Cyberspace on Campus: Computer Policies & Liability

A student uses a university computer to operate a bulletin board service allowing subscribers to copy software. Another student sends a pornographic death threat against a coed over the Internet. And someone pirates a professor's password and uses the university E-mail to send a racial "hate" message across the country. These situations have actually occurred at three separate universities. With the rapid growth of electronic technology on campuses, university administrators are faced with new liability concerns. These concerns were recently addressed at Stetson's annual Law and Higher Education Conference in a session by Paul J. Ward, general counsel for Arizona State University, and Patricia A. Hollander, general counsel for the American Association of University Administrators. The following is an edited version of their presentation.

Electronic Rights and Responsibilities on Campus

Campus officials are under pressure to keep pace with modern information technology. But new technology brings with it new liability exposures. From simple use of copyrighted software to complex issues of free speech stemming from the operation of a university bulletin board service (BBS), questions about liability abound. The legislative process is slow to react to rapid developments in technology. 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 resulting conflicts. A policy statement on the use of computers on campus can be an important means to avoiding some conflicts. The following are some of the issues institutions should consider when developing such a policy statement.

Copyright

Clarify in your policy copyright law as it pertains to software use and digital transmission of published materials. Computer software and digital transmissions of text and photographs are subject to copyright protection under the Copyright Act of 1976. Under the Act, it is legal to make an archival or backup copy of a software program, and some software may be copied for use in teaching, scholarship, or research under "fair use" guidelines. These guidelines take unto account the purpose of the use, the nature of the work, the amount copied, and the effect on the potential market for the work.

As an electronic bulletin board service operator, what liability does a university have for infringing acts of third parties? The law is not clear yet, but in two separate cases bulletin board service operators have been found liable for copyright infringement based on the actions of their subscribers. In one case, a BBS operator was understandably found liable for infringement by directly encouraging subscribers to download (copy from the BBS) unauthorized copies of video games (Sega Enterprises Ltd. v. MAPHIA, 1994). However, in the second case an operator was found liable when subscribers were uploading (copying to the BBS) and allowing others to download copyrighted photographs without the operator's knowledge (Playboy Enterprises, Inc. v. Frena, 1993).

Recommendations for changes to the Copyright Act were recently proposed by a working group on intellectual property of the Federal Government's National Information Infrastructure Task Force. The group has presented a preliminary draft of its report in which it suggests changing the language in the Copyright Act to clarify guidelines for electronic materials. However, no recommendations have been made to regulate "browsing" on-line, eliminating fees for on-line access, or library and classroom use of works in digital form.

Privacy

Include in your policy the institution's guidelines for collecting, storing, and accessing information on students and employees. Lack of privacy in the Computer Age is a real concern for faculty, staff, and students. Universities collect and retain a significant amount of information in electronic format. Concerns about privacy are so strong among the general population that three major studies in the past two decades have recommended the establishment of a permanent governmental agency to deal with privacy issues. However, due to the anti-regulatory mood of the country and strong opposition from the business community, no such agency has been created. At a minimum, all persons with computer accounts must be informed of the institution's practice concerning retention and backup of E-mail messages.

Encryption

The widespread use of E-mail has created another privacy concern. Many people assume E-mail is private communication; some who realize there are no privacy guarantees are opting to "encrypt" (encode) their messages using commercial software programs. The institution's guidelines may recognize certain categories of electronic communication as appropriate for extraordinary protection. This might include proprietary data in connection with sponsored research or the development of research data on human subjects. Nevertheless, the institution must address who will maintain the electronic keys to these computer records.

Legal Access to Electronic Data

E-mail communications and other electronic data are increasingly sought in public record requests and through discovery in litigation. Retrieving and providing archived electronic data can be a major job for an institution in terms of time and money. Courts differ on whether the requester has the right to demand the information be provided in a particular format or medium (e.g. computer tape, computer disk, microfiches, etc.).

In federal litigation matters, it has been well established that E-mail, electronic bulletin board messages, and automatic computer backup files are data compilation documents that can be requested as evidence. Raids have been permitted to conduct on-premise searches to prevent destruction of software (Quotron v. Automatic Data Processing, Inc. 1992). Access to electronic data under state public records statues seems equally likely, even if the law is not well settled.

Freedom of Speech

Freedom of speech issues impact public and private institutions differently. However, all institutions should include in their policies guidelines on political and commercial messages, as well as restrictions on harassing or libelous statements. Computer networks offer an inexpensive and instantaneous avenue for interactive communication, and the Interment offers global access. Networks are being used not only for academic discussions, but also for commerce, political expression, and communication among every imaginable interest group. System operators at colleges and universities are raising concerns about liability resulting from the activities of the network's users, including the posting of alleged defamatory or harassing messages.

In Cubby v. CompuServe (1991) the court dismissed the first libel action suit filed against a commercial computer service for statements made by a subscriber. CompuServe did not dispute the statements in question were defamatory, however it asserted it had a contractual relationship with the subscriber which required prompt posting and no editorial control over the publication. The district court concluded the only consideration was whether it knew or had reason to know of the statements before they were posted.

Another major commercial bulletin board operator, Prodigy, has been taken to court for allegedly allowing third parties to post defamatory messages. This case has not been resolved. Because Prodigy markets itself as a family-oriented network, the court may find it had assumed a greater duty of care.

Are computer bulletin boards the public fora of the 21st Century? Whether or not cyberspace is a public forum is still subject to debate. However, the First Amendment has been applied to the public

university in a variety of contexts, and there is no reason to believe that campus computer bulletin boards will be treated any differently from other campus facilities. Thus, institutions may subject both commercial and non-commercial speech to the reasonable constraints regarding time, manner, and place.

Political Speech

Hypothetical #1

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 (sic). 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 allowed them back only because they loved Jesus and Mohammed."

In light of the first Amendment, what do you advise the postmaster?

Under the First and Fourteenth Amendments to the Constitution, a public institution cannot prohibit speech unless it is obscene or "fighting words" that could incite riots. As offensive as it may be, it is unlikely a court would deem the message obscene or inciting. If the system is considered a public forum, speech cannot be restricted simply because it is offensive. (A private institution may place much tighter restrictions on what users say on its system.) However, public institutions can prohibit employees from using university resources to make personal political statements. The institution could also check to verify that the sender of the offensive message was an authorized user of the system. Unauthorized users of a system are not entitled to free speech protection.

Hypothetical #2

A hacker posts a message containing racial slurs to a Usenet discussion group causing readers to believe 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?

A hacker is either an unauthorized user who gains access to a computer system, or an authorized user who has exceeded his or her level of authorization. In Arizona, hackers can be prosecuted for computer trespassing, which is a Class VI Felony, and other states may have similar laws. Under federal law, hacking is a misdemeanor. In either case, the institution should contact law enforcement authorities and let the authorities decide how to pursue the case.

Password Protection

It is unclear what is reasonably required insofar as institutional protection of users' passwords and related security measures. An institution should at least be able to show it offers training programs for users that include information on how to select passwords that would be difficult for others to bypass or forge.

Commercial Speech

The computer policy should clearly state in what parts of the electronic bulletin board service commercial speech is allowed, and whether or not employees are allowed to use the university system to post commercial messages.

Hypothetical #3

Upon request, a public university issues student Jane a computer account. This account permits Jane to send E-mail messages to other students/faculty 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?

The university cannot prevent unsolicited commercial speech from sources outside of the university community. However, both public and private institutions may regulate commercial speech by faculty, staff, and students using the institution's computer services. A good policy will establish parameters for commercial speech and inform users of the guidelines.

Author: Reason & Risk (Vol. 3, No. 2), the quarterly newsletter of United Educators Insurance Risk Retention Group, Inc. Reprinted with permission, Feb., '97.