“VIRTUAL LEGALITY”

Presenter:

MARJORIE W. HODGES
Policy Advisor
Office of Information Technology
Cornell University
Ithaca, New York

Stetson University College of Law:

WORKSHOP: “VIRTUAL LEGALITY” Campus Electronic Communications Law and Policy
Clearwater Beach, Florida
February 16, 1997
Marjorie W. Hodges  
Cornell University  

Stetson University College of Law  
Law and Higher Education  
Legal Issues and Challenges in 1997  

"Virtual Legality"  
Campus Electronic Communications Law and Policy  

Introduction:  

College and University Computer Use Policies  

Policy Development:  

Cornell's Responsible Use of Electronic Communications Policy  
http://www.cornell.edu/Computer/responsible-use/Index.html  

Stages of development  
Committee membership  
Timeline  
Alliances  

Lessons learned  
Highlights of policy  

Handling Violations:  
Existing University Disciplinary Procedures  

Campus Implementation:  
Educational programs  

World-Wide Scrutiny  

Electronic Communications on Campus. Reprinted with permission.  

Example Policies  

Sample College and University  
Information Technology Policies  

This list includes a sampling of college and university policies relating to information technologies. Most of the policies address responsible or acceptable use of computing issues as well as some of the legal and ethical concerns raised by computer use. This sample is intended to give participants an idea of how different institutions of higher education address these issues. The policies were chosen, not necessarily because they are
model policies, but for the diversity represented. In addition, these policies are all available on the Web.

Currently, CAUSE maintains the most comprehensive list of college and university information technology policies. Many of the listed policies are also available through the CAUSE Information Resource Library, http://cause-www.colorado.edu/information-resources/ir-library.html.

Brigham Young University

Computing/Network Patron Policies and Guidelines
http://acs1.byu.edu/info/policy.html

Contact Information: Academic Computing Services
Last updated: No date given.
Length: 2 pages

This document contains a general policy statement regarding use of personal accounts as well as guidelines on appropriate use of the university computing network that includes a list of necessary behavior and inappropriate behavior. Quote:

"Remember that the Honor Code also applies to your computer and network accounts. Accounts are not to be used for anything that would be inappropriate by BYU standards or wasteful of computer or network resources. Downloading of pornographic or other inappropriate material can result not only in losing your account, but expulsion from the university. Game playing is discouraged and may be prohibited in some labs or during certain hours."

Brown University

Computer Systems Policies
http://www.cs.brown.edu/system/policy/

Contact Information: Vice President for Computing and Information Services
Last updated: February 8, 1996
Length: 10 pages

This policy includes a general introduction; guidelines for appropriate computing behavior that incorporates a list for responsible and ethical behavior; and information on user's rights concerning access to computing resources, data security and integrity, privacy, copyright, errors in software, hardware and consulting. The appendix includes procedures for handling alleged abuses, Brown's contractual agreement with a data communications service provider, extracts from relevant state and federal laws, and guidelines for political activity. Quote:

"Although not legally required to do so, CIS respects the privacy of all users. Members of CIS staff are forbidden to log on to a user account to to access a user's files unless the user gives explicit permission (for example, by setting file access privileges). Exceptions to this privacy policy are made, however, under specific conditions."
Dartmouth College

Dartmouth College Computing Code

http://www.dartmouth.edu/comp/comm/citbook/

Contact Information: help@dartmouth.edu and Nancy L. Hossfeld
Last updated: August 25, 1995
Length: 2 pages

Quote:
“The primary goal and objective of the Computing Code is to assure that every user of Dartmouth College computing has two fundamental rights: privacy and a fair share of resource.”

George Mason University

Responsible Use of Computing Policy


Contact Information: Vice Provost for Information Technology and Services
Last updated: September 25, 1995
Length: 6 pages

This document includes general policy information, rules of use, information on privacy and a description of the stopit process (named after the MIT program). Quote:

“This policy establishes a Security Review Panel that is responsible for reviewing [System Administrator’s] decisions regarding abuses, responding to email, and periodically reviewing this policy.”

Georgia Institute of Technology

Computer and Network Usage Policy

http://www.gatech.edu/itis/policy/usage/

Contact Information: support@oit.gatech.edu
Last updated: August 8, 1994
Length: 12 pages

This document contains a memorandum of transmittal from the acting University president, an announcement of the policy which includes individual guidelines, and the policy. The policy contains information on the background and purpose of the policy, definitions, individual privileges, individual responsibilities, Georgia Tech privileges, Georgia Tech responsibilities, and procedures and sanctions. Quote:

“Just as certain privileges are given to each member of the campus community, each of us is held accountable for our actions as a condition of continued membership in the community. The interplay of privileges and responsibilities within each individual situation and across campus engenders the trust and intellectual freedom that form the heart of our community. This trust and freedom are grounded on each person's
developing the skills necessary to be an active and contributing member of the community. These skills include an awareness and knowledge about information and the technology used to process, store, and transmit it.”

**Lewis & Clark College**

Responsible Use of Information Technology Policy

http://www.lclark.edu/GENERAL WEB POLICY use.html

Contact Information: Bret Ingerman, Director, Academic Technologies, ingerman@lclark.edu.

Last updated: December 1, 1995

Length: 2 pages

This policy differentiates between primary and secondary computer use activities, a list of “impediments” to other’s use, potential consequences for violations and information about where to report violations. Quote:

“"The institution seeks to place its efforts towards the enhancement of technology resources and not the policing of those resources.”

**Marquette University**

General Computing Policy and WiscNet/Internet Policy

http://cause-www.colorado.edu/information-resources/ir-library/text/csd0633.txt

Contact Information: Ann Mallinger, User Services Manager, Computer Services Division

Last updated: December 17, 1991

Length: 3 pages

This policy focuses on authorized use of the university public computer systems and requires an application for uses other than those for research and educational purposes. It includes a list of misuses and consequences for that behavior. It also includes a policy specifically addressing the legal, security, privacy and acceptable use issues for university network and Internet use. Quote:

""The purpose of WiscNet is to advance education, research and public service by assisting in the exchange of information among research and educational institutions by means of high-speed data communication techniques and to assist those institutions in gaining access to scientific and educational resources.”

**Nassau Community College**

College Policies

http://www.sunynassau.edu/policies/POLICIES.HTM

Contact Information: None

Last updated: July 13, 1996

Policy Statement on the Use of the Computing Resources
The EDUCOM Code on Software and Intellectual Rights
Length: 2 paragraphs

Student's Rights and Responsibilities
General Student Code of Conduct
Length: Multiple pages

Acceptable Use Policy for Computer Facilities
Length: 1/2 page

This document includes a general policy statement and examples of unethical and unacceptable behavior. Quote:

"Policies and regulations of the college, and state and federal laws, are applicable to computer resources."

Stanford University

Residential Computing Acceptable Use Policy

http://rescomp.stanford.edu/use.html

Contact Information: dane@rescomp.stanford.edu
Last updated: April 16, 1995
Length: 3 pages

This policy focuses on residential computing at Stanford which includes residential clusters as well as in-room connections. The residential computing policy address acceptable use issue mainly by referring to the standards of conduct for students at Stanford. Quote:

"The Fundamental Standard has set the standard of conduct for students at Stanford since 1896. It states: Students at Stanford are expected to show both within and without the University such respect for order, morality, personal honor and the rights of others as is demanded of good citizens. Failure to do this will be sufficient cause for removal from the University."

University of Colorado

University Electronic Mail Policy

http://www.colorado.edu/HyperHelp/news-info/email.html

Contact Information: Lindsay Winsor, University Management Systems
Winston_l@wizard.Colorado.EDU.
Last updated: March 1, 1996
Length: 4 pages

This policy focuses exclusively on electronic mail. It includes a general statement, information on the Electronic Communications Privacy Act, prohibited uses of e-mail, information about university access and disclosure of e-mail and a general statement that prohibited use will result in disciplinary action. Quote:

"Electronic mail has become an essential tool for faculty, staff, and students of the University. Yet like all powerful tools, it has the ability to damage as well as to assist. In 1993, the Policy Board for Information Technology asked the assistant vice president for computing and information systems to
draft a University e-mail policy to promote constructive, rather than destructive, use of e-mail. A working group including representatives of information technology, internal audit, legal counsel, personnel, and faculty prepared the policy after reviewing comparable documents from around the country.

University of Missouri/Columbia

Code of Conduct for Legal and Ethical Computer Use

http://music.phlab.missouri.edu/policy/

Contact Information: webmaster@www.missouri.edu
Last updated: July 2, 1996
Length: Multiple page unfinished outline

This policy page illustrates the use of information technologies in policy development. The "What's new" link contains updates of the policy progress, instructions on how to join the MU-Acceptable Use Policy electronic discussion group, links to new policy material and links to the text of ACLU v. Reno. In addition, the page links to the draft document of safe computing and draft user service agreement. Quote from the safe computing document:

"Authorized access to data or information entails both privilege and responsibility, not only for a user, but also for the system administrator who can observe the user's data or activities. Some court precedents have found service provider liability for the misbehavior of users, implying a duty to restrict and monitor user files and processes. Other precedents have found service providers liable for violation of privacy or free speech when doing just that! MU's policy tries to resolve this dilemma for MU members by several distinctions. Most University facilities are not "public forums" or "common carriers". Appropriate use is judged first by institutional missions, and secondly by perquisites. A service-provider necessarily owns all data (the input, storage, communication, or display medium)—but not necessarily all levels of information (the meaningful content, the intellectual property) presented by the data. Users must accept specific minimally-invasive restrictions and monitoring as a condition of service."

University of Missouri/Columbia (cont.)

Code of Conduct for Legal and Ethical Computer Use

http://cause-www.colorado.edu/information-resources/ir-library/text/csd0632.txt

Contact Information: Campus Computing Help Desk (314) 882-5000
Last updated: No date given. Apparently around 1990.
Length: 9 pages

This policy divides legal and ethical computer uses into three categories; abuse of federal and state laws, including access, privacy, harassment and tampering; abuse of copyright and plagiarism; and waste and frivolity. It quotes relevant federal and state laws. Quote:

"The following code is rooted in two schools of ethical thought, 'utilitarianism' and 'mixed rule deontology.' Utilitarianism teaches that an action is ethical if an individual acts in the interest of a majority of other people. Mixed rule deontology teaches that an action is ethical if an
individual acts in accord with the rules and considers the consequences of his or her action. Both theories include a strong focus on the interests of 'other people'.
Introduction

Few topics are as complicated and controversial as electronic communications and student conduct on campus. This edition of Synthesis is designed to help you identify and address some of the most pressing issues, especially the scope of freedom of expression on campus computer networks.

A good place to start your reading would be our interviews with two national authorities in the field:

Marjorie W. Hodges, Policy Advisor for the Office of Information Technologies at Cornell University, discusses the design and implementation of campus computer use policies. Her model is the policy at Cornell University (reprinted on p. 552 of this issue), which we think is one of the most comprehensive in the country.

Steven J. McDonald is Associate Legal Counsel at The Ohio State University. Before coming to Ohio State he represented CompuServe in Cubby v. CompuServe, the first on-line libel case. His interview focuses on pressing issues in communications law, including the Communications Decency Act.

In addition to our editorial, and selected excerpts, this edition of Synthesis also contains a detailed case study, with relevant citations. We think you will find it a valuable resource in helping staff members on your campus identify, understand, and discuss some of the fascinating challenges now arising in the world of electronic communications on campus.

From the Editor

College administrators as immigrant parents

Gary Pavella

What do most college administrators and first generation immigrant parents have in common?

One answer is that both live in different cultural worlds from the young people around them. The difference is especially pronounced in terms of knowledge of computers and electronic communications—a field where many adolescents and young adults have demonstrably superior skills than their elders.

With superior skills on the part of the young can come an attitude of superiority, and a sense that the older generation cannot comprehend the new world. Tensions will inevitably arise, particularly when the old try to assert values and traditions the young think are irrelevant. Permanent divisions are likely without the application of wisdom and good will.

The attraction of libertarianism

The cultural differences between students and administrators on college campuses go beyond knowledge about and attitudes toward computers. They also include different perspectives about politics and the role of government.

While many of the young seem socially liberal (on issues like gay rights or abortion, for example) their "liberalism" may be grounded in distrust for authority rather than a commitment to use government to protect the less fortunate. It's not that government is perceived to have no role at all—large numbers of young people support environmental regulation, or funds for education—but that most forms of social engineering are distrusted, especially if coercion is involved. This feeling is likely to intensify as more young people join what may be a new anti-establishment counter-culture, associated with greater use of marijuana and other illegal drugs.

Many young people are also increasingly convinced that they will have to rely on themselves—not the government—to obtain medical care, or provide for retirement. Their views in this regard are reflected in significantly higher savings rates than baby boomers, when baby boomers were at a comparable age. A USA TODAY-Roper poll, reported in the January 15, 1996 issue of USA TODAY (p. 51) found that:

Chief among Generation Xers attributes: a highly developed sense of personal financial responsibility. They don't expect the government or their employers to take care of them. Eight in 10 are counting on personal savings to bankroll their retirement, vs. only half of baby boomers when they were in their 20s ... And 72% of Xers expect to financially support an aging parent ...

With a greater sense of personal responsibility and self-reliance comes libertarian social and political perspectives.
It's not surprising that membership in the Libertarian party has increased by 20 percent since 1994, and that about forty percent of the new members are under 35 (see "A New Kind of Party Animal," New York Times, January 20, 1996, p. 23).

The ethos of the Internet

The cultural differences between old and young are also compounded by the individualistic, "don't tread on me" ethos of the Internet. Cornell University saw an example of that ethos when a group called the "Online Freedom Fighters Anarchist Liberation" (OFFAL) "mailblast[ed] a bogus, satirical e-mail message to more [than] 21,132 students, staff and faculty" to protest Cornell's alleged, covert "punishment" of four students responsible for creating and sending misogynist e-mail (see "OFFAL strikes Cornell," Syntax Weekly Report week of December 4, 1995, p. 427).

A good sense of the social and political attitudes associated with the Internet can also be found in a January 1996 article by David Kline and Daniel Burstein in Wired magazine ("Is Government Obsolete," p. 86). The purpose of the article was to challenge the radical libertarianism expressed by those who would severely limit the role of government in regulating the evolving telecommunications industry. Still, even with that goal—and while asserting that "the law of supply and demand has never by itself prevented businesses from skunking the consumer"—the article is full of observations like:

- "Compared with business, which must constantly adapt and innovate in order to compete successfully, government seems to grow more bloated and ineffective as its leaders claim they are making it leaner and meaner."
- "Governments may pontificate about desirable social goals, but business has a much better track record in turning ... innovative technology ... into a material force that transforms millions of lives for the better."
- "Sure enough, Adam Smith's invisible hand theory has generally proven to be remarkably valid . . . ."

If this is the "liberal" perspective on-line, one can only imagine the scope and depth of "conservative" views expressed there.

American culture—and campus culture

The Internet, of course, is a product of the culture in which it was created. And, from the beginning, American culture has exhibited what Seymour Martin Lipsett calls "American Exceptionalism": a strong commitment to anti-statism individualism, mixed with populism (American Exceptionalism, New York: 1996). At the end of his book, Lipsett reprinted a worldwide survey of 15,000 managers—and concluded that Americans continue to show an "astonishing" preference for personal initiative and competition, compared to managers in Europe and Japan.

On the issue of anti-statism and individualism, however, one part of American society marches to a different drummer. Especially in recent years, higher education has tended to stress group obligations rather than individual rights. This emphasis is highlighted by the fight to maintain race-based affirmative action programs on campus, and in the affinity for neo-Marxist approaches in teaching and scholarship (see, generally, Pavela "Deconstructing Academic Freedom," 22 Journal of College and University Law 359 (1995).

A conflict of values

The appeal of the left at colleges and universities may reflect a more egalitarian youth culture in the 1960s, now entrenched in the professorate, and in many student affairs offices (see our editorial "Generations" in the Winter 1991 issue of Synthesis, p. 221). If so, there are serious implications for freedom of expression on campus. Duke University law professor William Van Alstyne, writing in Freedom and Tenure in the Academy (Durham, 1993) observed that college teachers who were campus activists in the 1980s were "influenced strongly by Herbert Marcuse's writings (for example, Repressive Tolerance . . . )." Van Alstyne concludes that "[m]any SDS members believed that prevailing First Amendment doctrine was itself vicious because it enabled entrenched elites to exploit others by perpetuating a myth of an open marketplace of ideas, which elites dominated for their own ends" (pp. 121-22).

There's a clear risk of confrontation when campus "establishment" views—generally on the left—come into conflict
with the more libertarian values of many contemporary young adults, the ethos of the Internet, and the culture of the larger country. It would be a particularly serious blunder for college administrators to rely on authoritarian approaches to combat "offensive" ideas and expression on campus computer networks, since doing so would also rekindle all the controversy and ridicule associated with the national reaction to college and university "speech codes."

The more colleges rely on authoritarian approaches, the more individualistic students are likely to become.

In addition to generating a level of opposition that would almost certainly force a retreat, a "speech code" approach to regulating student expression on-line would undermine efforts on many campuses to promote greater appreciation for community life. Indeed, the more colleges rely on authoritarian approaches, the more individualistic students are likely to become. An insight in this regard was expressed by the poet Joseph Brodsky, reflecting on his boyhood in Russia. It was precisely because the Soviet government tried so hard to regulate thought, Brodsky wrote, that he and his friends became:

real Westerners, perhaps the only ones. With our instinct for individualism fostered at every instance by our collectivist society, and our hatred toward any form of affiliation, be it with a party, a block association, or, at that time, a family, we were more American than the Americans themselves. And if America stands for the outer limit of the West, for where the West ends, we were, I must say, a couple of thousand miles off the West Coast. In the middle of the Pacific. ("A Boyhood in Western Russia," Harpers Magazine March, 1996, p. 30).

Alternatives to authoritarianism

Some regulation of electronic communication will be necessary. Students need to know they can be sanctioned for sending counterfeit messages, threats, stalking, sexual harassment (as defined by the courts), child pornography, and other forms of communication not protected by the First Amendment. But it will be best if voluntary compliance were secured whenever possible, and if general "standards of civility" were promoted by students—much in the way student honor councils at some colleges educate their peers about the importance of academic integrity.

Not long ago at Harvard University a first-year student violated cultural norms by mass e-mailing an announcement for an a cappella concert. The resulting articles and letters of indignation to the Harvard Crimson appeared to make the offender a campus pariah. Eventually, feeling some sympathy for "[t]he helpless first-year," Crimson editorialized that "[w]e sincerely hope that he will not be punished for his transgression, and we would like to see ... computer services transfer its energies from reprimanding [the student] to taking steps to deter such actions in the future" ("The Internet is Fragile," March 15, 1996, p. 2).

The Harvard example is a precursor to an electronic communications honor code. It suggests students can use persuasion and peer pressure to set reasonable standards for civility without a heavy reliance upon administrative sanctions. What is needed is creative action by administrators to institutionalize such a role, perhaps by giving student leaders an important voice in developing and approving campus-wide computer use policies.

Giving students authority to help shape the future of electronic communications makes sense—not simply as a way to minimize conflicts, but in recognition of the special knowledge and insights students have about the electronic world. To return to our analogy of immigrant parents, keeping a campus "family" together in a new world requires unique abilities: to assert and to listen; to affirm and to let go; to lead and to follow. How we perform this task may define our relationship with students for several decades to come.

Excerpt

Thinking About the Electronic Future

The use of computers and electronic communication may promote harmful ways of thinking. Our evolving use of e-mail and on-line publications seems to be associated with speed and superficiality. The sheer volume of electronic communication causes us to read quickly, one finger resting on the "delete" button. Particularly as video imagery becomes widely available on-line, "scanning" and "experiencing" may become more important than reading and thinking. The quiet moments of contemplation holding a book or magazine—without the hum or glare of a computer screen—may turn out to be more precious than we realize. Likewise, we may regret the loss of the capacity to focus, and to turn away from electronic stimuli in order to organize and discipline our thoughts.

There's a lesson to be learned from what some educators will see as an unlikely source: the highly successful Amish communities. The Amish, as described in the current issue of Technology Review (Eric Brende: "Technology Amish Style," February/March 1996, p. 25) follow a simple, intelligent approach to new technology. Unlike mainstream society, which "never test[s] the social impact of [its] products, but unscientifically presume[s] a beneficial effect, the Amish often adopt new technologies only after a trial period in which they assess the effects" (p. 28). Higher education administrators need to do the same. Technology should not determine how our mission is defined; our mission should determine how technology is used.

The nature of work may be changing faster than anticipated. James Fallows, writing in the current issue of the New York Review of Books ("Caught in the Web," February 15, 1996, p. 14) cited Bill Gates's goal of creating a "total communications" system that would promote "friction free" capitalism (i.e., direct links between consumers and producers, without intervening distributors or retailers). If Gates's view prevails, the resulting economic transformation will generate a new frenzy of downsizing, with a dangerous, largely unanticipated consequence: computers will eliminate much of the work done by the middle class, while enhancing consumer demand for goods and services. If our students are to survive in this world, they will require more than new technical skills. Educators will need to return to goals set by the Greek founders of the first academy: to teach the values of self-restraint and intellectual commitment in a world that appeals relentlessly and seductively to the transient joys of material gratification.


SYNTHESIS: Law and Policy in Higher Education • Spring, 1996 547
Mr. McDonald is Associate Legal Counsel at The Ohio State University, and also teaches a seminar at The Ohio State University College of Law titled "Electronic Communications and Tort Law." Before coming to Ohio State, he specialized in media law and First Amendment-related litigation—and represented CompuServe in Cubby v. Compuserve, the first on-line libel case.

SYNTHESIS: What do you think are the two or three most important issues the Communications Decency Act (CDA) raises for college administrators?

McDONALD: The first and, at least for now, the primary issue is whether to worry about the CDA at all. As most people probably are aware, the CDA is currently being challenged in a lawsuit in federal court in Philadelphia, and it is widely assumed that it will be held to be unconstitutional. However, while there are compelling First Amendment arguments against the CDA, it's not by any means a slam-dunk case.

In addition, while the government has agreed not to take any affirmative steps to enforce the CDA while the litigation is pending, it has reserved the right to go back and prosecute any violations that take place in the meantime if the CDA ultimately is upheld. Thus, there is a real, though probably fairly small, risk in simply waiting to see what happens. Even if you don't take any immediate action, it would be worth thinking through now how the CDA would apply to your particular system and what contingency plans would be appropriate if it should survive judicial scrutiny. In very general terms, the CDA prohibits you from "knowingly" allowing "indecent" material to exist on your own system in such a way that it is accessible to minors. Also as a general matter, you're not responsible for "indecent" material on other systems, even if minors are able to access them through your system.

You can reduce your liability to some extent by adopting a computer use policy that expressly prohibits system users from violating the CDA and, when you learn of any such violations, enforcing the policy. Doing so should give you fairly good protection against individual, unofficial violations. If you don't "know" about those violations and don't "intend" for your system to be used in violation of the CDA, you shouldn't be liable.

If you have the alt.sex and related Usenet newsgroups on your system, you clearly have what Senator Exon had in mind when he used the term "indecent." Web pages operated by art departments (e.g., copies of the Mapplethorpe photos), English departments (discussions of the Canterbury Tales or Ulysses), medical schools (anatomical images) and the like might well also be considered "indecent." Those two items are probably the biggest sources of concern on most campuses, and if you allow them or similar materials to exist officially on your system, a computer use policy won't help. You presumably do "know" about those materials and do "intend" for them to be there.

Of course, removing those materials once they're there would raise additional First Amendment and academic freedom issues (not to mention being, in many instances, bad educational policy). Unfortunately, however, the only other alternative under the statute—removing the minors—would be equally difficult and unpalatable. You could theoretically deny computer accounts to your underage freshmen and shut down any "schoolnet" and similar programs that physically operate on your system, but doing so would not give you much protection. Passwords can be shared with underage friends more easily than alcohol, and, given the way the Internet currently operates, minors who establish accounts elsewhere would still have essentially free access to your web pages and other substantial portions of your system.

The only other alternative under the statute would be to take "good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors" to whatever "indecent" materials are on your system. Unfortunately, however, the methods Congress approved, such as using credit card restrictions, are geared primarily to commercial providers, and, while the FCC has authority to prescribe additional methods, it appears to be in no hurry to do so. Thus, there do not currently appear to be any viable alternatives short of setting up your entire system—and the entire Internet—on a subscription-only, commercial model.

SYNTHESIS: Let's say a student in a residence hall, using university computer services, sent a private e-mail message to a 17-year-old friend in another state. The recipient's parents saw the e-mail, and referred it to federal law enforcement authorities. If a jury subsequently decided the e-mail was "indecent," might the university have violated the CDA?

Would it make any difference if the parents of the recipient had previously complained to the university about prior "offensive" or "indecent" communications received from the accused student?

McDONALD: In the first instance, no. The language of the statute and the legislative history both make it fairly clear that Congress intended primarily to punish the people who create and disseminate "indecent" material, not those who "merely" provide access to the Internet. There is nothing in the CDA to suggest that we can be held vicariously liable for the acts of our students simply because they are our students and are using our systems. The university in the first part of the hypothetical would be liable only if it knew about the message beforehand, allowed the student to send it, and intended for its system to be used for such purposes.

There is nothing in the CDA to suggest that we can be held vicariously liable for the acts of our students simply because they are our students and are using our systems.

The second situation is a much closer call, for there would be a much stronger argument that the university "knew" about the message. It would probably depend upon the ac-
tions the university took after the first offense. I don't think that we necessarily have to banish every first-time violator from our systems in order to avoid institutional liability for recidivists under the CDA, but we do need to demonstrate good faith efforts to comply. Again, I think that the adoption and enforcement of a computer use policy prohibiting violations of the CDA would be fairly good protection in this situation.

Depending upon the technical set-up, the university might have an additional defense in both situations. If the student composed the messages on his or her own, personal PC and simply transmitted them through the university's system, the university might be able to argue that the student's PC was not under its "control" and that the section 233(e)(1) defense therefore applied. Again, as a general matter, we're not liable if all we do is provide access to the Internet. If, however, the student used his or her PC to telnet into the university's system and composed and transmitted the message from there, the section 233(e)(1) defense wouldn't work, because the relevant system would be under the university's control. That may seem to be a fairly elusive and meaningless distinction, but it's only one of many in the statute.

SYNTHESIS: Should universities try to monitor student e-mail sent through institutional computer services for possible indecent communications? Should we try to monitor Internet discussion group or WWW postings sent through our systems? What are the implications of the Electronic Communications Privacy Act (ECPA)?

McDONALD: Absolutely not, and for several reasons. First, as a practical matter, it's simply not possible to do so. On most campuses today, the volume of traffic is staggeringly large, and more and more of it is encrypted.

Second, you wouldn't be able to determine with any precision whether a particular transmission would be considered to be "indecent" by a jury applying "contemporary community standards" in the relevant jurisdictions. In fact, you wouldn't even be able to determine what all of the relevant jurisdictions are. Under current obscenity law standards, which are likely to be applied if there ever is a prosecution under the CDA, jurisdiction is appropriate in any location from which, to which or "through" which obscene material is sent. Given the way the Internet works, jurisdiction could therefore conceivably be appropriate in dozens or even hundreds of locations for any particular transmission, and you would have no way of identifying them in advance.

Third, unless you have a computer use policy that very clearly allows you to monitor everything that flows through your system, doing so certainly would create issues under the ECPA (and, for public institutions, the Fourth Amendment). Under the ECPA, monitoring is permitted only in fairly narrow circumstances. While the ECPA is, as one court noted, "famous (if not infamous) for its lack of clarity" about just what those circumstances are, one thing that is clear is that violating it can be fairly costly in terms of damages. Moreover, the CDA expressly provides that it does not limit or override the ECPA in any way.

Finally, even attempting to monitor might subject you to the argument that you "knew" about every "indecent" material on your system and thereby increase your potential liability. The drafters of the CDA certainly wanted to encour-

SYNTHESIS: Please consider another example. University officials "know" a student AIDS awareness group is using university computer services to host a Web site, and to send Internet discussion group postings (all apparently available to individuals under eighteen years of age), that some might regard as being indecent. Might it be reasonable for the university to assert it has not violated the CDA, since it has not "intended" to send indecent material to minors?

McDONALD: Precisely what the "intended" requirement of the statute means is unclear. It does appear to be a valid argument, but if I were the university, I wouldn't want it to be my only defense. If you "know" about "indecent" material on your system and don't do anything about it, it's not much of a stretch to say that your acquiescence demonstrates sufficient "intent" for you to be held liable.

To me, this hypothetical highlights the real problem with the blunderbuss approach of the CDA. In the words of an earlier Supreme Court case that I hope will be central to the outcome of the pending litigation, it's like "burning the house to roast the pig."

SYNTHESIS: Aren't institutions legally responsible for student Internet communications (e.g. defamation, copyright violations) when students use our computer facilities—and when the Internet address (e.g. umd.edu) leads back to us?

McDONALD: No, and that's actually one of the few good aspects of the CDA. Even before the CDA, I don't think we would have been held vicariously liable for the acts of our students in that situation. Under what now appears to be reasonably well-established law, we would be responsible for the defamations of our students only if we knew or should have known about them and failed to take appropriate action. Just like a bookstore, library or telephone company, we are not liable simply for providing the means by which defamatory material happens to be distributed, and we have no obligation to prescreen the materials that flow through our systems to ensure that they are not defamatory.

Sections 230(g)(1) and 230(d)(3) of the CDA, however, appear to take that principle one better. As with much of the CDA, the intent of those provisions is not entirely clear, but they appear at a minimum to adopt the "knew or should have known" standard and, arguably, exempt us from liability for student defamations regardless of our prior knowledge.

The law with respect to copyright infringement is somewhat less settled, but it, too, appears to follow the "knew or should have known" standard in this context. Thus, as a general matter, we should be liable for student copyright infringements on our systems only if we receive a valid complaint and don't do anything about it.
SYNTHESIS: What advice would you give to an institution that receives a complaint of Internet copyright infringement, or defamation?

McDONALD: This can be the single most difficult situation you can find yourself in, and I don't have a foolproof answer. In some cases, it will be fairly simple to determine what to do. For example, if an online service notifies you that one of your students is downloading copyrighted materials from the service, sending them to a listserver, and posting them to a web page, and if, when you look at the web page, the materials are designated as coming from major commercial news outlets, are posted in their entirety without any critical or commentary, and are formatted in the service's distinctive style, you're pretty much at the "know, or should have known" stage. Unless the student can show you a copyright license covering the use, you should remove the materials from your system as promptly as you can, or you may well be held to be a contributory infringer.

In other cases, however, it won't be immediately apparent whether allegedly infringing materials are copyrighted in the first place, whether and to what extent there are any licenses or permissions, or whether the particular use is "fair." If the material is alleged to be libelous, it will rarely be clear from its face whether it is, in fact, false or, if so, whether one of the many legal privileges applies. Making those determinations can take a fair amount of factual investigation and legal research.

The most important thing to do in these "gray area" situations is to not simply ignore the problem. If you don't want to be held liable as a contributory infringer or defamer, you do need to deal with it. On the other hand, you can't and shouldn't simply remove everything about which you receive a complaint—there are also countervailing First Amendment, academic freedom and due process interests to weigh in the balance. Thus, you do have to sort through the issues as best as you can.

Unfortunately, there is virtually no law yet for guidance on just how to do that. It seems to me, however, that the "right" way to proceed is to place a sort of "burden of proof" on the person making the complaint. Again, as a system owner, you should be liable for a user's infringement or libel only if you "knew or should have known" about it and failed to do anything. An allegation of infringement or libel will, in most instances, be enough to impose a duty on you to investigate, but it is not definitive proof of infringement or libel in and of itself.

To my mind, therefore, it neither establishes "knowledge" nor creates an affirmative duty to remove the material. If you can't tell simply by looking at the material, if the only other thing you've got is a bare allegation, and if the student denies that allegation, the complaining party probably hasn't met its burden of proof. Put another way, even if a court were ultimately to find that the student had infringed copyright or committed a libel, it probably wouldn't find you liable under those circumstances.

I'm not saying that you should always side with the student in every disputed situation. You need to assess whether evidence you've got, preferably with the assistance of your legal counsel, and make your best determination. Things that the complaining party could provide to tip the balance might include a copy of the relevant copyright registration, an affidavit as to the falsity of the alleged libel, or the like. The relative credibility of the parties may also be a consid-

eration. If, on the basis of all of that, it appears more likely than not that the material is an infringement or defamation, you should require the student to remove it or do so yourself.

The bottom line is that you need to act responsibly and promptly, but with due regard for the rights of both parties. One thing that has worked reasonably well for us is the "gray area," situations is to start out essentially as a mediator and to encourage the parties to work the issue out themselves. If they won't or can't, you'll still have to make a decision one way or the other, but you may be able to minimize the burden on yourself. In cases of alleged libel, you might also offer the complaining party an opportunity to respond in the same forum. That may resolve the situation altogether and, if nothing else, should reduce the risk of damages.

One thing that has worked reasonably well for us in the "gray area." Situations is to start out essentially as a mediator and to encourage the parties to work the issue out themselves.

Another thing that can be tremendously helpful in sorting out the truth in copyright cases is to explain to the student the basics of the law, including the limitations of the fair use doctrine, the concept of statutory damages (up to $100,000 per infringement), and the personal and monetary costs of defending a lawsuit.

SYNTHESIS: Would it be legally prudent for public colleges to use something like the indecency standard to punish "offensive" or "insensitive" communications between adult students, either in private e-mail, or on campus electronic bulletin boards?

McDONALD: Just the opposite. The entire constitutional argument for the CDA is that it is necessary for the protection of minors. While sexual harassment and similar policies can certainly be applied to online communications between adults, going beyond that to a general prohibition of "offensive" or "insensitive" communications would clearly be a major First Amendment problem, for the same reasons that "hate speech" codes are.

SYNTHESIS: Might public institutions of higher education define use of institutional computer services (including campus electronic bulletin boards and discussion groups) as a privilege, not a right? Under what circumstances might we have created a "public forum," where First Amendment standards apply?

McDONALD: Legally, I think we certainly have the right to determine whether to have a computer system in the first place and, if we do, whether it will be a "public forum." A "limited purpose public forum" or not a public forum at all, under the same standards that apply in other contexts. As a practical matter, however, I can't imagine that a college or university wouldn't want to provide at least basic Internet access to all of its students. It has become an educational, if not a legal, "necessity."

As bandwidth and storage capacity become cheaper, most campuses seem to be drifting, if not consciously moving, toward a public forum model with respect to some or all of their computer services. The Usenet is pretty much already
there—in fact, it may now be the epitome of the public forum—and web pages don't seem to be far behind.

SYNTHESIS: Might it be a reasonable "time, place and manner restriction" to insure that only "appropriate" student postings are linked to official university web sites (e.g., information from the office of admissions)? Likewise, can a student who insists on discussing abortion in a physics department research discussion group be barred from further (electronic) group discussions?

McDONALD: We certainly do have the right to establish "reasonable time, place and manner restrictions" on the use of our systems. For example, we could theoretically prohibit uses that are not university-related (e.g., running a private business) or that unduly burden or interfere with the system (e.g., "spamming"). Any such restrictions, however, would have to be "content-neutral" and not subject to arbitrary interpretation or discretionary application. A prohibition against "inappropriate" use of the system would therefore be problematic, because what is "appropriate" is largely in the eye of the beholder, but a more specific prohibition against posting copyrighted materials without authorization or making repeated off-topic comments in a discussion group dedicated to a particular subject or course, for example, should be okay.

Enforcement of any such restrictions, of course, would be another matter. Internet users have become remarkably adept at evading any efforts at control, and, given its design, the Internet itself seems almost to be a "co-conspirator."

SYNTHESIS: What kinds of behavior does it make sense for a computer use policy to prohibit? What due process should be accorded, as a matter of law, or policy, before a user's account is terminated?

McDONALD: That's an issue we're currently working through ourselves, and there aren't any definite answers. You'll certainly want to prohibit illegal uses of your system, such as unauthorized posting of copyrighted materials, transmission of obscenity (and, if the CDA survives, "indecency"), and e-mail "stalking." You won't be able to catalog every conceivable illegal use, so you probably also want to include a catch-all prohibition against "any other illegal use." You also should consider whether to draw some sort of a line between university-related and personal uses of your system. Beyond that, content-based restrictions can be difficult to define and may raise additional legal issues.

You should also consider establishing some sort of content-neutral resource allocation or "traffic" rules, so that individual users don't do things that overwhelm the entire system or interfere with others' uses. Along the same lines, you should think through whether students will be allowed to have personal web pages, which can be a significant commitment of resources.

Security and privacy are also important considerations: who has access to what and on what terms? You might also think about incorporating "netiquette"-type rules into your policy, but they are also difficult to define and many of them certainly would raise First Amendment issues.

On the enforcement side, it's extremely important to think through what sort of monitoring and investigating rights you want to reserve for yourself and to state them clearly in your policy. If you don't, your view and your users' views of what is a "reasonable expectation of privacy" are likely to differ, and you may run into problems under the ECPA, the Fourth Amendment and invasion of privacy tort law when, inevitably, you do have to investigate an incident.

I'm not sure that there is anything unique about computer use from a due process perspective. While we have been sorting through these issues, we have, essentially by default, handled any serious computer misuse issues that have arisen through our normal judicial affairs process. Our computer services people have assisted in the investigatory phase, but not in the adjudicatory and disciplinary phase, and that division of responsibilities seems to have worked quite well.

SYNTHESIS: There are many ways to access the Internet, and more coming. Might it be prudent for colleges to help students find those access providers, rather than be providers ourselves?

McDONALD: Perhaps, but, if so, for resource reasons rather than legal ones. The legal risks associated with being an Internet access provider really aren't all that overwhelming, are manageable, and, to my mind, are certainly outweighed by the educational benefits.

SYNTHESIS: Are there any relevant issues fast coming upon us that you think we need to be thinking about now?

McDONALD: Apart from whatever comes out of the litigation over the CDA, the biggest issue right now is copyright infringement. It is becoming increasingly easy and inexpensive to digitize virtually any form of information, including text, images, video and audio, to make multiple copies, and to transmit them through computers. In fact, the very act of transmission itself creates even more copies. For example, every time you look at a web page, you generally create two copies—one in your computer's RAM and another, more permanent one in the web cache on your hard drive. When you post a message to Usenet, you create a copy on every Usenet server around the world—or roughly 200,000 copies.

If you apply existing copyright law literally in this context, the entire Internet is really just one giant photocopying machine, and just about everything you do or see on it is technically a copyright infringement. Unfortunately, however, many people seem to forget about copyright law altogether when they sit down in front of a computer. People who intuitively understand that they cannot simply make a photocopy of a copyrighted work and sell it often have no qualms about scanning the work into a computer and sending thousands of copies out over the Internet.

If we don't do a better job of educating our system users about their copyright responsibilities, it won't be long before we see significant changes in copyright law.

If we don't do a better job of educating our system users about their copyright responsibilities, it won't be long before we see significant changes in copyright law—including, very likely, potential new liabilities for system operators and drastic restrictions on the scope of fair use. Several such bills have already been introduced in Congress.
"Responsible Use of Electronic Communications"

Abridged and reprinted by permission of Cornell University. For further information, contact Marjorie W. Hodges at mwh2@cornell.edu

Overview
Introduction to this policy

Computers and network systems offer powerful tools for communication among members of the Cornell community and of communities outside of the university. When used appropriately, these tools can enhance dialog and communications. Unlawful or inappropriate use of these tools, however, can infringe on the rights of others. The university expects all members of its community to use electronic communications in a responsible manner.

The university recognizes the complexity of deciding what constitutes appropriate use of electronic communications services. What is appropriate or offensive to some members of the community may be inappropriate or offensive to others. CAUTION: Having open access to network-based services implies some risk. In a community of diverse cultures, values, and sensitivities, the university cannot protect individuals against the existence or receipt of material that may be offensive to them.

The university cherishes the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The university does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis (i.e., if required to ensure the integrity, security, or effective operation of university systems).

Nevertheless, the university reserves the right to place limited restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of university policies or codes, or state or federal laws. Once evidence is established, the university authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific restrictions, which could include the removal of material posted on a computer and/or limiting access to the university's networks.

This policy is in accordance with university policies concerning harassment, use of computers and network systems generally, and related judicial codes. Any restrictive actions taken by the university will be in accordance with the guidelines and procedures set forth in these policies, codes, or laws. The restrictive actions pertaining to this policy and described below (see the "Policy Specifics" segment of this document) conform to the Electronic Communication Privacy Act of 1986.

CAUTION: In exceptional cases, a system or network administrator may detect evidence of a violation while performing his or her duties operating or maintaining a system. In such instances, the system or network administrator should contact the college/unit policy officer, the Judicial Administrator, or the Office of Information Technologies for further guidance.

CAUTION: This policy does not abrogate local policies governing the operation and maintenance of university systems provided they do not conflict with the precepts of university policy. Colleges and administrative units may wish to develop ancillary procedures that support organizational requirements. Specifically, procedural guidelines with regard to security, privacy, and other areas of critical importance to the administration of these systems are not addressed as part of this policy, nor are violations of principles of network etiquette.

Procedures
Policy Specifics

1. The university reserves the right to limit access to its networks when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor or generally restrict the content of material transported across those networks.

2. The university reserves the right to remove or limit access to material posted on university-owned computers when applicable university policies or codes, contractual obligations, or state or federal laws are violated, but does not monitor the content of material posted on university-owned computers.

3. The university does not monitor or generally restrict material residing on university computers housed within a private domain or on non-university computers, whether or not such computers are attached to campus networks.

Policy Violations

Violations of this policy may involve the use of electronic communications to:

- harass, threaten, or otherwise cause harm to a specific individual(s), whether by direct or indirect reference;

- impede, interfere with, impair, or otherwise cause harm to the activities of others;

- download or post to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements, or otherwise is damaging to the institution;

- harass or threaten classes of individuals (see next Caution).

CAUTION: As a matter of policy, the university protects expression by members of its community and does not wish to become an arbiter of what may be regarded as "offensive" by some members of the community. However, in exceptional cases, the university may decide that such material directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted.

Reporting Violations

1. If you believe that a violation of this policy has occurred, contact the system or network administrator responsible for the system or network involved, who will report the incident to the college/unit policy officer in accordance with local procedural guidelines, should they exist.

2. There may be situations when the following additional offices should be contacted:

- University Health Services and/or the Cornell Police, if an individual's health or safety appears to be in jeopardy;

- University Human Resource Services, if violations occur in the course of employment;
Office of Information Technologies, if an incident potentially bears external or legal consequences for the institution. This office is available to assist with investigations, generally under the auspices of the college/unit policy officer. You may also contact this office if you wish to report an incident but are unable to do so through normal channels.

Procedures for Systems or Network Administrators

If you receive a complaint and are presented with evidence that a violation of this policy has occurred, proceed as follows:

1. Refer to Table 2 to determine what type of violation may apply:
   - violations targeted at a specific individual(s) (4 types identified);
   - violations causing harm to the activities of others (8 types identified);
   - violations involving illegal, proprietary or damaging material (4 types identified);
   - violations targeted at classes of individuals (1 type identified).

2. If you are unable to match your incident with a description in Table 2, or if multiple descriptions seem to apply, contact your college/unit policy officer or the Office of Information Technologies for guidance.

3. Follow the guidelines in Table 2. In addition to the type of violation, the guidelines are framed by other factors, specifically:
   - who reported the violation;
   - whether you administer the university system involved or some other affected system;
   - how participants or affected parties are affiliated with Cornell.

[From Policy Appendix: general information about violations]

[The information from Table 2, which follows] presents general information about the kinds of violations covered by this policy; the party or parties normally serving as complainant(s); the university authorities to whom complainants normally refer incidents; and the appropriate actions and/or restrictions that systems and network administrators may take upon receiving a complaint and being presented with evidence of a violation. Instructions regarding how to proceed are intended for the system or network administrator responsible for the university resource from which the incident is perpetrated or on which the offending material resides, unless specified otherwise.

A. Violations targeted at a specific individual(s)

**VIOLATION:**

A1. Sending an individual repeated and unwanted (harassing) communication by electronic mail or other electronic communication; OR

A2. Sending an individual repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is sexual in nature; OR

A3. Sending an individual repeated and unwanted (harassing) communication by electronic mail or other electronic communications that is motivated by race, ethnicity, religion, gender, or sexual orientation.

4. In all cases, these guidelines tell you:
   - which university authority should receive a formal complaint;
   - the party or parties who normally file such a complaint;
   - what actions, if any, you should or may take.

5. Report the violation in accordance with these guidelines and those established by your college/unit.

6. Document the incident and any actions you take, recording at a minimum the information depicted in Exhibit 1 (see the "Appendix" Section of this document). Protect this information as you would any confidential material: update and retain it as appropriate. This information may be subject to review by appropriate university authorities, so it is important that the information be current, complete and correct, maintained in an electronic database, and easily retrievable.

In exceptional cases, the priorities of protecting the university against seriously damaging consequences and/or safeguarding the integrity of computers, networks, and data either at the university or elsewhere, may make it imperative that you take temporary restrictive action on an immediate basis. In such instances, you may take temporary restrictive action, preferably with the prior approval of the college/unit policy officer, pending final adjudication by the university. All restrictive actions taken must be documented and justified in accordance with this policy. If there is no designated policy officer, or if the policy officer is not immediately available, you may contact the Office of Information Technologies for guidance or assistance.

CAUTION: In some instances, documentation prescribed above will constitute education records . . . and therefore will be protected under the Family Educational Rights and Privacy Act of 1974 . . .

**Who files complaint:** Targeted individual, whether or not a member of the university community.

**Who receives complaint:** Office of the Judicial Administrator.

**Note:** Cornell's Judicial Administrator can act upon a complaint only if the sender of the material is a member of the Cornell community. If the sender is not a member of the Cornell community, the Judicial Administrator will assist the targeted individual by referring him/her to appropriate sources of help outside the university.

**Appropriate action if violation is reported by targeted individual:** Provide the targeted individual with the following information:

1. "Harassment is a violation of Cornell's policies and codes, and in some cases, state or federal laws. Write the sender directly and state that you find the continued correspondence to be harassing and formally ask the sender to cease all communications with you. Save a copy of this message and any other correspondence for evidence."

2. "If you continue to receive correspondence after formally requesting that the correspondence stop, notify Cornell's Office of the Judicial Administrator. Consultations with the Judicial Administrator are confidential."

3. "If you are concerned about your personal safety, contact the Cornell Police or your local law enforcement agency."

**Appropriate action if violation is reported by another individual(s):** Thank the party for forwarding the information and add the following: . . . [continued on page 551]
Developing a Computer Use Policy

Interview by Gary Pavela

Ms. Hodges is Policy Advisor, Office of Information Technologies, Cornell University. She formerly served as Cornell's Judicial Administrator, and is a frequent presenter on legal issues concerning campus computer networks.

SYNTHESIS: Many campuses developed computer use and abuse policies about a decade ago. Are those policies outdated?

HODGES: Yes, many of these policies are outdated because the kinds of behaviors that computer abuse policies need to address have changed dramatically. Ten years ago, institutions of higher education worried about computer hackers and crimes of unauthorized access, including computer viruses and worms. Computer users, back then, were generally people who understood computer programming and used computers for things other than a communications device.

Today, with the evolution of the computer industry and the Internet, almost everyone in higher education uses computers for daily communications. As a result, institutions are seeing an increase in complaints involving general network etiquette, chain letters, forged e-mail, harassment, hate speech and pornography. In short, the kinds of behavior common in other arenas on campus are appearing in electronic communications. Colleges and universities need to update computer use policies to address these kinds of behavior.

SYNTHESIS: What do you think should be the basic components of a computer use policy?

HODGES: A computer abuse policy can take many forms, but there are several universal components. A good policy should contain both a statement about what the policy covers and a statement explaining the reason for the policy. These will give the reader an understanding of the university's position on appropriate use of information technologies. In addition to these general statements, the policy needs to identify the individuals covered by the policy, provide specific examples of inappropriate behavior, give instructions about how to report a violation, and information about potential consequences for violations. Ideally, a computer abuse policy will work with existing university disciplinary procedures and will refer the reader to those related policies as well.

SYNTHESIS: What components of a good policy are frequently overlooked?

HODGES: Many policies fail to provide either specific information about the procedures following a violation or potential consequences for such misconduct. These components are important because they help the institution respond consistently to people with complaints about computer misuse.

SYNTHESIS: What components are we tempted to add, but shouldn't?

HODGES: It's tempting to create a monitoring component, but I would advise against that option.

SYNTHESIS: Who should set computer use policies? What role should students have in determining them?

HODGES: A computer abuse policy needs to reflect the institutional culture. Therefore, it is very important for community members to be a part of its creation. At Cornell, students were not part of the committee that drafted the policy, but they were included in the review process before implementation. As a result of conversations during the review process, we did make revisions to the draft. The groups that reviewed the policy prior to ratification included: the Dean's Counsel; the Faculty Committee of Representatives; and the University Assemblies, representing the students, faculty and staff. After such wide campus involvement, the ratification process was smooth, paving the way for implementation and education.

It's tempting to create a monitoring component, but I would advise against that option.

SYNTHESIS: The honor code model comes to mind. Are there ways we can give students a larger voice in defining the "institutional culture" regarding computer use? If we give student leaders a greater role in educating their peers, and policy enforcement, do you think we would regret the results?

HODGES: The honor code is the perfect model to apply to computer abuse policies. Both rely on an understanding and acceptance of basic behavioral expectations. In fact, existing honor codes should already encompass computer use issues. Moreover, the computer culture already embraces its own form of an honor code, and experienced users not only have an understanding of netiquette, but attempt to enforce those expectations on-line.

I also don't think we would regret giving students a larger role in defining the "institutional culture" regarding computer use.

I also don't think we would regret giving students a larger role in defining the "institutional culture" regarding computer use. Students can play a very active role in educating the campus on these issues both by adapting existing programs to include an electronic communications component and through the creation of new programs.

SYNTHESIS: Should computer use policies vary from campus to campus?

HODGES: Definitely. Colleges and universities need to rely on their fundamental principles and mission when developing any policy. A computer use policy is no exception and should conform to existing institutional understanding of issues such as freedom of expression and academic freedom. For example, private and public institutions may have different approaches to these issues and the computer use policies ought to reflect those differences.

SYNTHESIS: Most of us don't have telephone or fax use policies, why do we need computer use policies?
The "indecency standard" and the "dominant culture."

It would be a violation of the First Amendment for public colleges to use something akin to a CDA "indecency standard" to censor lawful communication among adults in a public forum (i.e., communication that was not obscene, threatening, or harassing). Private colleges have more latitude, but we urge administrators at both public and private institutions to consider the views of Justices Brennan and Marshall, expressed in Justice Brennan's dissent in the 1978 Pacifica case [FCC v. Pacifica Foundation], 75 L. Ed. 2d 1073, 1110-1111:

The words that the Court and the [FCC] find so unpalatable may be the stuff of every day conversations in some, if not many, of the innumerable subcultures that compose the Nation...As one researcher concluded, "[w]ords generally considered obscene like 'bullshit' and 'fuck' are considered neither obscene nor derogatory in the [black] vernacular..." [citation omitted].

Today's decision will thus have its greatest impact on broadcasters desiring to reach, and listening audiences composed of, persons who do not share the Court's view as to which words or expressions are acceptable, and who, for a variety of reasons, including a conscious desire to flout majoritarian conventions, express themselves using words that may be regarded as offensive by those from different socio-economic backgrounds. In this context, the Court's decision may be seen for what, in the broader perspective, it really is: another of the dominant culture's inevitable efforts to force those groups who do not share its mores to conform to its way of thinking, acting, and speaking...


Mass democracy on the Internet

A February 14, 1996 front page Washington Post story reported that a University of Maryland student had sent a public Internet message to at least 11 Internet discussion groups accusing a local woman of child abuse. The Maryland student—who never tried to verify the hearsay information he relied upon—urged readers to call the woman at home "and tell her you are disgusted and that you demand she stops." A "half-dozen" subsequent calls were reportedly received by the alleged "abuser" ("Internet Message Alleges Mother Mistreated Girl," February 14, 1996).

Two days later the Post editorialized in support of freedom of expression in cyberspace:

The episode of Internet-borne harassment this week at the University of Maryland...is a reminder that new technology has not changed human nature...Recent legislation notwithstanding, in our view only speech that is defined as criminally or civilly liable...is the outside world—stalking for instance—should be punished in the same way [in the on-line] world. The rest of Internet speech, like real speech, may be best understood as cultural behavior that needs to be unlearned—and likely will be—as the on-line society takes shape ("Ethics On-line..."). February 17, 1996 p. A24).

SYNTHESIS: Are you satisfied Cornell's policy does not inhibit lawful expression?

HODGES: Yes. The policy does not create any new definitions of "wrong behavior" or "wrong expression." In order to violate our "Responsible Use of Electronic Communications Policy," there must be a violation of institutional policies, state or federal law. Our Campus Code of Conduct includes an entire section on responsible speech and expression which strongly supports lawful expression. Moreover, the computer policy states that "The University cherishes the diversity of values and perspectives endemic in an academic institution and, accordingly, is respectful of freedom of expression." We also make sure our educational programs highlight these points.

SYNTHESIS: Cornell was in the news last year when four first-year students sent some highly offensive e-mail. Please tell us some of the details, and explain why formal penalties were not imposed.

HODGES: This case received a tremendous amount of publicity. Four Cornell students compiled an e-mail message entitled "75 reasons why women (bitches) should not have freedom of speech." In a public letter of determination which was authorized by the accused students, Barbara Krause, Cornell's Judicial Administrator explained that the four students distributed the list to a narrow group of friends whom they did not believe would find the content offensive. Apparently, one or more of the original recipients forwarded a copy and the distribution spread all over the world. Barbara Krause's determination letter stated "[b]y far the widest distribution of 75 Reasons came from people who were offended by its content. Given the facts of this case, I could not conclude that these students had engaged in sexual harassment. Sexual harassment requires conduct that is directed at an individual or group, or conduct that creates a hostile environment."

Barbara Krause's decision explained that the four students deeply regretted the consequences of their actions and, in an attempt to restore their reputations, decided to write a letter of apology to the community, attend a program on acquaintance rape, gender roles, relationships and communications, volunteer 50 hours of community service and meet with a group of administrators to apologize for their actions. Once in the campus judicial system, the four students acted responsibly and Barbara Krause handled the case perfectly.

SYNTHESIS: It must have taken courage not to respond to the public outcry by rushing to impose some sort of official penalty.

HODGES: I think it took a belief in our policies, including our policies on sexual harassment and freedom of speech. Given the facts of this case and our campus code of conduct, an attempt to find the students in violation would have demonstrated a lack of commitment to those policies and that would have been harmful to our campus judicial system and the university as a whole.

This incident underscored: (1) the importance of having a carefully crafted policy in place prior to an incident such as this one; (2) the importance of following the policy, regardless of the pressures to act otherwise; and (3) the importance of communications regarding such a public incident.

SYNTHESIS: Why should we worry about freedom of expression on computer networks if we own those networks? If we're the publisher, don't we have the final say on what gets published? Also, since our name is on the transmission (e.g. cornell.edu, etc.) aren't we responsible when someone says something offensive or illegal?

HODGES: Institutions of higher education may not want to exert control over the content of material that is on their networks. Institutional liability is likely to come down to the determination of the role the college or university played in a given case. Very little case law exists regarding the legal liability of institutions or organizations that provide Internet access and services, but in the cases that do exist, the courts look to existing law for analogies. In determining liability, courts consider the degree of control exercised by the provider. So it may be that the exercise of greater control increases the risk of liability.

In determining liability, courts consider the degree of control exercised by the provider. So it may be that the exercise of greater control increases the risk of liability.

Take a defamation case for example, publishers may be held liable, but distributors of information are held liable only if they knew or had reason to know of the defamatory material. As a result, institutions developing computer use policies will want to compare Stratton Oakmont, Inc. v. Prodigy Servs. Co. [23 Media L. Rep. 1797] and Cubby, Inc. v. CompuServe Inc. [776 F. Supp. 135]. In Stratton Oakmont, the New York Supreme Court (a trial court) held Prodigy, a commercial on-line service provider, was a publisher of defamatory material posted on one of the company's computer bulletin boards. In determining whether to consider Prodigy a publisher rather than a distributor, the New York Supreme Court considered Prodigy's policies.

The court reviewed public statements by Prodigy that it exercised editorial control over the content of messages posted on computer bulletin boards and that it was a "family-oriented" computer network. The court found it significant that Prodigy provided "content guidelines" and used software to screen postings for offensive language. Following this logic, if a college or university monitored student electronic communications in an effort to catch offensive language, then the institution risks increased liability for the content of every message that originates from the institution's system. Prodigy appealed the decision and Stratton Oakmont settled the case before appeal. Regardless, the decision exists for other courts to follow, if they are so inclined.

The court in Stratton Oakmont distinguished that case from Cubby, Inc. v. CompuServe Inc. (1991), a decision by the U.S. District Court of the Southern District of New York. In Cubby, the court held that...
Baxter goes on-line by Gary Pavela

Baxter is a senior history major, known for an abrasive personality, and his relentless efforts to introduce other students to the philosophy of Friedrich Nietzsche. Baxter transferred to a public university after being expelled from a private college for threatening a professor (see Baxter and His History Professor, Part II, in the November 1989 issue of Synthesis: Law and Policy in Higher Education).

Baxter seemed to find a new direction in life after reading Nietzsche, and discovering the world of computers, electronic mail, and the Internet. His new avocation, however, led him into trouble, based on the following incidents:

- Baxter enrolled in an advanced "conflict resolution" seminar and participated in the assigned e-mail discussion group. Baxter’s opinions were harshly criticized on-line by several classmates, which prompted him to send each of them an e-mail “warning.” The “warning” stated that Baxter had some friends associated with organized crime, and if he were subject to any further abuse his friends would "visit" the offending students.

Two of the students who received this message continued their criticism, and received subsequent messages from Baxter indicating their names had been passed on to his “friends,” who could be expected to arrive later in the week. The messages were repeated, several times a day, even though both students asked Baxter to stop. The students felt threatened, sought immediate police protection, avoided going to their scheduled classes, and filed written complaints with the dean of students.

- Baxter’s polemics spread through the Internet to the world off-campus. He was particularly critical of “traditional,” anarchists, largely due to their “lack of organizational skills.” In an Internet-accessible “Student Voices” Web site posting, using a university computer server, Baxter contended that one anarchist writer, identified by name, was a plagiarist. The writer learned of the posting, called the president of the college, and stated that Baxter’s accusation constituted defamation—for which the college might ultimately be liable. The president promised that a prompt response would be forthcoming from the dean of students.

- Baxter formed a new campus organization: the United Anarchist Collective (UAC). After protracted procedural wrangling, all three members elected Baxter President. The group obtained “registered” status as a student organization, thereby allowing use of university facilities, including computer services necessary to create a UAC “web” page, accessible on the Internet. UAC used its computer account to send automated e-mail messages to hundreds of campus addresses, containing selected quotations from Nietzsche. UAC also posted Nietzsche quotations on a campus-wide “student opinion” electronic bulletin board, and on the UAC “web” page.

Many students and faculty members complained to the dean that the quotations clogged their mailboxes, were frequently anti-Semitic, and offensive. Furthermore, the director of admissions was furious that some prospective students saw the UAC web page, and read what she regarded as "outrageous" pronouncements, critical of the university.

- The dean arranged an urgent meeting with legal counsel to discuss the various complaints against Baxter and the UAC. On his way to the meeting, his secretary asked him to view her computer screen. Displayed there was the most recent addition to the UAC web page: a simulated picture of Nietzsche and Ayn Rand, both in the nude, holding hands while climbing a mountain. Several parents and two different student organizations had called to complain about the web page, and to assert that the nude images constituted public “indecency” and “sexual harassment.”

How should the Dean respond?

Commentary

1. It’s prudent for the dean to seek legal advice, since the complaints against Baxter raise a host of law and policy issues. The first place both the Dean and Legal Counsel need to turn is to the compilation of campus policies, including any computer use policy, and the code of student conduct. Any attorney representing Baxter will look carefully to see if a case can be made that the college violated its own rules.

2. Electronic communications give individuals remarkable power to disseminate ideas and opinions. Each student can become a publisher, with a reach equal to or greater than the traditional campus newspaper. The current electronic medium, largely without face-to-face contact, also seems to inspire abrasiveness and incivility. Still, preliminary indications from the courts are that traditional First Amendment standards will apply. See U.S. v. Baker, 890 F. Supp. 1375 (E.D. Mich. 1995) (Fantasies or “musings” about violence on the Internet are protected by the First Amendment, absent some expression of intent to commit the injury) and Cubby v. CompuServe Inc. 776 F. Supp. 135 (S.D.N.Y., 1991) (electronic news distributor, like a library or newsstand, not liable for defamation unless it knew or had reason to know of defamatory statements).

The dean should realize that Baxter did not lose (and cannot be forced to waive) his First Amendment rights when he enrolled at a public institution of higher education. See Tinker v. Des Moines School District 393 U.S. 503, 508 (1969) (wearing arm bands in silent classroom protest protected by the First Amendment). Justice Fortas observed that students do not “shed their constitutional rights to freedom of speech or expression at the schoolhouse gate.” See also Healy v. James 408 U.S. 169, 180-181 (1972):

...the precedents of this court leave no room for the view that, because of the acknowledged need for order, First Amendment protections should apply with less force on college campuses than in the community at large. Quite to the contrary, “[t]he vigilant protection of constitutional freedoms is nowhere more vital than in the community of American schools.” Shelton v. Tucker, 364 U.S. 424, 487 (1960). The college classroom with its surrounding environs is peculiarly the ‘marketplace of ideas’ and we break no new constitutional ground in reaffirming this Nation’s dedication to safeguarding academic freedom.
The fact that Baxter has First Amendment rights does not mean he can say whatever he wants whenever he pleases. Reasonable "time, place, and manner" restrictions will apply. See Perry Educational Ass'n v. Perry Local Educators' Ass'n 400 U.S. 37 (1983) (a school internal mail system is not a traditional public forum). Baxter's e-mail discussion group was created as a classroom activity to address a particular subject. He may legally receive a lower grade, or be subject to a disciplinary sanction, for engaging in extraneous discussions, especially if those discussions can be said to have "substantially interfered with the opportunity of other students to obtain an education." Healy, p. 189.

Baxter may also be subject to disciplinary and criminal charges for threatening two of his classmates. The Supreme Court has distinguished "true" threats from "conditional" threats, especially when the latter may represent nothing more than the expression of strongly held social or political views. An example of such a "conditional" threat can be found in Watts v. United States 394 U.S. 705 (1969).

There, the Supreme Court held that the following public statement—"crude" and "offensive" though it might be—was protected by the First Amendment:

They always holler at us to get an education. And now I have already received my draft classification as 1-A and I have got to report for my physical this Monday coming. I am not going. If they ever make me carry a rifle the first man I want to get in my sights is L.B.J. They are not going to make me kill my black brothers.

The threat articulated by Baxter in this case does not seem to be conditional, and it did inspire what appears to have been genuine fear on the part of the recipients, who acted accordingly. Although some might see it as an example of childish braggadocio, consideration of all the circumstances could lead a reasonable person to infer that Baxter had indeed summoned friends who would harm the two complainers. Baxter can be held accountable if he knew or should have known "that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of intent to harm or assault." United States v. Orozco-Santillan, 903 F.2d 1262 (9th Cir. 1990).

Furthermore, Baxter appears to have tried to use a threat of physical harm to prevent other students from exercising their First Amendment rights. This behavior could violate campus rules against "intentionally and substantially interfering with the freedom of expression of others on university premises or in university sponsored activities." See Pavela "Limiting the Pursuit of Perfect Justice on Campus" 6 Journal of College and University Law 137 (1980).

Baxter's internal e-mail message was not transmitted in interstate commerce. Otherwise, he could have been charged with a violation of federal law. 18 U.S. Code, Section 875 (c) provides that: "Whoever transmits in interstate commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined not more than $1,000 or imprisoned not more than five years, or both" (emphasis supplied).

Aside from the issue of threats, or interference with freedom of expression, Baxter's repeated and unwelcome e-mail messages, designed to harass the recipients, may violate state law, and campus computer use policies. In Maryland, for example, a recent amendment to Section 555A, Article 27 of the "Crimes and Punishments" code (House Bill 441, 1995) provides, in part, that:

(A) It shall be unlawful for any person to use telephone facilities or equipment, or electronic mail or similar electronic communication:

(1) For an anonymous call or calls if in a manner reasonably to be expected to annoy, abuse, threaten, or embarrass one or more persons;

(2) For repeated calls, if with the intent to annoy, abuse, threaten, harass, or embarrass one or more persons; or

(3) For any comment, request, suggestion, or proposal which is obscene, lewd, lascivious, filthy, or indecent.

(B) Any person violating any one of the provisions of this section is guilty of a misdemeanor, and, upon conviction thereof, shall be subject to a fine of not more than $500 or to imprisonment for not more than 3 years, or both . . .

Baxter's Web site posting accusing a writer of plagiarism may constitute defamation, if it is untrue. The college probably won't be held liable, however, unless it claimed to exercise editorial control over the content of messages posted, or failed to take reasonable action after knowing, or having reason to know, of the allegedly defamatory statements. See Cubby, supra, . . .

As Steven McDonald, Associate Legal Counsel at Ohio State University, suggests in his Synthesis interview (p. 550) the college must respond in a way that takes into consideration Baxter's "countervailing First Amendment, academic freedom, and due process rights." A simple accusation of defamation does not mean the college "knows" defamation has occurred. Assuming the "Student Voices" Web site is considered a "public forum," the college should not remove the disputed posting unless a complaining party shows there is substantial evidence to support a defamation claim.

It may even be reasonable for the college to contend that a campus Web site "public forum" is analogous to an independent campus newspaper, supported by student fees and/or provided subsidized space on campus. One court has held that the First Amendment precludes a college from censoring or controlling the content of such a newspaper, thereby shielding the college from accusations of libel. Mazart v. State of New York 441 N.Y.S. 2d 600 (Ct. Cl. 1981).

A ban on the use of automated or "chain mail" messages will probably be upheld as a reasonable time, place, and manner regulation. If necessary to prevent disruption of computer services, Baxter may lawfully be held accountable for sending prohibited chain mail—not because the mail he sent contained quotations from Nietzsche. Baxter also has ample alternative ways (e.g. a Web site posting) to communicate his views.

Given the facts of this case, and assuming there is no proven copyright violation, Baxter's publication of Nietzsche quotations, and statements critical of the university, in what would probably be considered public forums (the "student opinion" bulletin electronic board, and the UAC Web page) are protected expression, and may not be removed, or result in punishment to Baxter or the UAC, even if deemed anti-Semitic, offensive, or outrageous. A key case
is National Socialist White People’s Party v. Ringers, 473 F. 2nd 1010, 1015-1019 (Fourth Cir., 1973), involving a re-quest by an organization advocating racist policies to use public school facilities for an after-hours meeting:

We conclude that the school auditorium, since it has effec-tively been partially dedicated for first amendment uses, may be used for purposes of assembly, communicating thoughts between citizens and discussing public questions. In a public place regularly used for the exercise of free speech and the exchange of ideas, we do not see how walls and roofs can insulate against the reach of the First amendment’s commands. That amendment’s protections cannot be made to turn on . . . structural distinctions . . .

[T]he expression of racist and anti-Semitic views in a public place and the right to assemble in a public place for the purpose of communicating and discussing racial and anti-Semitic views are protected activities and may not be circumscribed by the state, except where “advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action” Brandenburg v. Ohio, 395 U.S. 444, (1969) . . .

The use of facilities partially dedicated as a public forum for the exercise of diverse views does not amount to state espousal of racist views . . .

As Mr. Justice Brandeis said years ago, “If there be time to expose through the discussion the falsehood and fallacies, to avert the evil by processes of education, the remedy to be applied is more speech, not enforced silence.” Whitney v. California 274 U. S. 357, 377 (1927).

See also Widmar v. Vincent 70 L.Ed. 2d 440, 452 (1981). There, the Supreme Court held that a University of Missouri at Kansas City decision to bar a student religious group from using university facilities “for purposes of religious worship or religious teaching” was an unjustifiable infringement upon the First Amendment rights of freedom of speech and freedom of association. The Court wrote that:

The basis for our decision is narrow. Having created a forum generally open to student groups, the University seeks to enforce a content based exclusion of religious speech. Its exclusionary policy violates the fundamental principle that a state regulation of speech should be content-neutral, and the University is unable to justify this violation under applicable constitutional standards.

In University of California Board of Regents v. Bekke 438 U. S. 265 (1978), Justice Powell agreed with an argument made by the University of California that the University had a right, protected by academic freedom, to select students who would contribute most to a “robust exchange of ideas” on campus. Accordingly, at least in Justice Powell’s view, the goal of achieving greater “diversity” appears to have some linkage to freedom of expression. The more colleges try to limit expression, the more hollow their arguments for affirmative action will become.

Colleges sometimes offer indirect support to student newspapers (e.g. use of institutional facilities, or access to student fee monies) in order to promote debate and discussion on campus. The same rationale probably applies when students and student groups are allowed to use college computer equipment to create Web pages. If so, as stated in Mazer, supra, at 605:

[C]ensorship or prior restraint of constitutionally protected expression in student publications at State-supported institutions has been uniformly proscribed by the Courts. Such censorship or prior restraint cannot be imposed by suspending editors . . . suppressing circulation . . . requiring prior approval of controversial articles . . . excising or suppressing distasteful material . . . or by withdrawing financial support . . . [extensive citations omitted].

A particularly good example of how a court might view the UAC Web site—pertinent to the issue of protecting pro-vocative student expression critical of institutional policies—is Joyner v. Whiting 447 F. 2d 456, 458 (4th Cir. 1973). The court, in Joyner, held that campus administrators could not withdraw funding from a student newspaper at a predominantly black state university after an editorial referred to “a rapidly growing white population on our campus” and stated:

[w]e want to know why they are here . . . Black students on this campus have never made it clear to those people that we are indeed separate from them, in so many ways, and wish to remain so . . . aggression is the order of the day . . . [citing H. Rapp Brown].

Private institutions of higher education in most states are not obliged to adhere to First Amendment requirements. Still, First Amendment standards might be applied as a matter of policy. Consider the views of then Harvard University President Derek Bok in the March 15, 1991 Harvard University Gazette:

Although it is not clear to what extent the First Amendment is enforceable against private institutions, I have great difficulty understanding why a university such as Harvard should have less free speech than the surrounding society—or than a public university, for that matter. By the nature of their mission, all universities should be at least as concerned with protecting freedom of expression as the rest of society. Like the rest of society we should also worry about who will draw the lines and how wisely they will be drawn if we begin to restrict the bounds of permissible speech . . .

In addition, I suspect that no community can expect to be-come humane and caring by restricting what its members can say. The worst offenders will simply find other ways to irritate and insult. Those who are not malicious but merely insensitive are not likely to learn by having their flags or pamphlets torn down. Once we start to declare certain things “offensive,” with all the excitement and attention that will follow, I fear that much ingenuity will be exerted trying to test the limits, much time will be spent trying to draw tenuous distinctions, and the resulting publicity will eventually attract more attention to the offensive material than would ever have occurred otherwise (p. 1, 4).

The use of broad terms like “offensive” or “outrage-ous” to censor constitutionally-protected expression won’t impress a reviewing court. See generally Doe v. Uni-versity of Michigan, 721 F. Supp. 852. 867 (E.D. Mich., 1989), striking down the University’s “speech code”: “Stu-dents . . . were necessarily forced to guess at whether a comment about a controversial issue would later be found to be sanctionable under the policy.”


If there is a bedrock principle underlying the First Amend-ment, it is that the government may not prohibit the expres-sion of an idea simply because the society finds the idea itself offensive or disagreeable . . . We have not recognized an exception to this principle even when our flag has been involved . . . =>

SYNTHESIS: Law and Policy in Higher Education • Spring, 1996

Despite their sometimes caustic nature, from the early cartoons portraying George Washington as an ass, down to the present day, graphic depictions and satirical cartoons have played a prominent role in public and political debate... Respondent contends, however, that the caricature in question here is so "obscene" as to distinguish it from more traditional political cartoons... [But] "[o]bscenity" in the area of political and social discourse has an inherent subjectivity about it which would allow a jury to impose liability on the basis of the jurors' tastes or views.

The UAC Web page containing a simulated picture of Nietzschke and Ayn Rand in the nude probably isn't obscene. See Miller v. California 413 U.S. 15 (1973). To be "obscene," the material in question must be determined to be "patently offensive," appeal to "prurient interests," and, taken as a whole, lack "serious literary, artistic, political, or scientific value." College officials should refer the matter to the police if they have any doubts.

The picture in question, however, may be available on the Internet to minors. Accordingly, UAC may have violated the federal Communications Decency Act (CDA) (see the Syntax Weekly Report excerpt on p. 563). Some observers believe a university would also be in violation if it failed to remove (or shield) indecent expression from minors, once it "knew" about the expression. Others suggest a careful balance of interests, reflecting ambiguous language in the CDA, and the prominence of the First Amendment, will excuse a university, unless it "intends" that its facilities be used for conveying indecent expression to minors.

If the CDA (and comparable state statutes) are held to be constitutional, the most conservative course would require that the offending material be removed, or shielded. The CDA also contains a provision apparently designed to protect individuals and institutions from liability for taking such action.

Care should be taken to avoid applying something akin to a CDA "indecency" standard to communications among adult students on campus. See Peepish v. Board of Curators of the University of Missouri 410 U.S. 667, 670 (1973), in which the Supreme Court overturned the expulsion of a graduate student (associated with the Students for a Democratic Society), who had distributed a publication on campus containing "offensive" language, and debates the effect of this legislation. Even if a college or university determined that controlling the networks is a good idea, it may be practically impossible to monitor electronic communications. Cornell, for example, handles over 300,000 e-mail messages a day. What institutions can do, however, is respond appropriately when someone brings a complaint about misuse of institutional computer resources.

SYNTHESIS: What campuses would you cite as having particularly thoughtful computer use policies?

HODGES: Well, I may be biased, but I include Cornell's Responsible Use of Electronic Communications Policy in that list. The best part of the Cornell policy is the attached table that provides the reader with example complaints (violations),

Marjorie W. Hodges... [from p. 556]
CompuServe, a commercial on-line service provider, was not liable for defamatory statements posted on its computer bulletin board. The district court granted the defendant summary judgment noting that CompuServe had "little or no editorial control" over postings and likened the company to a distributor, rather than a publisher.

Drafters of campus computer use policies would be well advised to seek guidance from university counsel on state law as well as the Telecommunications Act of 1996 and ensuing court challenges. The CDA includes language that is an apparent attempt to overrule the Prodigy decision, and that attempt may impose some duties on institutions to shield minors from certain material. Currently, legal scholars are

SYNTHESIS: Law and Policy in Higher Education Spring, 1996
the language to use to respond to those complaints and the office responsible for a given violation. It is a practical document. I am also impressed with the University of Texas–Austin’s electronic mail policy. While it is more narrow in scope than some policies (it doesn’t include Web pages), it does provide a thoughtful analysis of the issues that an institution ought to consider when developing a computer use policy. I also recommend the University of Delaware’s Policy for Responsible Computing. This document is clearly written and works with existing laws and policies as well as existing university disciplinary procedures, which is something that I highly recommend.

SYNTHESIS: What is the best way to educate students about computer use and abuse?

HODGES: This is a particularly important question because there is a computer use culture that often runs counter to institutional policies and state and federal laws. For example, many individuals would violate copyright law on-line without thinking about copyright issues. Many computer users view all information, including images and literary works, fair game once placed on the Internet. In order for campus computer use policies to work, institutions will need to influence the on-line culture.

Sample Policy . . . [from p. 553]

"Harassment is a violation of Cornell’s policies and codes, and in some cases state or federal laws. Complaints must be filed by the targeted person. If appropriate, please encourage the targeted person to contact Cornell’s Office of the Judicial Administrator for information or assistance."

VIOLATION: A4. Posting or otherwise disseminating personal or sensitive information about an individual(s).

(Examples include postings of an individual’s academic records; medical information; social security number; or similar information of a personal or confidential nature that, if disseminated, could have legal or otherwise damaging implications either for the targeted person or the institution. Personal expression by an individual about another, even if posted in a public manner, is not subject to limitation or restriction under this policy, although a targeted person may have recourse under other campus policies or codes, or state or federal laws regarding harassment.)

Who files complaint: Targeted individual; OR System or network administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from targeted individual.

(Generally, preemptive restrictive actions are not warranted but may be in exceptional cases. If the material is of such a nature that it potentially bears external consequences for the institution, contact your college/unit policy officer and the Office of Information Technologies for further guidance or assistance.)


Appropriate action if violation is reported by targeted individual: Provide the targeted individual with the following information:

"This material may violate Cornell’s codes or policies, or possibly state or federal laws. If you wish the material temporarily restricted while you file a complaint, please contact me.”

Contact your college/unit policy officer or the Office of Information Technologies for further guidance or assistance.

Appropriate action if violation is reported by another individual(s): Provide the party with the following information:

"Thank you for forwarding this information. I will be working with campus authorities regarding this incident.”

Contact your college/unit policy officer or the Office of Information Technologies for further guidance or assistance.

B. Violations causing harm to the activities of others


Who files complaint: System or network administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from individual(s) receiving the chain mail.

Who receives complaint: Office of the Judicial Administrator.

Appropriate action if violation is reported: Provide the party with the following information and take steps outlined below:

"Although we understand that some of these letters can be offensive or unwanted, [name of unit] cannot prevent their circulation. Forwarding chain mail using university resources violates Cornell’s codes and policies, and in some cases may be illegal. I will be working with the campus authorities regarding this incident.”

1. Post a notice to your system alerting users to the incident and instructing them not to propagate further.
2. Refer Cornell propagators to the Office of the Judicial Administrator.
3. If the propagator(s) is not a member of the Cornell community, contact the administrator of the originating system, if possible, as a matter of courtesy or follow-up.
4. Contact your college/unit policy officer and the Office of Information Technologies if you believe the content of the material to be illegal, damaging, or otherwise to have external consequences for the institution.

VIOLATION: B2. Interfering with freedom of expression of others by "jamming" or "bombing" electronic mailboxes.

Who files complaint: Individuals(s) affected by the interference; OR
Appropriate action if violation is reported: Provide the party with the following information:

"This incident may violate campus policies or codes. I will be working with college authorities to review what actions may be appropriate."

Contact your college policy officer for further guidance.

C. Violations involving illegal proprietary, or damaging material

VIOLATION: C1. Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements: OR

C2. Launching a computer worm, virus, or other rogue program: OR

C3. Downloading illegal, proprietary, or damaging material to a university computer: OR

C4. Transporting illegal, proprietary, or damaging material across Cornell’s networks.

Who files complaint: Anyone who has evidence of such activities occurring or about to occur, and involving Cornell’s computer and network systems.


Appropriate action if violation is reported: Commensurate with the degree of urgency and potential damage to the institution, take pre-emptive steps—preferably with the approval of your college/unit policy officer—including ensuring the preservation of evidence. Contact the office of Information Technologies for further guidance or assistance.

Clarification regarding C1: Responsible Use policy and procedures govern incidents involving the illegal distribution of copyrighted material—as transported through Cornell’s networks or posted to Cornell’s computers—by electronic means. The possession of misappropriated copyrighted material by a member of the Cornell community violates the Campus Code of Conduct, the Code of Academic Integrity and the university’s policy on the Abuse of Computers and Network Systems.

D. Violations targeted at classes of individuals

VIOLATION: D1. Posting hate speech regarding a group's race, ethnicity, religion, gender, or sexual orientation.

Note: Posting hate speech generally does not constitute a violation of Responsible Use Policy, but may under certain circumstances.

Who files complaint: Member of the targeted group: OR

System or network administrator, in accordance with guidelines established by the designated college/unit policy officer, and in response to complaint from member(s) of the targeted group.

Who receives complaint: Office of Human Relations

Appropriate action if violation is reported: Provide the party with the following information:

"Although this posting/communication may be offensive to members of the community, the university is respectful of expression in its own right. However, this posting/communication may constitute harassment, which is a violation of Cornell’s policies and codes, and in some cases, state or federal laws. I will consult with campus authorities regarding this incident."

Contact the Office of Human Relations for guidance or assistance.
The Communications Decency Act

96.5 FUTURE / TECHNOLOGY

Indecent communications on interactive computer services

Congress has approved a new telecommunications law that included a provision (the Communications Decency Act) prohibiting indecent communications sent or displayed to minors through "any interactive computer service." This provision could have a significant impact on colleges, both as a possible model for campus computer use policies, and because users of college computer services (e.g., some first-year students) are likely to include individuals who are less than 18 years old. President Clinton reportedly will sign the law, which will be tested in lawsuits filed by civil liberties groups opposed to censorship on the Internet. We predict the Communications Decency Act (CDA) will be found unconstitutional because it erroneously applies the broadcast media "indecency" standard to computer networks, World Wide Web sites, Usenet newsgroups, or other forms of Internet communications.

Communications Decency Act

The CDA defines the term "interactive computer service" to mean "an information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

Among other changes, the United States Code (47 U.S.C. 223) is then amended by adding new subsections "(d)" and "(e)," as follows:

(d) Whoever—
1. (1) in interstate or foreign communications knowingly
   (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
   (B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

2. any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
3. knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

(e) In addition to any other defenses available by law:
1. (1) No person shall be held to have violated subsection . . .
2. solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the context of the communication . . .
3. No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.
4. It is a defense to a prosecution under subsection . . . that a person . . . has taken in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or . . . has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

The "indecency" standard and the broadcast medium

The CDA prohibition against "patently offensive" communication on interactive computer services tracks FCC "indecency" rules restricting language in the broadcast medium "that describes, in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities and organs, at times of the day when there is a reasonable risk that children may be in the audience." 56 FCC2d at 98, cited in FCC v. Pacifica Foundation 75 L. Ed. 2d 1073, 1082 (1978). Those FCC rules (and a related federal statute) were upheld by a sharply divided Supreme Court in Pacifica, for reasons that make it unlikely the CDA will survive a constitutional challenge. Essentially, five members of the Court in Pacifica were willing to limit the First Amendment right to freedom of expression on a broadcast medium "uniquely accessible to children, even those too young to read" (p. 1093). The limitation was described as a "narrow" one, designed to "channel" the broadcast of "indecent" expression, not ban such expression altogether.

Nebraska Senator James Exon and other supporters of the CDA cite the Pacifica case with approval. Reading the following excerpts from Justice Stevens' plurality opinion will help you decide if the reasoning in Pacifica can be construed to fit a criminal statute applicable to computer communications:

This case requires that we decide whether the Federal Communications Commission has any power to regulate a radio broadcast that is indecent but not obscene.

A salacious humorist named George Carlin recorded a 12-minute monologue entitled "filthy Words" before a live audience in a California theater . . . . The transcript of the recording, which is appended to this opinion, indicates frequent laughter from the audience . . . .

A few weeks [after a broadcast of the monologue] a man, who stated that he had heard the broadcast while driving with his young son, wrote a letter complaining to the [FCC] . . . .

[The] Pacifica [Foundation, owner of the radio station in question] characterized George Carlin as "a significant social satirist" who "like Twain and Sahl before him, examines the language of ordinary people . . . Carlin is not mouthing obscenities, he is merely using words to satirize as harmless and essentially silly our attitudes towards those words . . . ."

If there were any reason to believe that the Commission's characterization of the Carlin monologue as offensive could be traced to its political content—or even to the fact that it satirized contemporaneous attitudes about four-letter words—First Amendment protection might be required. But that is simply not this case. These words offend for the same reasons that obscenity offends. Their place in the hierarchy of First Amendment values was aptly sketched by Mr. Justice Murphy when he said "[S]uch utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality." Chaplinsky v New Hampshire 86 L. Ed. 1031 . . .

We have long recognized that each medium of expression presents special First Amendment problems . . . And of all
forms of communication, it is broadcasting that has received the most limited First Amendment protection . . .

The reasons for these distinctions are complex, but two have relevance to the present case. First, the broadcast media have established a uniquely pervasive presence in the lives of all Americans . . . [including] in the privacy of the home . . . Because the broadcast audience is constantly tuning in and out, prior warnings cannot completely protect the listener or viewer from unexpected program content . . .

Second, broadcasting is uniquely accessible to children, even those too young to read. Although a written message might have been incomprensible to a first grader, Pacifica’s broadcast could have enlarged a child’s vocabulary in an instant . . .

It is appropriate, in conclusion, to emphasize the narrowness of our holding. This case does not involve a two-way radio conversation between a cab driver and a dispatcher, or a telecast of an Elizabethan comedy. We have not decided that an occasional expulsive in either setting would justify any sanction or, indeed, that this broadcast would justify a criminal prosecution. The Commission’s decision rested entirely on a nuisance rationale under which context is all important. The context requires consideration of a host of variables. The time of day was emphasized by the Commission. The content of the program in which the language is used will also affect the composition of the audience, and differences between radio, television, and perhaps closed-circuit transmissions, may also be relevant. As Mr. Justice Sutherland wrote, a “nuisance may be merely a right thing in the wrong place—like a pig in the parlor instead of the barnyard” . . . [citation omitted].

We simply hold that when the [FCC] finds that a pig has entered the parlor, the exercise of regulatory power does not depend on proof that the pig is obscene.

Last month the Supreme Court refused to review a D.C. Circuit decision upholding a portion of another federal law (the Public Television Communications Act of 1992) that restricted the hours within which “indecent” radio and television programs could be broadcast. Action for Children’s Television v. F.C.C., 58 F.3d 654 (D.C. Cir. 1995). Although this decision will also be cited in support of the constitutionality of the CDA, the circuit court stressed “the unique context of the broadcast medium” and noted that—even in such a medium—it had previously struck down a total (24 hour) ban on indecent expression. Action for Children’s Television v. FCC, 932 F.2d 1504 (D.C. Cir. 1991).

"Indecency" and other forms of communication

The application of the broadcast medium indecency standard to interactive computer services is also called into question by Supreme Court cases refusing to provide comparable (i.e. lowest level) First Amendment protection to commercial telephone and cable communications.

In Sable Communications v. FCC, 106 L. Ed. 2d 93 (1989) the Court held that a ban on indecent interstate commercial telephone communications (e.g. dial-a-porn services) violated the First Amendment. After noting the government’s reliance upon the Pacifica case, the Court observed that:

Pacifca is readily distinguishable from this case, most obviously because it did not involve a total ban on broadcasting indecent material. The FCC rule was not “intended to place an absolute prohibition on the broadcast of this type of language, but rather sought to channel it to times of day when children most likely would not be exposed to it” . . . [citation omitted]. The Pacifica opinion also relied on the “unique” attributes of broadcasting, noting that broadcasting is “uniquely pervasive,” can intrude on the privacy of the home without prior warning as to program content, and is “uniquely accessible to children, even those too young to read” [citation omitted].

Under our precedents, [a ban on indecent interstate commercial telephone communications] has the invalid effect of limiting the content of adult telephone conversations to that which is suitable for children to hear. It is another case of "burn[ing] up the house to roast the pig." Buller v. Michigan, 352 U.S. 380 at 383 . . .

Likewise, when applying heightened scrutiny to content-neutral regulation of the cable television industry, the Court observed in Turner Broadcasting System v. FCC, 129 L. Ed. 2d 497 (1994) that:

The justification for our distinct approach to broadcast regulation rests upon the unique physical limitations of the broadcast medium . . . As a general matter there are more would-be broadcasters than frequencies available . . . Accordingly, the inherent physical limitation on the number of speakers who may use the broadcast medium has been thought to require some adjustment in traditional First Amendment analysis to permit the Government to place limited content restrictions, and impose certain affirmative obligations, on broadcast licenses . . .

The broadcast cases are inapposite in the present context because cable television does not suffer from the inherent limitations that characterize the broadcast medium. Indeed, given the rapid advances in fiber optics and digital compression technology, soon there may be no practicable limitation on the number of speakers who may use the cable medium . . . In light of these fundamental technological differences between broadcast and cable transmission, application of the more relaxed standard of scrutiny adopted in . . . … the broadcast cases is inapt when determining the First Amendment validity of cable regulation.

Practice Implications = Applying the broadcast "indecency" standard approved in the Pacifica case to a criminal statute applicable to interactive computer communications is a clearly a stretch. First, as University of Maryland General Counsel and Syntax Contributing Editor Terry Roach advised us, the Supreme Court in Pacifica indicated it might have reached a different result if a criminal prosecution had been involved.

Second, the Court continues to see a distinction between a broadcast medium in which children might be a passive or even captive audience (e.g. listening to a car radio) and forms of communication that require a listener or viewer to take "affirmative steps to receive the communication" (Sable, supra, at 106). Third, the Supreme Court—unlike Congress in the CDA—would not approve a complete ban on indecent expression simply because some minors might gain access to it. Finally, when considering the attributes of cable television (a form of communication comparable to and now blending with interactive computer communications) the Supreme Court expressly declined to apply the "more relaxed standard of [First Amendment] scrutiny" given to the "limited spectrum" broadcast industry.

The CDA is a complex, confusing law. Authoritative interpretation must come from legal counsel on your campus. Still, even if held to be constitutional, it’s our view the CDA would not authorize or require colleges to censor student-initiated interstate or foreign computer communications. Largely at the behest of on-line service providers, the law appears to protect those whose computer systems are used simply to transmit indecent material.

Furthermore, it’s reasonable to suggest the law could not be used to punish a service provider who failed to remove an "indecent" posting subsequently seen by a minor, unless the service provider intended that the minor see it . . .
