COLLEGE COMPUTERS IN THE FAST LANE: A REVIEW OF EMERGING LEGAL ISSUES AND TECHNOLOGY IN ELECTRONIC COMMUNICATION (VERSION 2.0)

Presenter:

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

Stetson University College of Law:

17th ANNUAL LAW & HIGHER EDUCATION CONFERENCE
Clearwater Beach, Florida
February 11-13, 1996
I. Introduction.

A professor at Eastern Washington University is suspended with pay after pornographic pictures of children were found on his campus computer. An investigation ensued to determine if the professor had violated any laws or university policies. [“Academe Today: Information Technology,” The Chronicle of Higher Education, August 11, 1995 at 19]

Political hate mail is posted to the Internet through a computer account at the University of Maryland. The messages originated at the University of Virginia, although it is believed a former student at Maryland created a computer account for the individual posting the messages. The University of Maryland regards this as a violation of the institution’s acceptable-use policy. [“Profusion of Electronic Hate Mail Puts School in a Bind,” San Francisco Chronicle, August 5, 1995 at A6]

At Cornell University four freshmen distributed a list of “75 reasons why women (bitches) should not have freedom of speech” to a small group of friends. The list was eventually posted to a USENET newsgroup accessible through the Internet prompting many complaints to the institution and death threats to the four students. [“Misogynistic E-Mail Sparks Controversy on Cornell Campus,” The Chronicle of Higher Education, November 24, 1995 at A20]
A student allegedly sent an electronic mail bomb overloading the university's computer system. The e-mail flooded the system with more than 24,000 messages in one day and prevented access by others for a period of five hours. The student was charged with federal computer fraud and the university was considering whether the student could be punished for violating the Monmouth University Code of Conduct. ["Academic Today: Information Technology," The Chronicle of Higher Education, December 18, 1995 at A21]

It is now abundantly clear that 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, library and 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 administrators and legal counsel alike is to determine whether the issue is capable of being addressed under some existing legal principle 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 and regulatory process has brought and promises to bring attention to certain issues in the fields of electronic records, computer fraud, privacy, and intellectual property. [See generally, Final Rule of the National Archives and Records Administration, "Electronic Mail Systems and Disposition of Electronic Records," 36 CFR Part 1220 et al., effective September 27, 1995; Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (September, 1995); Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030]

But in any event 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. The recent incidents mentioned at the beginning of this paper and other well publicized incidents too numerous to mention 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, access to electronic information, emerging theories of liability regarding administration of computer networks, and the framework for the development of a campus computer use policy.

II. Privacy Issues.

A. 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); see also, Dorothy E. Denning and Herbert S. Lin, Rights and Responsibilities of Participants in Networked Communities, (National Academy Press, 1994)] The technology is not only being utilized by academics for scholarly discussion; it is used for many purposes including commerce, political expression, and 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); see also, Marty Rimm, “Marketing Pornography on the Information Superhighway,” 83 The Georgetown Law Journal 1849 (1995)]

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 differently from other campus facilities, meaning public institutions may subject both commercial and noncommercial speech to reasonable constraints regarding time, manner, and place. Whether or not cyberspace itself is a public forum 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)] More recent scholarship, however, concludes that “it is unlikely that a public college or university could characterize the bulletin boards of its computer network as anything less than a limited open forum.” [Joseph C. Beckham and William Schmid, “Forum Analysis in Cyberspace: The Case of Public Sector Higher Education,” Ed. Law Rep. 11, 15, May 18, 1995] Accordingly, “[r]estrictions on the time, place and manner of speech in such a public forum requires that regulations be content neutral, reasonable, and narrowly tailored to realize significant institutional objectives.” [Id. at 17]

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 archived by forged posting may mean that no one can identify the origin of the posting.

The legal status of electronic anonymity and pseudonymity may be influenced by a recent decision of the United States Supreme Court. In *McIntyre v. Ohio Elections Commission*, 115 S. Ct. 1511 (1995), Ms. McIntyre had distributed a leaflet opposing a proposed school-tax increase. Following defeat of the school levy, the Ohio Elections Commission imposed a fine of $100 for violation of a state law which prohibited distribution of unsigned leaflets. Ultimately, on appeal to the U.S. Supreme Court, the statute was held unconstitutional. More specifically, the Court held “under our Constitution anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent ....” Thus, the freedom to publish anonymously is protected by the First Amendment. [*See generally*, Mark Eckenwiter, “Net.Law,” *Net Guide*, 37 (January, 1996)]

Also, 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)]

**B. 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 the practice of collecting information and retaining
communication records either in a centralized computing services facility 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 220 (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)] The term "personal computer" in a distributed computer environment, however, actually reinforces a perception of privacy. Also, it is argued 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)]

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 or 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.

III. 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, 13 (December 20, 1993); and Heide L. McNeil and Robert M. Kort, “Discovery of E-Mail and Other Computerized Information,” Arizona Attorneys, 16 (April 1995)]

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]

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.

Courts differ 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] However, the Ohio Supreme Court in State ex rel. Margolius v. City of Cleveland noted that “a set of public records stored in an organized fashion on a magnetic medium also contains an added value that inherently is part of a public record. Here, the added value is not only the organization of the data, but also the compression of the data into a form that allows greater ease of public access.” [584 N.E. 2d 665 (Ohio 1992)] Similarly, the Ohio Court of Appeals has held:

[t]he basic tenet ... is that a person does not come like a serf hat in hand, seeking permission of the lord to have access to public records. Access to public records is a matter of right. The question in this case is not so much whether the medium should be hard copy or diskette. Rather, the question is: Can a government agency, which is obligated to supply public records, impede those who oppose its policies by denying the value-added benefit of computerization? [Athens County Property Owners Ass’n Inc. v. City of Athens, 619 N.E. 2d 437, 439 (Ohio Ct. App. 1992)]

In a 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. The electronic information which was the object of the litigation was released to the plaintiff in April, 1994; however, the matter continued on the narrow issue of whether UM’s initial denials were arbitrary and capricious and thereby entitled the plaintiff to claim actual or compensatory damages and punitive damages. The litigation was concluded on a Motion for Summary Disposition finding the University in violation of
Michigan's Freedom of Information Act (FOIA) and not subject to the FOIA's privacy exemptions. The court also awarded the plaintiff reasonable attorney's fees, costs, and disbursements. [Zarko v. Board of Regents of the University of Michigan, Civil Action No. 94-3241-CK (June 30, 1995)]

IV. Computer Networks.

Colleges and universities and sysops are concerned about institutional and individual liability resulting from the operation of computer bulletin boards. Posting of allegedly 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 is a central issue in the Stratton Oakmont, Inc. v. Prodigy Services Company litigation matter which is pending at this writing. Prodigy is a joint venture of IBM Corporation and Sears-Roebuck & Company. It was organized
in 1990 and currently has more than two million subscribers. It was developed with the marketing strategy of a family-oriented computer network.

In October, 1994 a message was posted on Prodigy’s “Money Talk” computer bulletin board which stated Stratton Oakmont, a securities investment banking firm, and Daniel Porush, Stratton’s president, committed criminal and fraudulent acts in connection with the initial public offering of the stock of Salomon-Page Ltd. and that Stratton was a “cult of brokers who either lie for a living or get fired.” Stratton brought a $200 million libel and defamation suit.

Pursuant to a motion for partial summary judgment, Judge Ain held on May 24, 1995 that Prodigy is a “publisher” rather than a “distributor.” The importance of this distinction is that “distributors such as book stores and libraries may be liable for defamatory statements of others only if they knew or had reason to know of the defamatory statements at issue.” On the other hand “one who repeats or otherwise republishes a libel (i.e. a publisher) is subject to liability as if he had originally published it.”

In this case, notwithstanding the fact that 60,000 messages are posted daily on Prodigy’s bulletin boards, the facts that Prodigy Board Leaders may remove messages that violate Prodigy Guidelines, the use of an automatic screening program, and more importantly, that Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards, the New York Supreme Court (trial court) concluded that Prodigy is in fact a publisher. The court also expressly agreed with the holding in Cubby noting “Prodigy’s own policies, technology and staffing decisions ... (have) mandated the finding that it is a publisher.” For a critical discussion of Judge Ain’s decision, see Mike Godwin, “Leaky Logic,” Internet World 96 (February, 1996).

Sir William Blackstone, a noted 18th century English jurist, defines law as "a rule of civil conduct prescribed by the supreme power in a state, commanding what is right, and prohibiting what is wrong." Similarly, Oliver Wendell Holmes, an associate justice of the United States Supreme Court from 1902-1932, observed that law is a set of rules to enable the populace to predict how the judiciary will resolve a particular dispute -- "the prophecies of what the courts will do in fact, and nothing more pretentious, are what I mean by the law."

In my view, a sound policy statement on the use of campus computing systems, then, will enable the university community to know what is permitted and what is prohibited conduct, and it will enable campus administrators to respond to incidents in a manner which is contemplated by the policy. Paying careful attention to the rising tide of computer-related incidents some institutions have appointed study committees to recommend an appropriate policy. Many institutions have not reacted so quickly to this changing and volatile environment. The following section of this paper is devoted to some basic guidelines and governing principles in drafting a policy statement. At appropriate points this paper includes provisions from various institutional policies. These provisions have been selected as illustrative of particular points and are not intended in the aggregate as a model policy.

A. Basic guidelines:

(1) Computing System. Know the existing computing service function including both its centralized and distributed operations. In the absence of a policy statement the campus may have developed protocols or responded to incidents in a particular manner. This so-called "past practice" may be characterized as campus common law in the course of the campus' deliberations concerning new policy. Also, on an operational basis, computer administrators have made decisions regarding,
among other things, the length of time e-mail will be subject to automatic back-up. The policy should consciously ratify or modify those decisions which have policy implications.

(2) **Campus Culture.** Understand the culture of the institution; the existing system of governance may control the method of promulgating new campus policy statements. Also, whether the campus is a teaching or research institution or, indeed, the size of the campus may impact certain particulars of the computer policy.

(3) **Legal Environment.** Know the applicable statutory laws, regulations, and case law. Of course, being aware of federal laws and regulations referred to previously in this paper is necessary. Related state laws and even the enforcement attitude of the local prosecuting attorney are also important considerations.

(4) **Policy Approach.** Decide if the policy will be a university-wide, free-standing policy or a series of amendments to existing policies. The former would govern the entire university community in a self-contained policy statement, although it need not preclude the development of implementing procedures in certain units of the university such as the graduate college. If the latter approach is adopted special care must be taken to make certain there are no inconsistencies in potentially overlapping policies.

B. **Governing principles.**

(1) **Preamble.** A statement of philosophy or general purpose statement may be used to introduce the policy, to outline its intent, and to establish the university’s authority to regulate use of its computing facilities. It may also be helpful to recite the “legislative” history of the policy.
Access to modern information technology is essential to the pursuit and achievement of excellence across the MSU mission of instruction, research, and service outreach. The privilege of use of computing systems and software, as well as internal and external data networks, is important to all members of the University community. The preservation of that privilege for the full community requires that each individual faculty member, staff member, and student comply with institutional and external standards for appropriate use.

To assist and ensure such compliance, Computing and Technology, with the advice and counsel of the all-University Computing and Communications Systems Advisory Committee, establishes the following administrative ruling, applicable to all faculty, staff and students.

[Michigan State University]

Notice. The OSU computing and electronic communication facilities and services provided by Oklahoma State University are primarily intended for teaching, educational, research, and administrative purposes. Their use is governed by all applicable University policies, including the sexual harassment, patent and copyright, and student and employee disciplinary policies, as well as by applicable federal, state, and local laws.

[Oklahoma State University]

(2) **Scope.** At the outset the policy should define who is to be covered by the policy. More specifically, the scope of coverage should include all users of the system: students, faculty, staff, and guests. With respect to students this should include persons who are not enrolled for a particular term, but who enroll for courses from time to time.

A "User" is any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both. The term "User" thus includes system Sponsors, System Managers, and Faculty Staff.

[Michigan State University]

(3) **Privacy.** Perhaps the most delicate if not difficult issue is addressing the extent to which electronic communications shall be deemed private. A corresponding issue is the extent to which such communications shall be subject to being monitored for legitimate business purposes. Also, in this connection, a process should be undertaken to inform the various university constituencies...
of their respective rights and responsibilities under applicable laws relating to confidentiality, public
disclosure, and retention of electronic records.

The general right of privacy should be extended to the extent possible to the electronic environment.
TAMU and all electronic users should treat electronically stored information in individual files as
confidential and private. Contents should be examined or disclosed only when authorized by the owner,
approved by an appropriate institution official, or required by law. Privacy is mitigated by the following
circumstances.

1. TAMU is an agency of the State of Texas and therefore subject to the Texas Public Information Act.
For TAMU employees, electronic information created in the performance of their duties may be public
records, just as are paper records. Such records may be subject to review and/or release under the Texas
Public Information Act. In these cases, disclosure of personal e-mail or files not related to the specific
issue discussed in the Public Information request will be avoided to the extent allowed by law.

2. Administrative files of the University are generated as part of the process of managing the University.
Files that employees create or maintain can be reviewed by supervisors within this administrative context.
Generally, faculty research files and files relating to scholarly endeavor will not be subject to such a
review.

3. There is an acknowledged trade-off between the right of privacy of a user and the need of system
administrators to gather necessary information to ensure the continued functioning of these resources.
In the normal course of system administration, system administrators may have to examine activities,
files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems
with system software or hardware. Sometimes system administrators may access files to determine if
security violations have occurred or are occurring. In this case, the user should be notified as soon as
practical. System administrators at all times have an obligation to maintain the privacy of a user’s files,
electronic mail, and activity logs.

4. Computer systems and stored data are subject, by authorized personnel, to review for audit purposes
or when a violation of university policy or law is suspected.

[Texas A&M University]

It is the intent of the University to preserve the privacy of e-mail communications and maintain access
to communications intended for an individual. Given that universities place high values on open
communication of ideas, including those new and controversial, the intention of the University is to
maximize freedom of communication for purposes that further the goals of the University.

All e-mail communications, unless subject to a specific privilege, are subject to production under the
Oklahoma Public Records Act and, when relevant, to discovery in civil litigation.

[Oklahoma State University]
(4) Acceptable/Prohibited Uses. The policy-makers should consider and then address the following activities as they deem necessary and appropriate: (a) commercial activity e.g., solicitation in connection with personally-owned businesses; (b) political expression e.g., endorsement of candidates for political office; (c) electronic harassment e.g., communication which would be deemed violation of institutional sexual harassment policy, but which occurs in an electronic environment; (d) defamatory material; (e) copyright infringement; (f) violation of any criminal law e.g., obscenity or child pornography statutes; (g) extensive personal use, i.e., any use which impedes access to the system resources by other members of the university community or which subjects the institution to a material increase in its operating cost; (h) ability to install personally-owned software on university computers, either related to one’s discipline or unrelated e.g., electronic games; and (i) the use of encryption.

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

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.

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

[The University of Tulsa (revised July 26, 1995)]

The University respects encryption rights on its network and may itself encrypt information and transactions when secure confidentiality is an obligation.

[University of North Carolina at Chapel Hill]

(4) Administration. The policy should identify the administrative unit(s) responsible for the implementation of the policy. This unit should assume the responsibility to develop a
communication plan to inform the entire university community of the policy statement. This plan would include appropriate announcements, splash screens, and disclaimers upon entrance to the computing system.

OSU makes no warranties of any kind, whether expressed or implied, for the service it is providing. OSU will not be responsible for any damages you suffer through the use of OSU computing and electronic communications facilities and services, including, but not limited to, loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or by your error or omissions. Use of any information obtained via the Internet is at your own risk. OSU specifically denies any responsibility for the accuracy or quality of information obtained through its computing and electronic communications facilities and services.

The plan might also include some written acknowledgement and acceptance of the university's policy upon being granted computer privileges. The responsible administrator should refer members of the university community to resources necessary to interpret the policy e.g., the office of university counsel on matters relating to compliance with copyright law. The plan would also inform computer users about training opportunities. Training programs should go beyond the technical hands-on level (e.g., how to log on and password security) to include coverage of ethical issues and even suggestions for proper and effective communication in an electronic environment. Finally, of course, the plan should give adequate attention to the compliance and enforcement mechanisms.
Appendix A - Model University Computer Policy Framework.

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:
      ● commercial solicitation
      ● political expression
      ● libelous material
      ● electronic harassment
      ● extensive personal use
      ● ability to install personally-owned software on university computers
      ● use of encryption; and
   4) access to electronic information (including cost).

C. Process for retention/deletion of e-mail messages and disposal of computer equipment.

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

E. Communication plan.
   1) splash screens;
   2) consolidated materials;
   3) disclaimers; and
   4) acknowledgement of policy/procedure.

F. Training program including password security and ethical issues.

G. Compliance mechanisms.
Appendix B - Hypotheticals.

1. You serve as Dean of the Graduate School at Western State University. A faculty member in the Department of Political Science has created a home page on the World Wide Web which will be accessible to her students and any other interested persons. She has also created an electronic class folder that only her students may access. May she copy an article from the electronic *Washington Post* and display it through the home page and/or the class folder? Should you call the university attorney’s office?

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. Mary is enrolled at Eastern State University and has been assigned a student computer account. Mary sends a request via campus e-mail to the Registrar for an official transcript to be sent to Western College. She also requests that an unofficial transcript be sent to a prospective employer. How do you respond?

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. 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?