

# Legal Underpinnings for Creating Campus Computer Policy

by Marjorie W. Hodges and Steven L. Worona

Ten years ago, institutions of higher education worried about computer hackers and crimes of unauthorized access—break-ins, stolen files, viruses, worms. Back then, computers were used by technical people to do technical things. Perhaps understandably in that environment, computer crimes were met with computer punishments. What worse penalty for a hacker than closing his computer account? Today, however, computers are an essential part of day-to-day life. Students, faculty, and staff use computers in course enrollment, discussion groups, assignments, research projects, and exams. The old way of punishing computer-related abuse would, today, be tantamount to expulsion or termination. And yet, on many college campuses, computer use policies and practices have not evolved in concert with the changing computer culture.

As computer use has changed, so, naturally, have the types of misbehavior occurring on computer networks. The same misbehaviors that colleges and universities have addressed in student residence halls for decades are now appearing in computer-related incidents. Rather than inventing a whole new way to deal with these computer-related incidents, it is generally preferable to utilize the existing institutional policies and procedures that address misbehavior. Ideally, these policies rest on the fundamental principles of the institution. For example, most colleges and universities have a well-developed and tested campus code of conduct and/or honor code. By relying on the disciplinary models found in these codes, colleges and universities influence the online culture in the same fashion as they affect the on-campus culture.

Moreover, employing existing judicial systems also indicates the importance placed on incidents of computer-related misbehavior. While this may seem counterintuitive—if it is important, then shouldn't we treat it specially?—the best way to highlight the seriousness of an offense is to channel it through the offices capable of imposing the most serious institutional penalties—suspension and expulsion. Computer-based misbehavior is too serious to be treated as simply an administrative matter. As an

added benefit, if complaints about network behavior follow the same procedures applied in residence halls, the institution will adhere to established procedures for due process, notification, representation, and the like.

If computer use policies are to rely on existing institutional principles, then there will be a variety of policy choices matching the variety of institutions. While computer use policies can fall anywhere on a continuum, all should include the following six components:

- a statement explaining the reason for the policy
- a statement about what the policy covers
- the individuals covered by the policy
- specific examples of inappropriate behavior
- instructions about how to report a violation
- information about potential consequences for violations

Computer use policies cannot succeed unless they represent the institutional culture; therefore, it is essential for community members to be a part of their creation. A representative community cross-section might include the vice president for information technologies, the vice president of student affairs, the dean of students, campus legal counsel, the judicial administrator, the vice president for human relations, and representatives of students, faculty, and staff.

Once a policy is adopted, institutions have the opportunity to offer instruction on acceptable computer use, thus raising awareness of the issues and increasing compliance. Such instruction may be instituted as a precondition to network access; remedial instruction may also be offered (or required). A further way to encourage discussions about computer policies with faculty and student participation is to use the never-ending stream of current news reports as a springboard for debates and dialogue.

The rest of this paper deals with five key policy areas:

- ✓ Adult material
- ✓ Harassment
- ✓ Privacy
- ✓ Commerce
- ✓ Copyright



**Marjorie W. Hodges** (*mwh2@cornell.edu*) is Policy Advisor, Office of Information Technologies, at Cornell University and a frequent speaker on the ethical and legal aspects of computer policies. She has also served as Cornell's judicial administrator, a position in which she dealt with a wide variety of computer abuse cases. She is presently preparing a monograph on freedom of expression and the electronic campus.



**Steven L. Worona** (*slw1@cornell.edu*) is assistant to the Vice President for Information Technologies at Cornell University. In addition to collaborating with Marjorie Hodges in the area of computer policy and law, Worona is technical director of Cornell's digital library project, supervises development of the CUPID network printing system, and represents the University on a variety of off-campus working groups and organizations.

---

---

*“Contrary to a widely held perception ... the First Amendment protection of speech is not absolute.”*

---

---

### Adult material

Although concerns about adult material don't represent the majority of computer-related complaints, they currently cause the greatest public interest and are the most likely to receive media attention. Policies on adult material must be guided by both the institutional requirements imposed by law and institutional principles and culture. Especially with respect to legal requirements, the general class of “adult material” may be usefully broken down into these four categories:

- ✓ Pornography
- ✓ Obscenity
- ✓ Child pornography
- ✓ Indecency

For the most part, the laws that must be taken into account are the First Amendment of the U.S. Constitution, federal and state obscenity statutes, federal and state child pornography statutes, and indecency regulations.

The First Amendment of the U.S. Constitution prohibits the federal government from abridging freedom of speech, and the “due process clause” of the Fourteenth Amendment extends this prohibition to the actions of state governments. It is an accepted extension of these principles that public institutions, such as state universities, are also limited in their ability to control speech. Furthermore, private institutions, including private colleges, may be held to these same restrictions if they provide a “public forum” or if state legislation incorporates First Amendment language. Contrary to a widely held perception, however, the First Amendment protection of speech is not absolute. Reasonable time, place, and manner restrictions are permissible. The courts also give some speech a lesser degree of protection and have denied some speech protection altogether. We all know, for example, that “you can't shout fire in a crowded theater.”

In common parlance, “pornography” is a generic term for erotic material of all types. In general, pornography receives full First Amendment protection, but there are a variety of important exceptions. For example, the Supreme Court has upheld the constitutionality of statutes prohibiting the sale and distribution of certain adult material (pornography) to minors.

“Obscenity,” by definition, is a type of pornography that is not protected by the First Amendment. The Supreme Court in *Miller v. California* (1973) narrowed the permissible scope of obscenity statutes and outlined a three-part test to define obscenity. To be legally suppressed as obscenity, material must meet all three prongs of the test, which asks (1) whether an *average person*, applying *contemporary commu-*

*nity standards* would find that the work, *taken as a whole*, appeals to the prurient interest; (2) whether the work depicts or describes in a patently offensive way, sexual conduct specifically defined in applicable state law; and (3) whether the work *taken as a whole*, lacks serious literary, artistic, political, or scientific value. Virtually every state and municipality has a statute prohibiting the sale and distribution of obscene material and the federal government prohibits its interstate transportation.

Of all the types of adult material that fall outside the umbrella of First Amendment protection, “child pornography” carries the most far-reaching restrictions and the harshest penalties. Child pornography is defined as material that depicts minors in a sexually explicit way, which is much broader than the definition of obscenity—material does not have to be obscene to constitute child pornography. The age of a minor varies by state, but the federal child pornography statute applies the term to anyone under eighteen. The Supreme Court based child pornography restrictions on the state's compelling interest in protecting the children used to produce such material. Child pornography is the only category of adult material whose mere possession is a crime.

“Indecency” applies to a type of adult material which, while generally protected by the First Amendment, has been found by the Supreme Court to be legitimately regulated, in certain instances, by a narrowly tailored statute. Broadcast radio, for example, is such an area, where the courts allow FCC regulations limiting indecency to certain times of the day. In the well-known case *FCC v. Pacifica Foundation* (1978), the Supreme Court upheld FCC sanctions against the broadcaster who aired George Carlin's “seven dirty words” monologue during the middle of the afternoon, stressing its pervasiveness and the inability to exclude minors from the audience. The courts have also allowed regulation of indecency in telephone communications offered for a price, opening the door for so called “dial-a-porn” statutes, which require use of credit cards.

In addition to existing regulations on adult material, the Communications Decency Act of 1996 (CDA), attempts to criminalize indecency on the Internet. A number of states have already passed similar acts. Because the CDA was held unconstitutional by two district court panels, prosecutions are currently being deferred, pending decision by the Supreme Court.

The above summary, as further refined by applicable state and local laws, implicitly defines a range of legally acceptable institutional policies. Within this range, the institution is free to

---

create a policy consistent with its culture and values. There is no objectively “right” or “wrong” policy, and policies may be expected to change over time.

### Harassment

According to the dictionary, to harass is to “persistently annoy.” While many types of harassment include physical contact, physical contact is not necessary for an action to be considered harassment. Various state and federal statutes prohibit certain types of harassing speech and expression, and these statutes have survived First Amendment challenges. In addition, most institutions of higher education already have long-established policies addressing harassment. Although harassment that occurs over computer networks is limited to speech—words, images, sound—it is still covered by existing laws and policies. The new, relatively unfamiliar media raise questions of analogies—is sending e-mail to a list more like addressing a crowd or posting a handbill?—but no new concepts are involved.

The conventional definitions of harassment vary but usually require unwanted and repeated behavior targeted at one or more particular individuals. Even when harassment involves no physical contact, it is actions that are at issue, not speech. To ensure that this distinction is recognized, institutions need to rely on a clear definition of what constitutes harassment. For example, a single unwanted message to an individual is unlikely to constitute harassment. Repeated unwanted messages, especially after a request to stop, might well cross the line.

The distinction between behavior and speech is sometimes blurred, and the difference between general and specific targets is often overlooked. These issues were critical several years ago when a number of institutions attempted to promulgate “hate speech” regulations. Hate speech is a term used to describe speech which is uncivil, antagonistic, or derogatory, especially when applied to classes of people. These speech codes originated from a well-intentioned attempt to address a perceived decrease in civility on American campuses, and were not aimed at electronic communications in particular. While a few colleges and universities still have speech codes, those that have been tested in court have been found to be unconstitutional. Early cases held the first speech codes, which were ambitious in scope (such as those adopted at the University of Michigan and the University of Wisconsin) unconstitutionally vague and overbroad. The Stanford University speech code took these decisions into account, limiting its scope to

the use of “fighting words” intentionally directed at another individual in order for the University to impose sanctions. Nonetheless, a court also struck down this speech code, arguably the most narrowly drawn and well written in the country.

The subtleties in this area can be difficult to understand, and are made even muddier by the concept of “hostile environment” harassment. This type of harassment is characterized not by individual acts of harassment but by a general pattern of behavior explicitly or implicitly tolerated by an institution. Recent efforts by the U.S. Office of Civil Rights (OCR) to clarify how hostile environment concepts relate to peer-to-peer harassment are considered problematic for a number of institutions of higher education. Despite the unsettled and confusing nature of hostile environment harassment, institutional policies must nonetheless address these concerns.

### Privacy

Most Americans have a strong belief in the right to privacy, particularly students and other intellectuals on college and university campuses. This concern increases with each new technological advancement that has privacy implications (and each new technological advancement *does* seem to have privacy implications). The recent controversy surrounding Lexis-Nexis P-track services is a case in point.<sup>1</sup>

Despite our strong feelings about privacy, the legal basis for them is surprisingly tenuous. For example, neither the term “privacy” nor any synonyms appear in the U.S. Constitution. Privacy rights only became established in 1965 when Justice Douglas found them in the “penumbra” of the Constitution, an analysis still considered tortured by some legal scholars. (The penumbra doctrine holds that the federal government is authorized to take all actions “necessary and proper” to carry out a legitimate government purpose, even when these actions are not explicitly mentioned in the constitution.)

Traditional allegations of privacy violation involve such common-law claims as “intrusion,” “false light,” “disclosure,” and “appropriation.” These actions, however, generally apply only in specific circumstances. Their use in Internet-related privacy breaches is thus problematic. For example, intrusion is concerned with the protection of the commercial or property value of a person’s identity and likeness. False-light privacy involves erroneous negative publicity about an individual, but requires proof of actual malice. False-light privacy may also lose significance on the Internet because of the ease of reply, echoing a similar argument made by legal scholars in the area of defamation.

---

---

*“Despite our strong feelings about privacy, the legal basis for them is surprisingly tenuous.”*

---

---

<sup>1</sup> See <http://www.lexis-nexis.com/lnc/p-trak/index.html>

---

---

*“... the SuperPaint doodle on your Macintosh hard drive is a copyrighted work as much as the article you are now reading.”*

---

---

The unreasonable transmission of private facts on the Internet potentially involves the greatest possibility of recourse, but related case law in the area of disclosure requires proof that the privacy invasion would be highly offensive to a reasonable person and is not “newsworthy.” Moreover, the First Amendment significantly limits damages for truthful publication of private facts.

In addition to these common-law actions for invasion of privacy, federal law requires institutions of higher education to pay special attention to the privacy rights of students. The Family Education Rights and Privacy Act of 1974 (FERPA) protects the education records of students from certain disclosure without authorization.<sup>2</sup> Concern for and enforcement of student records privacy requirements under FERPA have traditionally been the province of college and university registrars. But new mechanisms for transmitting records and the emergence of new types of student records that can be generated in a networked environment are raising policy issues that must be more widely shared, suggesting the wisdom of engaging a broad segment of the campus community to address policy in this area.

In 1986, the federal government attempted to address privacy issues arising from new technologies with the Electronic Communications Privacy Act (ECPA). The ECPA was written as an extension of existing wiretap protections to non-telephone communications, making it illegal to intercept such communications in progress or to disclose stored private communications to a third party. The ECPA is relatively untested—it has never been applied, for example, to campus e-mail systems—and much of its language is confusing and contradictory. Nonetheless, it represents the only federal legislation in the area, and its strong support for privacy has influenced many college and university policies.<sup>3</sup>

Privacy policy represents a unique challenge. New technologies offer the promise of significant cost savings and important consumer services—both in high demand—but frequently entail a variety of risks to personal privacy, some not understood or not evident until too late. In the absence of clear legal requirements, colleges and universities have both the opportunity and the responsibility to create privacy policies that are carefully considered, well publicized, and conscientiously monitored.

### Commerce

For most of the lifetime of the Internet and of the Arpanet before it, commercial use of network resources was prohibited by law and by national policy. But a glance at almost any magazine or

TV ad will show how anachronistic such regulations have become. Billions of dollars worth of commerce is flowing from coast to coast over the Internet. Once the network crosses the campus boundary, however, a new set of rules takes hold.

Both the tax code and local laws have traditionally exempted colleges and universities from taxes on the assumption—and, indeed, with the stipulation—that there is a wall between the educational and commercial sectors. With the stated purpose of avoiding conflict with the Internal Revenue Service, most colleges and universities forbid the use of institutional resources—both conventional and computer-based—for commercial purposes. Colleges and universities frequently feel the need to apply these policies aggressively to their on-campus networks and computers. (In addition, and for the same ostensible reason, some institutions have attempted to regulate political speech on the Internet.)

Policy makers should review the facts, legal requirements, and policy motivations of their existing commerce rules, in order to determine how to reasonably apply them to computer- and network-based business. As the techniques and economics of network commerce evolve and mature, general policy principles will be more valuable than specific regulations. If a commercial World Wide Web server in a student residence hall is forbidden, based on use of the campus network, could that same server legitimately connect to a regional wireless net? As with the other areas covered in this paper, the key is creating a policy development process in line with institutional goals, principles, and missions.

### Copyright

The mandate to provide for copyright appears in the U.S. Constitution as a means to protect the economic incentive to be creative. By current U.S. law a work acquires copyright as soon as it is “fixed in any tangible medium of expression,” which includes not only ink on paper, but also magnetized regions on a ferrous surface. That is, the SuperPaint doodle on your Macintosh hard drive is a copyrighted work as much as the article you are now reading. While copyright requires no registration—no “circle-c”—absence of registration and notification may affect the damages due in case of infringement.

The owner of a copyright enjoys certain exclusive rights with respect to that work, including reproduction, adaptation/creation of derivative works, distribution, public performance, and public display. These rights may be sold or given away, in whole or in any combination of parts. In certain very narrow cases, one or another may be deemed to have been implicitly waived.

<sup>2</sup> FERPA is found at 20 U.S.C. 1232 g and is written in fairly plain language.

<sup>3</sup> A task force created by CAUSE, in cooperation with the American Association of Collegiate Registrars and Admissions Officers (AACRAO), is examining these issues, with the intention of circulating a white paper providing guidelines for the creation of policy on privacy of student information in a networked environment.

No other area of law has been thrown into as much definitional confusion by the new network technologies as copyright. For example, the process of viewing an image on the World Wide Web entails making a copy of that image—several copies, in fact—in a very real way, a phenomenon fundamentally absent from the process of watching a TV show or even a VCR tape. In a recent interview, Steven J. MacDonald, associate legal counsel at The Ohio State University, said, “If you are applying existing copyright law literally ... the Internet is really just one giant photocopy machine, and just about everything you do or see on it is technically a copyright infringement.”<sup>4</sup> And what about links: is a link to a Web page a copy? What about a link to an image embedded on that Web page? At least one publisher believes it has a right to control the use of such links.<sup>5</sup> What about links to an infringing copy of a work, perhaps pointing to a server in a country that doesn’t recognize copyright law? At least one version of the NII Copyright Protection Act would make such a link illegal.

The last major revision to U.S. copyright law occurred in 1974, after years of debate among such interested parties as publishers, librarians, and representatives of higher education. A key provision of the Copyright Act of 1974 is the establishment of “fair use” as a defense against a claim of copyright infringement, exempting copies made “for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.” The final determination of whether a use is “fair” is based on the court’s view of four factors, including the nature of the original work, the purpose of the use, and the economic impact of the copying. Also relevant is legislative history from 1976, the *Agreement on Guidelines for Classroom Copying in Not-For-Profit Educational Institutions*,<sup>6</sup> a document adopted by the publishing industry and thirty-eight educational institutions. Notwithstanding all of these guidelines, and even apart from the technological morass of the Internet and the World Wide Web, court decisions regarding what is and is not fair use have been less than completely consistent or predictable.

Exacerbating this confusion is the fact that copyright is a “strict liability offense,” which means that neither intent to infringe nor knowledge of infringement is necessary in order for liability to exist. As a result, a number of colleges and universities have faced threats of lawsuits for the actions of their community members accused of online copyright infringement. Despite this, the law is still unsettled with respect to institutional liability for the copyright infringement of

an Internet user. Courts have reached inconsistent conclusions regarding whether providers of various network services are more properly considered publishers or bookstores, whether they are completely responsible for content posted by third parties, or not responsible at all. Currently, the best advice for colleges and universities is to take allegations of such violations seriously and to consult with counsel.

A popular expression of Internet culture is “information wants to be free,” and there remains a sizable percent of Internet users—especially, it seems, among our student communities—who believe it to be immoral for publishers and other content providers to place limits—worst of all, *financial* limits—on the free flow of information over the net. A key goal of an institutional policy on copyright should be to help enlighten these and other segments of our communities to the facts of the law, if not its eminent wisdom.

As noted earlier, Congress is now considering another major change in the copyright law, the NII Copyright Protection Act, this time explicitly driven by computer and network technologies. No other technology-related legislation will have a greater impact on colleges and universities. Fortunately, it is not yet too late for higher education to affect the outcome.<sup>7</sup>

C/E

---

---

*“If you are applying existing copyright law literally ... the Internet is really just one giant photocopy machine, and just about everything you do or see on it is technically a copyright infringement.”*

---

---

<sup>4</sup> See *Synthesis: Law and Policy in Higher Education*, Volume 7, Number 4, Spring 1996.

<sup>5</sup> See <http://www.cs.princeton.edu/~dwallach/dilbert/>

<sup>6</sup> In H.R. Rep. No. 94-1476, 94th Cong., 2d Sess. (1976)

<sup>7</sup> See <ftp://ftp.loc.gov/>