CURRENT ISSUES RELATED TO COMPUTER NETWORKS, E-MAIL AND USE OF COMPUTERS ON CAMPUS

Presenter:

PAUL J. WARD
General Counsel
Arizona State University
Tempe, Arizona

Stetson University College of Law:

16TH ANNUAL LAW & HIGHER EDUCATION CONFERENCE
Clearwater Beach, Florida
February 12-14, 1995

Current Issues Related to Computer Networks, E-mail and Use of Computers on Campus

Paul J. Ward
General Counsel
Arizona State University

Presented at the
16th Annual National Conference on Law and Higher Education
February 12-14, 1995

1. Introduction.

The ubiquity of computers on campus requires increasing amounts of time and effort of university administrators. Campus officials must at once meet demands for improved information technology and then deal with issues resulting from the use of this technology. The context of these electronic issues includes not only traditional workplace, classroom, and library/laboratory environments, but also the campus as a gateway to the Internet.

More specifically, information technologies such as electronic mail and computer bulletin boards present a wide variety of apparently unique issues. A threshold consideration for university counsel, then, is to determine whether the issue is capable of being addressed under some existing legal principle and/or by analogy to some traditional theory of law or, in the alternative, if the issue actually requires the application of some development of cyberlaw.

There have been significant legal developments in the field of computer law. The legislative process has brought and promises to bring attention to certain issues in the fields of computer fraud, privacy, and intellectual property. [See, e.g., Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 *et seq.*; Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* and § 2701 *et seq.*; Electronic Freedom of Information Act of 1994 (HR 4917 & S 1782

not enacted by the 103rd Congress); and with respect to state legislation Seth E. Lipner and Stephen Kalman, Computer Law: Cases and Materials 539-44 (Merrill Publishing, 1989)] Indeed the single greatest decision the government may make is the extent to which the electronic environment will be privatized. [See Herbert I. Schiller, "The 'Information Highway': Public Way or Private Road," The Nation, p. 64, July 12, 1993] But the legislative process is slow to react to rapid developments in technology.

Similarly, the common law has been slow to fill the gap. It is the nature of American jurisprudence that only as colleges and universities attempt to manage computers on campus will the courts be asked to address the conflicts which result. Recent and well publicized incidents at several institutions including Santa Rosa Junior College (sexual harassment), Carnegie Mellon University (obscenity), MIT (copyright infringement), Texas A & M University (death threat), and The University of Michigan (freedom of information) highlight the anxiety campus administrators must feel in this area. The development of a campus policy statement on the use of computers appropriate to the particular campus can be an important means to avoid such conflicts.

This paper will explore certain privacy issues, developing theories of liability regarding administration of computer networks, access to electronic information, and the development of a computer use policy in the university setting.

2. Quick Overview - Background FAQ's.

A. What is a FAQ?

A FAQ is frequently asked question.

B. What is the Internet?

The Internet refers to global, interconnected networks which communicate via Internet Protocol (IP). A communications protocol allows different kinds of computers with various operating systems to speak to each other. In short, it is a network of networks. The origins of the Internet trace to 1969 when the Defense Department created ARPANET to transmit military data around the world and to pursue other military objectives. Today it connects educational institutions with individuals, business organizations, and the government. With over three million networks in 160 countries and a growth rate of nearly 20% per month the growth of Internet is phenomenal.

C. What is E-mail?

A term described as "various electronic communications systems which permit quick and accurate written communication without the need to print on paper.... E-mail differs from true mail since it sends text (and occasionally audio or graphic information) in digitized form from one person to another, and is capable of sending information simultaneously from one to many people." [Thomas, Robert H. "Hey, Did You Get my E-Mail?" 44 Journal of Legal Education 239 (June 1994)] At this time it is estimated that one-half of the traffic on the Internet is e-mail and that by the year 2000 forty million users will send sixty billion messages per year.

D. What is a computer bulletin board?

A computer bulletin board system (BBS) may be established with a computer running bulletin board software and a modem connected to a telephone. There are thousands of BBS's operating today ranging in size from wholly private boards to the major commercial services which include CompuServe, Prodigy and America Online. Many universities host bulletin boards in various disciplines and administrative areas. A Sysop is the system operator.

3. Privacy Issues.

A. Communication. "The vast majority of Americans believe that computers have improved the quality of their life..., but they are also extremely worried about the lack of privacy in the computer age...." [M. Betts, "Computers Invade Privacy," Computerworld, 12 (November 23, 1992)] This view is surely maintained by university students and employees as well. And with good reason. Universities have established a practice of collecting information and retaining communication records either in a centralized computing services facility and/or in decentralized personal computer environments.

Three major studies in the past two decades have recognized the loss of privacy resulting from the computerization of information systems and recommended the establishment of a permanent new governmental privacy agency. Nevertheless, none have moved beyond the hearing phase due to the anti-regulatory mood of the country in general and opposition from the business community in particular. [Robert Gellman, "Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions," 6 Software Law Journal 236 (1993)]

Noting that the right to privacy derives variously from the U.S. Constitution, state constitutions, statutory sources, and the common law, one author has observed that "none of these four sources adequately protects an employee's privacy in the computerized workplace." [Steven Winters, "The New Privacy Interest: Electronic Mail in the Workplace," 8 High Technology Law Journal 200 (1993)]

A leading case in the area of workplace privacy is O'Connor v. Ortega, 480 U.S. 709 (1987). In Ortega the Supreme Court balanced the competing interests of a public employee's legitimate expectation of privacy and the government employer's need for supervision, control and operation of the workplace. The Court held that a reasonableness standard obtains for

noninvestigatory, work-related purposes as well as for investigations of work-related misconduct. The Court noted that the government's interest in an efficient workplace outweighs the public employee's privacy interests, although the court concluded that Ortega had a reasonable expectation of privacy in his desk and file cabinets. However, the public sector supervisor investigating for criminal activity subjects the government employer to traditional Fourth Amendment constraints.

Winters asserts that the analytical approach in Ortega "probably excludes protection of computer technologies like E-mail." [8 High Technology Law Journal 205 (1993)] Another author argues that "an invasion of an individual's e-mail is an invasion of privacy" because (i) the e-mail system operates in a similar manner to an employee placing a document in a file cabinet or desk drawer, (ii) the e-mail system stores messages for later retrieval, (iii) the employee thinks s/he has exclusive use of the e-mail because of personal password access, and (iv) correspondence is personally addressed to an intended recipient also with password security. [Comment, "Terminally Nosy: Are Employers Free to Access our Electronic Mail?," 96 Dickinson Law Review 545 at 558 (1992)]

Perhaps Harvard Professor Lawrence Tribe concluded that an amendment to the Constitution is needed to protect individuals from inappropriate uses of computer technology in part because of the failure of the privacy initiatives. In any event he proposed a 27th amendment to the U.S. Constitution in an address "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier" at the First Conference on Computers, Freedom & Privacy (March 26, 1991) as follows:

> The Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protection against unreasonable searches and seizures and the deprivation of life, liberty or property without due process of law shall be construed as fully applicable without regard to the technological method of medium through which information content is generated, stored, altered, transmitted, or controlled.

Whether or not a Constitutional amendment is indeed necessary colleges and universities should exercise responsible leadership to address this issue. Perhaps the most important statement the university can make in this area is a clear policy statement on which communication records are private and the extent to which monitoring activity, if any, will occur. This should include e-mail and voice mail as well as traditional file information. The statement should also include an explanation of the record retention procedures.

B. Free Expression. Electronic communication technology has revived the era of the pamphleteer, one commentator has observed, because the cost to operate a bulletin board is much less than any other media and the technology offers the capacity for instant, multiple and interactive communication. [Comment, "Computer Bulletin Boards and the First Amendment," 39 Federal Communications Law Journal 217 at 223 (1987)] The technology is not only being utilized by academics for scholarly discussion. It is used for many purposes including commerce, political expression, humor, and by every imaginable interest group. It is also subject to abuse and has been used for criminal and other antisocial purposes. Indeed, it is thought that "computers have replaced magazines and videotapes as the primary means of distributing child pornography." [Note, "PC Peep Show: Computers, Privacy, and Child Pornography," 27 The John Marshall Law Review 990 (1994)]

Are computer bulletin boards the public fora of the 21st century? To be sure the First Amendment has been applied to the public university in a variety of contexts. There is no reason to believe that campus computer bulletin boards will be treated any different from other campus facilities meaning public institutions may subject both commercial and noncommercial speech to the reasonable constraints regarding time, manner and place. Whether or not cyberspace itself

is a public forum, however, is subject to debate. [Edward J. Naughton, "Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech, and State Action," 81 The Georgetown Law Journal 409 (1992)]

A controversial subject related to free expression is the matter of anonymity. So-called "apparent anonymity" allows a subscriber to a particular BBS to use a pseudonym and remain anonymous to other subscribers while the operator of the system can always trace the origin of a particular message. On the other hand, "true anonymity," offered by anonymous remailers or achieved by forged posting may mean that no one can identify the origin of the posting. Noting the potential for damage to reputation, spreading misinformation, and criminal activity and an unwillingness to grant service providers a legal safe harbor of immunity, one author argues for the establishment of industry-wide procedures for responding to copyright complaints, a commitment to right of reply in defamation cases, assumption-of-risk clauses in user agreements, and "promotion of a code of ethics for those who provide and for those who use anonymity." [Mike Godwin, "Who Was That Masked Man?," Internet World, 24 (January, 1995)]

4. Computer Networks.

Colleges and universities and sysops are concerned about institutional/individual liability resulting from the operation of computer bulletin boards. Posting of alleged defamatory or harassing messages are significant areas of exposure. In addition, network operators must consider general (negligence) liability issues as well as the exposure to prosecution for criminal acts of subscribers (e.g. publication of stolen credit card numbers).

In Cubby, Inc. v. CompuServe, Inc., 776 F.Supp. 135 (S.D.N.Y.1991), the court dismissed the first libel action filed against a commercial computer service on CompuServe's motion for summary judgment. CompuServe did not dispute that the statements at issue were

defamatory; however, it asserted that it had a contractual relationship which required prompt posting and no editorial control over the publication. Also, CompuServe asserted that it was a distributor and not a publisher. The district court concluded "[g]iven the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory ... statement." [776 F.Supp. at 138]

Although the Cubby decision is favorable to computer network operators, it may be of limited value because it was decided by summary judgment and also because computer networks do not fit neatly into a single classification. [Terri A. Cutrera, "Computer Networks, Libel, and the First Amendment," 11 Computer/Law Journal 555 at 579 (1992)] This view will be tested soon as another commercial bulletin board, Prodigy, has been sued for allegedly allowing third parties to post defamatory messages. If the result in this matter is different from Cubby it may be because Prodigy claims to be a "family-oriented" service and has assumed a greater duty of care. [New York Law Journal, p. 1 (December 6, 1994)]

5. Access to Electronic Data.

E-mail communications and other electronic data are increasingly sought in public records requests and through discovery in litigation. Indeed a recent article concluded with the observation that failure to seek electronic information may constitute legal malpractice. [Joseph M. Howie and Deborah Solomon Miller, "Electronic Media Discovery," Trial, 58 (March 1994); see also, Michael J. Patrick, "E-Mail Data Is a Ticking Time Bomb," The National Law Journal, p. 13 (December 20, 1993)]

In federal litigation matters, although subject to attorney-client and work product privileges, it is well established that e-mail, electronic bulletin board messages and automatic

computer backup files are data compilation documents within the scope of Rule 34 of the Federal Rules of Civil Procedure. Raids have been permitted to conduct on-premise searches to prevent destruction of software. [Quotron v. Automatic Data Processing, Inc., 141 F.R.D. 37 (S.D.N.Y. 1992)] The Software Publishers Association has been effective in securing ex parte orders to determine whether or not an organization is using unlicensed software. [See "Use of Freedom of Information Act (5 USCS § 552) as Substitute for, or as a Means of, Supplementing Discovery Procedures Available to Litigants in Federal Civil, Criminal, or Administrative Proceedings," 57 A.L.R. Fed. 903]

Access to electronic data under state public records statutes seems equally likely even if the law is not well settled. Courts do differ, however, on whether the requester has the right to request information in a particular medium (e.g. computer tape, computer disk, microfiche etc.) or format. ["State Freedom of Information Act Requests: Right to Receive Information in Particular Medium or Format," 86 A.L.R. 4th 786]

In Star Publishing Co. v. Pima County Attorney's Office, ___ P.2d ___, 1994 WL 425342, 22 Media L. Rep. 2381 (Ariz. App. 1994) the Arizona Court of Appeals affirmed an order to release computer backup tapes of the Pima County Assessor's Office containing all documents for 1993 including e-mail communications of employees. The court rejected a so-called deliberative process privilege recognized in Rogers v. Superior Court, 19 Cal. App. 4th 469, 23 Cal. Rptr. 2d 412 (1993) under the California Public Records Law.

In a pending matter involving the University of Michigan the plaintiff sought access to copies of certain computer conferences involving various members of the UM Board of Regents allegedly conducted in violation of the Michigan Open Meetings Law. In fact the electronic information which was the object of the litigation was released to the plaintiff in April, 1994. The matter now proceeds on the narrow issue of whether UM's initial denials were arbitrary and

capricious and thereby entitle the plaintiff to claim actual or compensatory damages and punitive damages. The litigation may yet provide guidance on whether or not these electronic conferences are public records within the meaning of the Michigan FOIA or are otherwise exempt from disclosure under Michigan law. [Zarko v. Board of Regents of the University of Michigan, Civil Action No. 93-1817-CZ]

6. Campus Computer Policies. (See Appendix A)

A. Evaluate the culture of the institution.

B. Establish a set of governing principles in the policy statement.

1) scope of coverage e.g. faculty, staff, students, and guest users;

2) extent of privacy - right to monitor;

3) specify acceptable and prohibited uses regarding the following:

- o commercial solicitation,
- o political expression,
- o libelous material,
- o electronic harassment,
- o extensive personal use,
- o ability to install personally-owned software on university computers.

C. Name an individual /unit responsible for administration of the system.

D. Communication.

E. Training program.

F. Compliance mechanisms.

7. Hypotheticals.

(1) A public college instructor creates gender separated electronic conference groups at the request of enrolled students in a credit course. The conferences are private (not anonymous) and are conducted subject to a protocol of confidentiality. A series of messages are posted which are alleged to constitute sexual harassment violative of Title IX. What claims and theories of liability may the college expect? Is the result any different if the postings are not on a gender separated conference?

(2) A hacker posts a message which contains racial slurs to a Usenet discussion group causing readers to believe that it was sent by a faculty member at your institution. Your faculty member is receiving hundreds of "reply" messages -- including death threats. What do you do?

(3) You serve as counsel to a public university. Your institution's computer postmaster receives the following message. "Someone with a computer address at your institution has been especially offensive in his postings. The latest message is attached. Kindly stop this nonsense. 'Every man, woman, that can carry a gun or can shoot of the Zionist Jews is considered a target. This means that killing such a person, terrorizing such a thug is a duty for every Muslim and for every Freedom Fighter.... This Terrorizing act is fine since it is directed against Thugs that robbed Palestine from the Inhabitants and expelled them out and never allow them back only because they loved Jesus and Mohammed.'" In light of the First Amendment what do you advise the postmaster?

(4) Upon request a public university issues student Jane a computer account. This account permits Jane to send e-mail messages to other students and faculty/staff on campus. It also permits Jane access to the Internet. Jane does not wish to receive unsolicited commercial messages. May the university regulate such commercial speech?

(5) Olson writes from Scandinavia that a university official has corresponded via Internet and offered a graduate assistantship to Olson. Olson replied with an acceptance also via Internet. University communicates by telephone that the person corresponding with Olson lacked contract authority. Olson states that she believed the University's representative had authority to make the offer, that she relied upon this representation, and that she has made preparations to immigrate to the United States. Has the university made a legally enforceable contract with Olson?

(6) John is a staff employee at a public university. John wishes to advertise on a university computer bulletin board a service of home installation of Internet access software and appropriate training which he will provide outside of his regular university work schedule. May the university regulate such commercial speech? Jack wishes to send a political endorsement electronically to all other employees. May the university regulate this political speech?

(7) Jill, a staff employee at a private university, sends the following message to selected fellow employees: "This message has been sent to you for good luck. The original is in New England. It has been sent around the world nine times. The luck has now been sent to you. You will receive good luck within four days of receiving this message - provided you, in turn, send it on. This is no joke.... This message must leave your hands in 96 hours." Is this a problem for the university attorney?

APPENDIX A

UNIVERSITY OF TULSA
COMPUTER USE POLICY

The following policy, rules, and conditions apply to all users of University of Tulsa's computer and telecommunication resources and services. Violations of this policy are unethical and possibly unlawful. In accordance with established University practices, violations may result in disciplinary action that could result in expulsion from the university or dismissal from a position, and /or legal action.

I. PURPOSE

To establish a policy to ensure the provision of computer and telecommunication resources and services to the faculty, staff, and students of University of Tulsa ("UT"). This policy applies to the use of all institutional data regardless of the office in which it resides or the format (paper, film, electronics, etc.) in which it is used.

II. POLICY

UT strives to provide all computer users with privacy and a fair share of technical resources. All computer users have the responsibility to use the UT computer resources in an efficient, effective, ethical, and lawful manner consistent with the Rules and Regulations of the University. The ethical and legal standards that all users should maintain are derived directly from standards of common sense and common decency that apply to the use of any public resources within the University and are documented in local, state, and federal statutes and UT codes, rules, regulations, policies, and procedures.

UT seeks to protect computer-based information, recognized as a primary administrative, educational and research asset, from accidental or intentional unauthorized modification, misuse, destruction, disruption, or disclosure. In order to make every reasonable effort to protect the integrity of its computing systems, workstations, networks, lab facilities, etc., the University has the right to monitor its computing resources.

UT has an obligation to respect the privacy of a user's files, electronic mail, and printer listings to the best of its ability. With reasonable cause for suspicion, UT has the right to monitor any and all aspects of a system, including individual login sessions to determine if a user is acting in violation of the policies set forth in this document or as stated by law.

Computer users are governed by the following provisions which apply to all use of computing and telecommunication resources. Computing and telecommunication resources include host computer systems, University-sponsored computers and workstations, software, datasets, and communications networks controlled, administrated, or accessed directly or indirectly by UT computer resources or services, employees, or students.

1. USERS MUST ABIDE BY ALL SOFTWARE LICENSES, UT COPYRIGHT AND INTELLECTUAL PROPERTY POLICIES AND APPLICABLE FEDERAL AND STATE LAWS.

2. Users are responsible for safeguarding their user identification password. Users should not print, store on-line, or give their ID password to others. The user is respnsible to make authorized usage of the ID for its inteded purpose only. Each user is responsible for all transactions made under the authorization of his or her ID.

3. Computer users shall not intentionally seek, provide, or modify information in or obtain copies of files, programs, or passwords belonging to other computer users without the permission of those other computer users. This includes all system files and accounts.

4. Files controlled by individual users are considered private, whether or not they are accessible by other users. A user must obtain written permission from the owner of a file to alter or copy a file that does not belong to him or her. The ability to read, alter or copy a file does not imply permission to read, alter, or copy that file.

5. Each account owner and workstation user is solely responsible for the usage incurred through her/his account or workstation. Individuals who intentionally abuse accounts and privileges, degrade system performance, misappropriate computer resources or interfere with the operation of the computer and/or telecommunication facilities are subject to disciplinary action. The removal, modification, or reconfiguration of files on UT computer hardware or software is prohibited.

6. The electronic communication facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, destructive programs, political material, or any other unauthorized or personal use.

7. The development and/or use of self-replicating code is allowed only under the direction of the academic faculty and the department of Administrative Information Systems.

8. Computer users will use network links solely for the purpose permitted in the network guidelines (e.g., BITNET, Internet). Users are responsible for obtaining and adhering to all network acceptable use policies.

9. The ability to connect to other systems through the network does not imply the right to connect to these systems or to make use of these systems unless properly authorized by the owners of those systems.

10. Users share many resources, such as disk space, CPU cycles, printer queues, batch queues, login sessions, software licenses, etc. No user may monopolize these resources and should utilize these resources only to the extent necessary for purposes related to authorized use.

11. Computer users shall not intentionally develop or use programs that harass other computer users or that infiltrate the system and/or damage the software or hardware components of the system. Users have the right not to be harassed whether by physical, verbal, electronic, or other form of abuse and may complain or bring formal grievance through appropriate channels where the abuse complained of is by a UT authorized user, whether on or off campus.

12. Although each user has the right to freedom of speech, harassing or defamatory material may not be sent via electronic mail or posted to electronic bulletin boards, news groups, etc.

13. Use of the electronic communication facilities (such as electronic mail, telephone mail, or systems with similar functions) to send fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages is prohibited.

14. Users will not aid, abet, or act in conspiracy with another to violate any part of these policies, rules, and conditions.

15. Occasional proper personal use of computer equipment and software is permitted when personal use does not interfere with expected work performance or violate any applicable policy, rule, or law. An employee's performance appraisal may take into account personal use and a supervisor may require a change in personal use as a condition of employment where appropriate.