, 1991, p. 92). CMC "speeds up information flow" (Finholt & Sproull, 1990, p. 41) and has the potential for increasing productivity and satisfaction within the workplace (Rockhart & Short in Scott Morton, 1991, p. 189).

CMC users must have the ability to electronically link with other users--something that is accomplished through networks. Networks link computers to pass information between individual users (Uncapher, 1991; Turner, 1990). Network member computers may be directly wired to each other, or linked by fiber optics, telephone lines, satellite or microwave receivers--whatever is necessary to form, transmit, manage, present and trigger application from the data in question (Cerf, 1991). "Typically such networks are arranged in hierarchies, starting with local-area networks that might link an academic department, then campus networks that link departments, then state or regional networks, and finally national and international networks" (Turner, 1990, p. A16). Increasingly, networks are becoming interrelated; often a message will cross several networks as it travels between sender and recipient(s) (Uncapher, 1991; Sproull & Kiesler, 1991; Kramer, 1990). Klausmeier (1984) breaks computer networks into three basic categories: local area networks of linked computers (LANs), microcomputer-based messaging systems (including bulletin boards), and commercial information systems. These network systems, working together, help substitute information technology for human coordination. They increase coordination between information sources and bring about "a shift toward the use of more coordination-intensive structures" (Malone & Rockhart, 1991, p. 94). The end result is an increasingly globally-networked society and workplace (Negroponte, 1991; Tesler, 1991), where "even managerial jobs will be handled from afar" (Weiss, 1992, p. 7).

There are many ways in which information promulgated through CMC is distributed. One way is through what is known as Electronic Mail. E-Mail, as it is commonly known, allows a user to create a paperless message for a specific recipient and then "send" that message to an electronic "mailbox" where only the intended recipient can retrieve it. Recipients of E-Mail can answer their correspondence in the same fashion (Zachmann, 1991; Sproull & Kiesler, 1991; Canipe, 1983).

Frequently, CMC users have the option of joining a "mailing list" so that they may automatically receive messages that deal with particular topics. Recipients often subscribe to, or choose to be on, several mailing lists (Turner, 1990).

Computer Bulletin Boards (BBS) have been described as "a major new communications medium, one of the few ways in which the PC revolution is having an enduring impact upon life at home" (Miller, 1991, October 21, p. R8). Surely the impact of BBS use is just as great in the workplace, since there are at least 45,000 BBS systems operating worldwide and servicing both at-work and at-home CMC users (Miller, 1991, October 21).

> A BBS is a modem-equipped computer that can communicate with other modem-equipped computers over ordinary telephone lines. A modem translates computer text and numeric data into an audio signal that can be passed back and forth; the BBS software tells the computer how to act as a host for other computers that dial in. Use of the BBS varies extensively from "underground" boards to businesses using them to communicate with employees, to investment groups swapping ideas, to churches using them as outreach tools, and to schools, which are especially interested in their use.
>
> (Manning, 1986, Abstract)

BBS systems are basically open marketplace idea exchanges, where CMC users can engage in discussions of current events and issues (Oldenburg, 1991), ask for assistance with technical problems (Segal, 1990), make social arrangements (Turner, 1990; Turner, 1988), share educational research (Tesler, 1991; Sproull, 1986), gather textual information about a variety of general interest subjects (Lacy, 1991; Cerf, 1991), download specific

publications (Belsie, 1992; Cressy, 1984), or copy computer software programs (Brennan, 1991; Hume, 1989).

BBS systems almost always focus on relatively specific subjects, and, generally charge little or no fees to participants (Manning, 1992).

Frequently, CMC network participants engage in computer conferencing to help facilitate decision making. Such conferencing can take place in a Group Communication Support System or Decision Support System. These computer-supported cooperative work systems--which encompass information storage and retrieval, presentational capabilities, and group "collaboration support" are primarily used as information aids (Pinsonneault & Kramer, 1990). As such, they focus on "relatively short-term problem-solving and decision making" (Connolly, Jessup, & Valacich, 1990, p. 689).

Conferencing can also occur within the confines of a Group Decision Support System, which goes a step beyond basic decision support systems to combine "communication, computing, and decision support technologies to facilitate formation and solution of unstructured problems by a group of people" (DeSanctis & Gallupe, 1987, p. 559). GDSS systems attempt to structure the process to guide groups toward making effective decisions (DeSanctis & Gallupe, 1985; DeSanctis & Gallupe, 1987).

Although CMC offers great potential to increase learning and productivity as well as expand our social outreach--in many ways we have not yet learned how to handle the conflicts that this increasingly proficient communication medium has brought to society.

Organizational Conflicts in the CMC Workplace

> All large institutions--whether they be governments, universities, corporations, libraries or computer networks--must face a fundamental choice: Will they or will they not read the mail and get into the business of deciding what is sufficiently offensive to justify censorship?
> (Dershowitz, 1991, p. B5)

Issues of Content

There has been, to date, no specific legal protection assigned to the content of CMC--primarily because CMC hasn't been legally defined as speech, as press, or as assembly. It is has not been determined to be among any of the categories of expression that the U.S. Constitution explicitly protects. Douglas Abbott, University of Massachusetts Associate Vice Chancellor for Information Systems, is among the CMC managers struggling to weigh the free-speech rights of university computer users against a perceived need to regulate the content of CMC on campus--while coping with the uncertain legal status of CMC. "We've been trying to come up with some guidelines that might be enforceable. But, generally, the way it's defined is the old conundrum: I know it when I see it," he says (Oldenburg, 1991, p. E5).

Much of the debate over content issues focuses on the First Amendment to the U.S. Constitution, which states that Congress ". . .shall make no law respecting an establishment of religion, or prohibiting free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances" (in Kahn, 1984, p. 10).

There is general agreement that certain, narrowly-defined categories of racist and/or violence-inciting speech can be restricted (Tatel, 1990). Such restriction has been extended to words that present a "clear and present danger of creating public disorder" (Tatel, 1990, p. B1).

The "clear and present danger" axiom stems from the Supreme Court's 1969 "Brandenburg decision" (Kalven, 1988; Nelson & Teeter, 1982). Brandenburg v. Ohio had to do with a Ku Klux Klan leader who had been convicted in Ohio for advocating the necessity of criminal activity, violence or terrorism to accomplish political reform. The KKK leader's conviction was reversed by the Supreme Court, which cited an earlier ruling in Dennis v. United States (1951) and found that the speech given by Brandenburg did not pose

significant potential threat--or "clear and present danger" that a crime would be attempted or accomplished as a result. Thus, the court found the speech did not warrant government restriction (Nelson & Teeter, 1982, p. 42). Thus, "[w]ords challenging the authority of the state have brought criminal conviction at trial, but . . . have continued to find protection under appeal to the Supreme Court", Nelson & Teeter summarize as they examine the aftermath of the court's decision (1982, p. 45).

With its ruling, the Supreme Court set "the boundary line of permissible censorship" Kalven writes (1988, p. 124), suggesting that the new line is located where advocacy is directed toward "inciting or producing imminent lawless action and is likely to incite or produce such action." Kalven contends this boundary line established by the court marks the "minimal jurisdiction over political speech that concern with public order requires be ceded to censorship" (1988, p. 124).

But the issue is still not resolved, since, more than 20 years after the Brandenburg decision, scholars still disagree on its potential impact.

Bogen contends that the Supreme Court, though it has agreed on the standard that "advocacy must be directed at producing imminent unlawful action and be likely to produce some action" (1984, p. 42), may still not be taking into account the possibility of a greater threat to the public. Some justices, Bogen writes, "may find illegal action likely whenever there is some advocacy of specific, concrete immediate acts, because such advocacy does not permit time for counterargument [,] and judicial judgements on the likelihood of affirmative response are difficult to make. Others may find illegal action is imminent where the evil is overwhelming and the advocacy is specifically directed to accomplishing that illegal goal by specified action even though such action is not to take place for an indefinite period of time. Still other people would call for a combination of the advocacy of immediate specific illegal acts together with a substantial likelihood that the advocacy would succeed" (Bogen, 1984, p. 42).

Bogen states his belief that "all judges" seem to agree on the function of the line--to prohibit the government from suppressing ideas that pose no threat while permitting it to prevent illegal action which could follow from such ideas (Bogen, 1984, p. 42). Still, he offers no hope that the justices--or anyone else for that matter--will reach agreement any time soon on exactly what construction of "ideas" can have the context of the earlier court rulings applied to them.

Tribe (1991) suggests that answers can be found by simply taking a more macroscopic perspective of the issue. "New technologies should lead us to look more closely at just what values the Constitution seeks to preserve," he writes (p. 16). He suggests that the Constitution is in fact a document "whose principles are suitable for all times and all technological landscapes" (1991, p. 17); that Constitutional principles "are subtle enough to bend [and] needn't be broken or tossed out" (p. 19).

The Fourth and Fourteenth Amendments are often cited when CMC advocates discuss issues related to the privacy of information within CMC systems and protection of the people who use them--primarily because there have been so many government attacks against that privacy.

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (in Grolier, 1992).

Section One of the Fourteenth Amendment to the Constitution reads: ". . . No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws. . ." (in Kahn, 1984, p. 10).

There has been an escalation in sophisticated federal, state, and local law enforcement agency "raids" against CMC operators for alleged "illegal" activities in the past couple of years (Uncapher, 1991; Hentoff, 1991; Elmer-Dewitt, 1991; Brennan, 1991; Kramer, 1990). The primary government complaint against these operators--most of whom are BBS sponsors--is that they are "suspected of trafficking in stolen credit-card numbers, telephone access codes and other contraband of the information age" (Elmer-Dewitt, 1991, p. 81). Often, attorneys and others who represent the companies which claim to be victims of the alleged criminal activity are permitted to accompany law enforcement officers on these raids and immediately seize "the computer, backup discs and tapes used to run and record activity" on the BBS systems in question (Brennan, 1991, p. 97).

The primary question in regard to the Fourth and Fourteenth Amendments is whether these searches and seizures are "unreasonable" or conducted without "due process of law." Hentoff (1990) contends they are--not just because of the property seized, but because many law enforcement agencies actively peruse alleged computer entrepreneurs as "racketeers" under terms of the federal Racketeer Influenced and Corrupt Organizations (RICO) Act (Hentoff, 1990, p. 12).

"RICO makes it a crime for anyone to commit a "pattern" of two or more "racketeering" acts in conducting the affairs of an "enterprise," [and] just about any kind of crime can be prosecuted as a RICO violation" Hentoff writes (1990, p. 12).

Hentoff details several pending cases as he explains how RICO laws can--and have been--used against protest organizations "engaged in any sort of confrontational tactic as a form of protest" (p. 13). The statutes, he contends, allow prosecutors to seek and gain not only property seizure but triple the damage award initially sought against a defendant if the crime is judged to be a RICO crime.

Although Hentoff says that RICO does not really apply to these cases and that attorneys and prosecutors must surely "recognize that RICO and free speech are profoundly

incompatible" (1990, p. 13), "to others the temptations of so powerful a weapon--as well as the prospect of punishing a wicked defendant by inflicting triple damages--is overwhelming."

There have, of course, been instances in which specific criminal acts were carried out with the assistance of CMC. These include the case of a Virginia man convicted of using a national BBS to distribute "formulas for homemade bombs (Duggan, 1990, p. A1); alleged reports of "distributions of child pornography via electronic bulletin boards" (Lindquist, 1991, December, p. 7); the introduction of computer viruses into systems to disrupt operations and damage software (Rothfeder & Schwartz, 1990), and the illegal posting of copyrighted software on BBS systems for CMC users to copy and use without paying the requisite royalties (Alexander, 1991; Glowacki et al, 1988). Although highly publicized in the media, these instances of criminal activity would appear to be the exception and not the rule (Rifkin, 1991; Kramer, 1990)--even though Rothfeder and Schwartz contend that hackers engage in "sabotage [which] could cause a catastrophe" in the world economic community (Rothfeder & Schwartz, 1990, p. 72).

While it's doubtful that many reasonable CMC users would support the establishment of CMC "data havens" to foster criminal activity (Tribe, 1991, p. 18), there is growing concern that law enforcement authorities cannot be kept from going too far with their extensive warrants, searches, surprise raids and seizures of equipment (Rifkin, 1991; Elmer-Dewitt, 1991; Kramer, 1990).

What's more, corporations which feel they've been victimized by computer hackers are gleefully assisting in the government's effort (Brennan, 1991; Elmer-Dewitt, 1991; Rothfeder & Schwartz, 1990). Novell, Inc., for example, has an extensive "crusade" mounted to prevent unauthorized accessing of its technology and software. Novell has investigators who go looking for company software which shows up on BBS systems--and the firm actively seeks civil and criminal damages against those who may end up with information taken from Novell (Brennan, 1991).

Another highly-publicized example of corporate action is the case involving the uploading of a Bell South telephone company document to an Illinois BBS in 1988. The BBS operator who passed along the document--even though he did not personally acquire it and had contacted telephone company officials to obtain further information about it--was crushed by the corporate bureaucratic, law enforcement and judicial systems. His equipment was seized, his BBS subscriber list was confiscated; he was investigated by the Secret Service and brought to trial. He was released from suspicion after running up more than $108,000 in legal expenses, losing a year of his personal life and collegiate studies to the legal fight and being threatened with a 30 year prison term (Uncapher, 1991; Rothfeder & Schwartz, 1990). The case was at trial when it was revealed that the document--which Bell South alleged was worth $79,449--was in fact "available to the general public for $16." Prosecutors dropped their complaint. (Uncapher, 1991, p. 13).

The situation is distressing for many because CMC does not present "tangible objects everyone could understand" (Dyson, 1991, p. 288)--although she says some are trying to. ". . . [W]e should make a distinction between pranksters and larcenists and not tar all hackers with the same brush," Dyson says (1991, p. 288). "The law should protect both property-holders from miscreant individuals and individuals from miscreant officials. It should also protect the rights of all of us to unrestricted electronic communication" (Dyson, 1991, p. 288).

In addition to pushing for an interpretation of Constitutional rights with a concern for their application to CMC, many activists in the field are seeking to better educate the public on the importance of CMC in a free society. They believe the on-line information system is the equivalent of a printing press--something that would allow BBS operators to be "legally recognized as publishers, not unlike newspaper publishers" (Kramer, 1990, p. 53). "Just as AT&T is not charged when drug dealers use telephones to arrange an illegal transaction, so should BBS operators not be arrested or blamed when the tiny minority of computing

criminals takes advantage of their services," Kramer writes (1990, p. 53). (See also Scarborough, 1992; Uncapher, 1991; Oldenburg, 1991; Dershowitz, 1991).

Some CMC users have proposed a 27th Amendment--one which would help bring the late 18th century laws and legal principles more in line with 20th century technology. Elmer-Dewitt (1991, p. 81) quotes Harvard law professor Laurence Tribe, who says a 27th Amendment would make the information-related freedoms guaranteed in the Bill of Rights fully applicable "no matter what the technological method or medium" by which that information is created, stored, or transmitted.

"While such a proposal is unlikely to pass into law," Elmer-Dewitt observes, "the fact that one of the country's leading constitutional scholars put it forward may persuade the judiciary to focus on the issues it raises" (Elmer-Dewitt, 1991, p. 18).

Of course, not everyone is so optimistic. Carroll, for instance, offers no hope for a legal resolution of privacy rights. "A firm link between privacy and freedom has yet to be established by objective and systematic research," he contends (1975). "And there is reason to believe that concepts of privacy may turn out to be too culture dependent and possibly too transient to permit any valid conclusions to be achieved were such studies to be undertaken" (Carroll, 1975, p. 278).

Regardless--as things now stand, "without clear limits on searches and seizures, federal law-enforcement agencies have essentially been able to drive whomever they want out of business. The lesson has not been lost on anyone; the overall impact on . . . bulletin boards has been rather chilling" (Uncapher, 1991, p. 13).

Issues of Access

As with issues of content, debate over access to CMC messages usually focuses on E-Mail and BBS functions. The primary question is: Who may access E-Mail and BBS and under what circumstances? We will examine this question from the perspective of members of

management, subordinates and others who are now debating CMC access issues in academic and business environments.

A number of organizations, primarily academic institutions, have taken the position that CMC access--which goes hand-in-hand with questions of the appropriateness of content--remains primarily the right of the individual. (Unfortunately, there's not a significant chronicling of the extent of this opinion--Turner, 1990 is the primary source for information on this subject, which needs much more attention in the general and scholarly literature.)

A prime example of the upholding of the rights of individual CMC users is at Carnegie Mellon University, one of the most aggressive institutions in the nation in "pursuing and shaping the new computer technology" (Kiesler & Sproull, 1987, p. 38). At C.M.U., Chris Thyberg, Assistant Director for Academic Computing, says even messages that bring complaints from CMC users remain on the system "along with the discussions they have prompted." C.M.U. has decided, he says, that "if we take down items in bad taste, we set the standards of taste. We become the arbiters." For that reason, the university leaves most decisions to the users (Turner, 1990, p. A16).

At the State University of New York, Associate Vice President for Computer Services Geraldine E. MacDonald says that "the student's computer file [is] viewed the same as his notebook--private. We would have to get a subpoena to get the information in it" (Turner, 1990, p. A16).

A similar attitude prevails at the New York Institute of Technology, which does not access computer files to review the information held in them or monitor traffic on its conferencing system. "We take the position that ownership of the message belongs to the person who put it on the system," reports Stanley Silverman, Director of Academic Computing (Turner, 1990, p. A16). Silverman says he would intercede in the CMC process "only in the clearest case of violation of law" (Turner, 1990, p. A16).

The universities which have engaged in open campus debate over the question include Stanford and the University of Massachusetts in Amherst. At Stanford, CMC managers erased an electronic file which contained a racial joke. Faculty members came forward to protest, calling the erasure "censorship." The university later "backed down and posted the jokes file again on the main campus computer" (Turner, 1990, p. A16).

At Amherst, a line between censorship and sensitivity was drawn in 1989, when a dispute arose over a sex-oriented CMC conference, "Cyberlust." The conference was carried over the New England Academic and Research Network which serves the University of Massachusetts and other institutions in the region. U.M.A. Associate Vice Chancellor for Computing Services, Douglas Abbott reviewed the files in question and held public hearings to help formulate a university policy. "There are people who have great objections to having that material on the network even though it is well-identified and you have to log into it to read it," Abbott says (Oldenburg, 1991, p. E5). In the end, Abbott says that the university "wanted to err on the side of leaving it alone" and no attempt was made to drop the conference from the network or from the university's computer system (Oldenburg, 1991, p. E5).

A somewhat similar incident at the University of Michigan was resolved in a different manner--with the consent of users. A U.M. BBS system carried a file of "tasteless" jokes, including several having to do with a campus suicide. After some users complained, the university asked BBS users to "decide whether the jokes were out of line." Students voted to stop posting them (Turner, 1990, p. A16).

These academic institutions have made the decision to uphold the rights of the individual CMC users over that of the organization at large. They have, in effect, answered the question posed by the author at the start of this section by indicating that CMC users may have the right of access to, and control over, E-Mail and BBS--and that the institution will not involve itself in the process.

Other institutions have decided in the opposite direction, ruling that the institution has primary access and control over CMC--and relegates access to the users--to the extent that the users do not in any way threaten the hierarchy of the institution.

Within academia, problems with BBS access--and content of messages therein--resulted in elimination of all BBS systems except those initiated and monitored by administrators and faculty at the Princeton University, the University of Nebraska, S.U.N.Y. Binghamton and Cornell (Turner, 1990, p. A16).

Cornell is perhaps the prime example of an institution upholding the rights of the hierarchy over the rights of the individual. Cornell has the policy that it owns its computer system, and that it has "the right to read and even impound anything that might be a threat to the system's security" (Turner, 1990, p. A16). When a graduate student was suspected of authoring a computer virus, Cornell University administrators accessed and read the student's files, and assisted law enforcement agencies in charging the student with violating federal computer-security laws (Turner, 1990).

Other institutions which "take the position that they own their systems and make them available to users as a courtesy" include Baylor University and Brown University. At Baylor, a computer program run on the university system searches student's files and identifies those in which "foul language" is used (Turner, 1990, p. A16). At Brown, Brian Hawkins, Vice President for Computing and Information Services believes "the system and the files are property of the university. Therefore I have ownership and legal access to anything on the system" (Turner, 1990, p. A16).

Within the private sector, the Prodigy Interactive Personal Service has been at the center of an extensive public debate over content of, and access to, CMC messages. In 1991, Prodigy announced it was initiating an effort to ban user access to messages "grossly repugnant to community standards" by deleting such messages from its BBS. It is a decision that goes one step further than an earlier Prodigy policy to bar "obscene, profane or otherwise

offensive messages" from posting (Miller, 1991, October 24, p. B1). The action followed complaints about alleged anti-Semitic messages posted on the Prodigy BBS, which is available to 1.1 million subscribers (Schwartz, 1991).

At least one user, whose access to the Prodigy BBS has been restricted, complains that he was denied the opportunity to distribute information on account of "vaguely defined sins and misdemeanors" (Lacy, 1991).

Although Prodigy officials said the plan of action would support "family values" (Miller, 1991, October 24, p. B6) while still allowing for a diversity of opinions on the system's BBS, outsiders disagreed. "Once they decide to make decisions about what they're going to allow, then they take responsibility for what they do allow," contends Mike Godwin, counsel for the CMC users rights advocacy group Electronic Frontier Foundation (Miller, 1991, October 24, p. B6).

Prodigy faced additional public wrath when it was alleged that Prodigy administrators were uploading and examining users' personal files through the STAGE.DAT file created when Prodigy is installed on users' hard drives. The Los Angeles County District Attorney's Office Consumer Protection Division was investigating the allegations after receiving complaints from Prodigy subscribers (Lindquist, May, 1991).

Prodigy denies uploading user files, and contends its BBS content regulation balancing act will work. But if Prodigy should fail to keep the public trust, warns Electronic Frontier Foundation President Mitchell Kapor, "it will be that much more difficult to attract any major investment for on-line services" (Schwartz, 1991, p. 48).

In the corporate world, IBM has demonstrated extensive control over employee use of CMC--and of employee communication in general. IBM audits employee phone mail greetings (Carroll, August, 1991). It has created policies stipulating that information about the actions of the company released to the news media be communicated in a more "controlled" manner (Carroll, May, 1991, p. B2). It has an extensive centralized authority structure that

employees commend works hard to create the impression that "[e]verybody thinks they're going to be out of a job" if employees don't tow the company line and measure up to performance standards (Depke, 1991, p. 115). Part of that towing the company line has to do with knowing what not to post on the IBM BBS.

IBM has been in a difficult financial situation for several years. Its earnings--and its market share--have dropped dramatically since the mid-1980s (Carey & Coy, 1991; Carroll, 1991, May; Carroll, 1991, August; Carroll, 1991, October; Burke, 1989).

In mid-1991, IBM Chairman John Akers gave what was described as a terse and threatening speech to employees, urging them to "wake up" to the demands of the changing computer industry (Carroll, May, 1991, p. B1). Although Akers' comments were not intended to be widely-distributed, "through the magic of IBM's extensive electronic mail network, the word quickly spread through the company" (Carroll, May, 1991, p. B1). The comments posted on the BBS relayed Akers' feelings that he was "goddamn mad" about IBM's loss of market share, that the "tension level" among employees was insufficiently high, and that the company would be saying "goodbye" to employees who were unable to produce to IBM's expectations (Carroll, 1991, May, p. B1, B2.

Shortly after the comments attributed to Akers were disseminated by employees on the company BBS, IBM management moved in to censor the remarks and restrict access to the system. IBM executives ordered "thousands" of comments erased from files on the central computer BBS and re-drafted job descriptions to gain greater control over BBS accessibility (Carroll, August, 1991, p. A1). When the news media learned of the erasure and questioned IBM about it and the circumstances associated with it, IBM Vice President Mary Lee Turner responded angrily that the company was fully within its rights and that the comments were "totally unrepresentative of what's going on at IBM" (Carroll, August, 1991, p. A4).

The company later admitted that its executives had "sorted through" the messages--all of which were traceable to their senders. It admitted that employees overwhelmingly felt

morale was poor, but said its own "official morale survey" found spirits to be high (Carroll, August, 1991, p. A4). This claim was made despite other reports that, at IBM, "head-rolling . . may be a healthy exercise" (Sullivan-Trainor, 1991, p. 23). (See also Collingwood, 1991.)

Through the actions of its corporate hierarchy, IBM has demonstrated its desire to regulate all electronic communication between employees to force support of the hierarchial structure. One can only wonder how many other organizations take this same aggressive posture.

A Guide for Forming Organizational CMC Policy

We've seen examples of the impact CMC has in today's organization. CMC can both speed and expand the reach of information processing--leading to greater organizational performance and efficiency. But CMC also has the potential to cause divisions in organizational hierarchy, when there are no clear rules--acceptable to all parties involved--for its use.

Clearly, then, an organization in which CMC is used needs an effective management plan to balance the needs of the organization for information processing with the needs of individuals for privacy, socialization and personal empowerment.

The author could locate no comprehensive plan along these lines, although he did locate proposals for defining "moral responsibilities" of computer use (Friedman, 1990); for determining "ethical considerations" of computer use (Weintraub, 1986); for escaping "legal problems" associated with BBS use (Nobile, 1990); for ensuring privacy rights of employees (Allred, 1988; American Bar Association, 1987; Shepard & Olsen, 1986); for ensuring the privacy rights of employers (Carroll, 1975); for ensuring free speech through CMC in the university environment (D'Souza, 1991; Tatel, 1990); for using "telecommunications" to foster organizational wellbeing (Keen, 1990); for enforcing CMC system security (Landberg, 1986); for creating proper CMC "etiquette" (Turner, 1988); for creating the computer supervisor job

description for "your next administrative hire" (Wepner & Kramer, 1984); and for establishing a national commission to examine issues related to CMC (Ware, 1984).

None of the above makes an effort to pull together all the complex issues surrounding content of, and access to, CMC in the workplace. For that reason, the author offers this guide, containing pertinent questions to ask oneself when considering development of organizational CMC policy:

1. Is there a need for an organizational CMC policy?

Initially, there should be a thorough understanding of the extent to which CMC is used within the organization. Has the organization established its own network--and for what purpose(s)? Is the network effective in helping people work toward goals, or could it be scrapped for a non-electronic system? Who participates in CMC on the network--and do they need to do so to complete their task assignments? Is the CMC carried out strictly within the workplace, or are employees of the organization using their modem-equipped PCs to involve themselves in CMC which extends outside the physical boundary of the workplace? (Areas of off-premises conduct by employees in which the organization has determined it has a legitimate interest need to be specifically identified--and communicated to employees. Improper behavior during nonwork time or in off-premises situations--which are specifically addressed in a code of conduct agreement--may then be subject to disciplinary action in accord with an organization's CMC policy.)

Of course, any policy which is created to govern conduct needs to be absolutely clear and fully explained in the context of all possible workplace situations where it might be applied.

2. If there is a need for an organizational CMC policy, who should be involved in formulating that policy?

Clearly, no one can be expected to write a policy on a subject he or she does not understand. While it is important to obtain input from all sectors of the organization, it is equally if not more important to obtain input from the people most knowledgeable about the subject.

If the policy is to apply throughout the organizational hierarchy, then certainly it should be developed with the participation of upper management, middle management, the rank-and-file employees, clerical staff, and the organization's legal counsel.

It is important to involve legal counsel to assure that the policy does not run afoul of statutory limits and legal requirements--especially in regard to the National Labor Relations Act. (Nobile, 1990, has written a brief but comprehensive review of the NLRB requirements and expectations with regard to organizational BBS systems and employees' right to be informed about workplace issues.)

Regardless of which individuals--from what levels of the organizational hierarchy--are chosen to sit on the committee to develop a CMC policy, the author agrees with Tatel (1990) that such policies are best developed through open-door sessions. Tatel urges policy writers to let CMC regulations "evolve from a process that includes all elements of the institution" (1990, p. B3) with testimony taken in a series of hearings over an extended period of time that allow for plenty of comment from anyone who has the potential to be affected by policy. A policy developed in this fashion is not only more representative of the individuals and organization it serves, but will be much more defensible should it be challenged in court later. It goes without saying, of course, that once the decision to implement a policy has been made, everyone who works within the organization needs to be fully informed that the policy

has taken effect, what it allows and does not allow, what the regulation and enforcement procedures are, and what the penalties are for those who violate the new policy.

3. If a policy is to be formulated, exactly what is it being formulated to prevent--and what will it be designed to support?

If those constructing a policy know beforehand what they're aiming at, they will be able to create a policy that is specific and limited. If the policy were to be developed the other way around, that is, before problem(s) had been identified--the policy would end up being either vague and too broad-based, or narrow and non-encompassing.

A policy which--for example--prohibits certain types of speech within an organizational BBS will be more effectively written if there's agreement before hand on what speech is to be prohibited. Also, the writers of such a policy will be able to make a stronger defense of their actions later, should a legal challenge be raised on First Amendment grounds.

The policy can be as narrow as to prohibit personal attacks or "flaming" in corporate E-Mail messages--or as lengthy as to cover proper etiquette for E-Mail and BBS messages throughout the organization (Turner, 1988).

The policy is also likely to be more enthusiastically supported by the rank-and-file if it is presented in a way in which the positive, beneficial attributes of the policy are highlighted (employees should be shown what the policy does for them--does it reduce uncertainty about their jobs, allow them more freedom to communicate in certain ways, allow them to cut down their work load by concentrating on some tasks while letting go of others, etc.--?).

4. Who will be the individual to ensure the policy is enforced--and, if violations occur, how will they be detected?

Ideally, there should be one individual who has ultimate authority for supervision of an organizational CMC system and assuring that it is maintained and used in accordance with organizational expectations. The duties of this individual would vary from organization to organization, but basically he or she should be a "computer supervisor" as proposed by Wepner & Kramer (1984). As such, he or she may have technical skill (computer proficiency, a knowledge of hardware and software, knowledge of programming languages, awareness of computer organizations and consortia, and an understanding of computer applications); interpersonal skill (the ability to work one-on-one and in groups with others, effective communication skills, cultivation of resources, and community involvement skills/experience); and managerial skills (ability to direct and organize people and programs, budget planning and management, program evaluation ability, scheduling knowledge, leadership ability).

Based upon the hierarchy of the individual organization and the configuration of the computer system, the individual charged with supervising CMC and regulating policy for its use would enforce proper use and cite employees for improper applications of the rules.

5. What will be the consequences for individuals who break the policy?

Again, this is an area that has to be fully developed in the body of the policy, so that it is clear from the start what consequences will be for violation. Exact operationalizations will vary from organization to organization, but it is critical that procedures be in place to deal consistently with all infractions. All those who violate the rules must be identified, and all those identified must be disciplined in the same manner. If the policy is inconsistent in this regard, it will surely fail to effect the behavioral change sought.

Any CMC policy must be uniformly introduced and enforced throughout the organization. If some employees are made to follow the policy while others are not, great dissatisfaction will occur--no matter how appropriate the policy may be.

In addition to asking for equal sacrifice from all members of the organization, the policy must be written and enforced to assure that all individuals accused of infractions of the rules are treated fairly and equally. From the C.E.O. or down to the janitor's helper, everyone who breaks a policy rule must be detected, cited, and dealt with in an adjudication system. As with any employee grievance matter, the worker who stands accused must have the opportunity to defend himself or herself before an unbiased individual or group of individuals charged with hearing appeals and handing out punitive sanctions. No exceptions to the policy can be allowed.

6. How will the policy face review to assure that the outcome of the policy is consistent with the goals originally established for it?

A regular review process must be written into the policy so that individuals from all levels of the hierarchy have the opportunity to re-think the policy, re-examine how it works for them in their jobs, and interact with others about the appropriateness of continuing the policy. The formation and maintenance of an organization's CMC policy should not be a "management job"--nor should it be "the workers' job"; it's everyone's job, because the establishment and carrying out of a sound policy protects and benefits everyone within the workplace.

7. If future adaptation and alteration is needed, how can this be accomplished without scrapping the policy foundations already established?

The ability to fine-tune CMC policy goes hand-in-hand with the evaluation process. The organization must be able to conduct a comprehensive evaluation of the policy and its

ability to meet goals--and then alter that policy as needed to make it stronger and more applicable. As much as possible, the alteration must take place without disrupting rules and regulations that workers have become accustomed to working within. As with the review process delineated in (6) above, individuals from all levels of the organization must be encouraged to participate in the process.

For organizations lacking a CMC policy--or lacking a policy that works effectively to balance needs of the organizational structure with the wants and desires of workers within it--these questions may serve as an effective precursor to action. They lend themselves to the creation of a CMC policy that is appropriate for each organization's particular needs and goals because they take into account the needs of the organization and its people. Most importantly, they involve the people within the organization in the decisions that affect them.

The author agrees with Carroll (1975), who believes that society's need to protect the status quo while preserving the privacy and empowerment rights of the individual "calls for the use of more information, not less" (Carroll, 1975, p. 296). CMC is critical in this process, so it must be effectively initiated and managed. It is hoped this guideline may suggest effective means toward that end.

References

Alexander, M. (1991, March 4). Pirate boards a perplexing problem. Computerworld, p. 83.

Allred, S. (1988, Spring). School personnel records: New requirements for ensuring employee privacy. School Law Bulletin, p. 1-5.

American Bar Association. (1987). Law in the workplace: You and the law series. Chicago, IL.

Belsie, L. (1992, March 26). Publishing without paper or ink. The Christian Science Monitor, p. 12.

Bogen, D. S. (1984). Bulwark of liberty: The court and the First Amendment. Port Washington, NY: Associated Faculty Press.

Brennan, L. (1991, August 12). Novell raids two bulletin boards in antipiracy campaign. Consumer Computers and Electronics, pp. 97-99.

Burke, S. (1989, January 23). Cutbacks spur prolonged IBM exodus: Despite solid performance, further consolidation expected. PC Week, p. 53,54.

Canipe, S. L. (1983). Business computers. (ERIC Document Reproduction Service No. ED 231 064)

Carey, J., & Coy, P. (1991, December 16). The new IBM. Business Week, p. 112-118.

Carroll, J. M. (1975). Confidential information sources: Public & private. Los Angeles: Security World Publishing.

Carroll, P. (1991, May 29). Akers to IBM employees: Wake up! Wall Street Journal, p. B1, B2.

Carroll, P. (1991, August 7). Computers indicate mood at big blue is practically indigo. Wall Street Journal, p. A1, A4.

Carroll, P. (1991, October 1). IBM is said to plan tougher reviews of performance of employees in the U.S. Wall Street Journal, p. A5.

Cerf, V. G. (1991, September). Networks. Scientific American, pp. 42-51.

Collingwood, H. (1991, December 9). IBM raises the ax again. Businessweek, p. 44.

Connolly, T., Jessup, L. M., & Valacich, J. S. (1990). Effects of anonymity and evaluative tone on idea generation in computer-mediated groups. Management Science, 36, 97-120.

Cressy, C. L. (1984, October). The electronic PAW. Currents, p. 22-24.

Depke, D. A. (1991, December 16). Any complacent IBMers left? Business Week, p. 115.

Dershowitz, A. M. (1991, November 11). The old itch to censor finds a new medium. The Los Angeles Times, p. B5.

Dertouzos, M. L. (1991, September). Communications, computers and networks. Scientific American, pp. 30-37.

DeSanctis, G., & Gallupe, R. B. (1985, Winter). Group decision support systems: A new frontier. Data Base, p. 3-10.

DeSanctis, G., & Gallupe, R. B. (1987). A foundation for the study of group decision support systems. Management Scie e, 33(5), 589-609.

D'Souza, D. (1991, April 24). In the name of academic freedom, colleges should back professors against students' demands for "correct" views. Chronicle of Higher Education, p. B1, B3.

Duggan, P. (1990, January 6). Md. man gets three years in bombing. Washington Post, p. A1, A22.

Dyson, E. (1991, January 7). Random access: Hacker's rights. Forbes, p. 268.

Elmer-Dewitt, P. (1991, April 8). Cyberpunks and the Constitution. Time, p. 81.

Finholt, T., & Sproull, L. S. (1990). Electronic groups at work. Organization Science, 1(1), 41-64.

Friedman, B. (1990, April). Moral responsibility and computer technology. Paper presented at the annual meeting of the American Educational Research Association, Boston, MA.

Glowacki, M. et al (1988, November). A survey of university students' behavior, knowledge, and opinions regarding unauthorized copies of computer software. Paper presented at the annual meeting of the Mid-South Educational Research Association, Louisville, KY.

Grolier Electronic Publishing, Inc. (1992). Constitution of the United States (Prodigy Interactive Personal Service document). New York: Author.

Hentoff, N. (1990, February). First amendment racketeers. The Progressive, p. 12-13.

Hiltz, S. R., & Turoff, M. (1978). The network nation: Human communication via computer. Reading, MA: Addison-Wesley.

Hume, B. (1989, February 6). A primer on using an electronic bulletin board system. Washington Post, pp. 30, 31.

Kahn, F. J. (Ed.) (1984). Documents of American broadcasting. Englewood Cliffs, NJ: Prentice-Hall.

Kalven, H. (1988). A worthy tradition: Freedom of speech in America. New York: Harper & Row.

Keen, P. G. (1990). Telecommunications and organizational choice. In J. Fulk & C. Steinfeld (Eds.) Organizations and Communication Technology (pp. 295-312). Newbury Park, CA: Sage Publications.

Kiesler, S B. (1967). Social aspects of computer environments. Social Science, 72(1), 23-28.

Kiesler, S. & Sproull, L. (1987). The social process of technological change in organizations. In S. Kiesler and L. Sproull (Eds.) Computing and change on campus. New York: Cambridge University Press.

Kiesler , S., Siegel, J., & McGuire, T. W. (1984). Social-psychological aspects of computer-mediated communication. American Psychologist, 39, 1123-1134.

Klausmeier, J. (1984). Networking and microcomputers. (ERIC Digest Report). Syracuse, NY: ERIC Clearinghouse for Information Resources. (ERIC Document Reproduction Service No. ED 253 326)

Kramer, M. (1990, July 23). Fighting back against the fed's BBS crackdown. PC Week, p. 58.

Lacy, A. (1991, January 31). When is gardening a subversive act? The New York Times, p. C1, C10.

Landberg, T. (1986). Electronic bulletin boards. Washington, DC: National Bureau of Standards (ERIC Document Reproduction Service No. ED 325 112).

Levinson, P. (1990). Computer conferencing in the context of the evolution of media. In L. M.

Harasim (1990) Online education: Perspectives on a new environment, pp. 15-38. New York:Praeger.

Lewis, G. (1989, March 6). Is the computer business maturing? Business Week, pp. 68-78.

Lindquist, C. (1991, May 6). File data upsets Prodigy users. Computerworld, p. 4, 5.

Lindquist, C. (1991, December 9). "Child porn" sent on America On-Line. Computerworld, p. 7.

Malone, T. W., & Rockhart, J. F. (1991, September). Computers, networks and the corporation. Scientific American, pp. 92-99.

Manning, R. (1992, May). Dial a BBS for low-cost and timely info. Home-Office Computing, pp. 48, 49.

Miller, M. W. (1991, October 21). A new medium: Bulletin boards become a major means of communication. Wall Street Journal, p. R8.

Miller, M. W. (1991, October 24). Prodigy computer network bans bias notes from bulletin board. Wall Street Journal, p. B1, B6.

Negroponte, N. P. (1991, September). Products and services for computer networks. Scientific American, pp. 76-83.

Nelson, H. L. & Teeter, D. L. (1982). Law of mass communications: Freedom and control of print and broadcast media (4 ed.). Mineola NY. Foundation Press.

Nobile, R. J. (1990, June). Keeping posted on bulletin boards. Personnel, p. 12-14.

Oldenburg, D. (1991, October 1). Rights on the line. Washington Post, p. E5.

Pinsonneault, A., & Kramer, K. L. (1989). The effects of electronic meetings on group processes and outcomes. Decision Support Systems, 5, 197-216.

Rifkin, G. (1991, December 9). Mitchell Kapor: The in-depth interview. Computerworld, pp. 73-75.

Rockhart, J. F., & Short, J. E. (1991). The networked organization and the management of interdependence. In M. S. Scott Morton (Ed.), The Corporation of the 1990s: Information Technology and Organizational Transformation (pp. 198-219). New York: Oxford University Press.

Rothfeder, J., & Schwartz, E. I. (1990, August 6). Commentary: Computer anarchism calls for a tough response. Business Week, p. 72.

Scarborough, B. (1992, March 20). Computer bulletin boards. (Available from Communication Research and Theory Network, Pennsylvania State University)

Schwartz, J. (1991, November 4). A screenfull of venom. Newsweek, p. 48.

Segal, T. (1990, November 26). From PC user to schmoozer. Business Week, pp. 192, 193.

Shepard, I. M., & Olsen, H. (1986). Employee privacy rights: A management guide.

Washington, DC: College and University Personnel Association (ERIC Document Reproduction Service No. ED 275 272).

Sproull, L. (1986). Using electronic mail for data collection in organizational research. Academy of Management Journal, 29(1), 159-169.

Sproull, L., & Kiesler, S. (1991, September). Computers, networks and work. Scientific American, pp. 84-91.

Sullivan-Trainor, M. (1991, December 9). IBM head-rolling may be healthy exercise. Computerworld, p. 23.

Tatel, D. S. (1990, February 7). Clear, narrow policies on offensive speech may not run afoul of the First Amendment. Chronicle of Higher Education, p. B1-B3.

Tesler, L. G. (1991, September). Networked computing in the 1990s. Scientific American, pp. 54-61.

Tribe, L. H. (1991, September/October). The constitution in cyberspace: Law and liberty beyond the electronic frontier. The Humanist, pp. 15-21, 39.

Turner, J. A. (1990, January 24). Messages in questionable taste on computer networks pose thorny problems for college administrators. Chronicle of Higher Education, p. A13, A16.

Turner, J. A. (1988, April 13). "E-mail" technology has boomed, but manners of its users fall short of perfection. Chronicle of Higher Education, p. A1, A16.

Uncapher, W. (1991, September/October). Trouble in cyberspace: civil liberties at peril in the information age. The Humanist, pp. 5-14, 34.

Ware, W. H. (1984, Summer). Information systems, security, and privacy. EDUCOM, p. 6-11.

Weintraub, W. (1986, April). Computer piracy and the myth of computer innocence. School Administrator, p. 8-10.

Weiss, J. M. (1992, February 18). Rural business takes a fiber-optic leap. Christian Science Monitor, p. 7.

Wepner, S. B., & Kramer, S. (1984). The computer supervisor: Your next administrative hire. (ERIC Document Reproduction Service No. ED 257 417)

Zachmann, W. F. (1991, February 26). Corporate e-mail and bulletin boards. PC Magazine, pp. 95-96.