ONLINE COMMUNITIES: RISK AND REWARDS

31ST ANNUAL NATIONAL CONFERENCE ON LAW AND HIGHER EDUCATION
STETSON UNIVERSITY COLLEGE OF LAW

February 22, 2010

Steven J. McDonald
General Counsel
Rhode Island School of Design

For those of us college administrators who came of age in that (not so) long-ago era before the Internet and who (perhaps) are still struggling to master web browsing and even e-mail,[1] dealing with computer use issues can seem an almost hopelessly daunting task. Seemingly every week brings with it the announcement of a new computer technology that is both child's play and irresistibly tempting to our computer users (especially, but not exclusively, the students among them), but mind-numbingly confusing to the rest of us: blogs, vlogs, wikis, Flickr, Twitter, podcasting, yet another variation on file sharing, or some other equally bewildering, and frequently even unpronounceable, gizmo or doohickey.

Typically, we have addressed the inevitable misuse of these Next New Thingamabobs as though it were an entirely new problem requiring an entirely new solution, often in the form of an entirely new policy containing an entirely new set of prohibitions and an entirely new set of procedures. Thus, our computer use policies, which once were little more than general admonitions to "behave yourselves," generally have evolved over time into increasingly lengthy lists of "thou shalt not" prohibitions[2] or splintered into hodgepodges of individual policies specific to the web,[3] e-mail,[4] spam,[5] file sharing,[6] blogs,[7] and more.[8]

---

[1] Which is not to say that we (necessarily) are "old fogeys." Given the extraordinary speed of Internet developments, even people who have not yet reached the untrustworthy age of 30 can count themselves among this group. As one court aptly put it, "in the Internet environment," a single year is the equivalent of "several generations, if not an eternity." EarthWeb, Inc. v. Schlack, 71 F. Supp. 2d 299 (S.D.N.Y. 1999).

[2] See, e.g., Seattle University Computer Acceptable Use Policy, <http://www.seattleu.edu/OIT/download.aspx?ID=1320&Type=.pdf>.

[3] See, e.g., Colby College Web Policy, <http://www.colby.edu/info.tech/policies/html/webpolicy.html>.

[4] See, e.g., University of Colorado System Use of Electronic Mail Policy, <https://www.cusys.edu/policies/policies/IT_Email.html>.

[5] See, e.g., Fordham University Anti-Spam Policy, <http://www.fordham.edu/images/admin_offices/legal/it_policies/Anti-Spam_policy.pdf>.

In fact, however, computer misconduct is not a new problem, but, rather, simply the most recent manifestation of an old one: the abuse and misuse of new tools. While the Internet and the various protocols it has spawned may seem wholly novel and unprecedented, they are, at bottom, just another means of distributing information. And from a policy and legal perspective, the questions these new communications technologies raise when they are misused are really no different from those raised by misuse of the various communications technologies that preceded them. To be sure, laws certainly have evolved over time, but we did not throw out the old ones and start entirely anew when the printing press, the telegraph, the telephone, radio and television, or the fax machine came along, and there is no more need to do so with the advent of the Internet than there was then.[9]

Thus, when our students, faculty, and staff misbehave on the Internet, it really is no more illuminating to call what they are doing "*computer* misconduct" than to call it simply "misconduct" – and, in fact, it may actually obscure the real issue. Consider: If a student sends a series of sexually harassing e-mail messages, and your computer use or e-mail policy doesn't specifically prohibit sexual harassment, can you address it? Posed that way, the question somehow seems troublesome, and it is, indeed, one that many of us have struggled with (and that defense counsel have attempted to exploit) for years.

Recast the question, however, and the answer becomes apparent: If a student sends a series of sexually harassing *typewritten* letters, and your *typewriter* use policy doesn't specifically prohibit sexual harassment, can you address it? Of course you can! Your existing, generally applicable sexual harassment policy and (quite likely) your general code of student conduct already prohibit sexual harassment by any means and in any venue. Just as you

---

[6] See, e.g., Asuza Pacific Peer-to-Peer File Sharing Policy, <http://www.apu.edu/imt/policiesandprocedures/peer>.

[7] See, e.g., Williamette University Web Log Policy and Service Guidelines, <http://blog.willamette.edu/blog-policy.html>.

[8] For a good, though now somewhat dated, survey of the state of college and university computer use policies generally, see Susan Athey, Computer Use Policies at Major U.S. Universities, <http://www.educause.edu/ir/library/pdf/CSD1195.pdf>.

[9] In the words of one of the first cases to involve on-line communications technologies, "Technological advances must continually be evaluated and their relation to legal rules determined so that antiquated rules are not misapplied in modern settings. '[With] new conditions there must be new rules.' (Cardozo, The Nature of the Legal Process, at 137 [Yale Paperbound 1960 ed].) Yet, if the substance of a transaction has not changed, new technology does not require a new legal rule merely because of its novelty." Daniel v. Dow Jones & Co., 520 N.Y.S.2d 334, 338 (N.Y. Civ. Ct. 1987). See also Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. Chi. Legal F. 207 at 207 (arguing that there is no more a "law of cyberspace" than there is a "law of the horse"; "the best way to learn the law applicable to specialized endeavors is to study general rules").

unquestionably can address sexual harassment committed by means of a typewriter without a typewriter use policy,[10] you can address e-mail sexual harassment whether your computer use or e-mail policy references the subject or not – indeed, you can do so even in the absence of a computer use or e-mail policy at all. The bottom line: the particular technology used to commit the harassment is nothing more than a red herring. The real issue is, and the real focus should be on, the harassment itself, which you already know how to handle.

Moreover, almost every bad thing computer users can (and do) do with their computers, not just sexual harassment, is already prohibited by some existing, generally applicable policy or law and already subject to some existing, generally applicable procedure. When your students make false and defamatory statements about others on a blog or in an e-mail message, for example, they are violating the law of libel, which also may be incorporated by reference in a general prohibition against tortious and illegal conduct in your code of student conduct. When they trade copyrighted music through the use of file-sharing software, they are engaged in copyright infringement, in violation both of copyright law and (if you have them) campus copyright policies. And when they post intrusively personal information about an "ex" on a web page, they are committing an invasion of privacy under standard tort law principles (which, again, may well be incorporated by reference into your student code). Another bottom line: as a rule, laws, policies, and procedures apply to the Internet whether or not they expressly and affirmatively reference the Internet – and even if they were written before Al Gore first conceived of the Internet. The only significant exceptions are laws, policies, and procedures that clearly are limited by their terms to a specific context or that specifically *ex*clude application to the Internet, of which there are very few.

So, do we need to constantly update our computer use (or e-mail, or file sharing, or blog, or . . .) policies in order to deal successfully with each new opportunity for computer mischief? In my view, no. Increasingly lengthy lists of "thou shalt nots" and increasingly tall stacks of increasingly specific policies are actually counterproductive for at least two reasons: First, they usually either (at best) duplicate other applicable laws and institutional policies, which adds to information overload and results in inattention, or (at worst) differ in some way from or even conflict with those laws and policies, which creates confusion. Second, policies drafted in that fashion encourage your computer users to become "tax lawyers," seeking out and exploiting the inevitable "loopholes"; the very existence of the list implies (or so they argue) that whatever is not expressly prohibited must, therefore, be permitted.

The real problem is not that we don't have enough laws and policies to deal with computer misconduct, but that our computer users (and, to be fair, often we ourselves) don't understand that existing, generally applicable laws and policies already apply to and prohibit that misconduct, let alone what those existing laws and policies have to say on the subject. This

[10] While typewritten letters frequently have been introduced as evidence in sexual harassment cases, it seems a fair assumption that typewriter use policies have not been widely adopted, let alone invoked as the basis for discipline. A Google search of "typewriter policy" and "typewriter use policy" yields only a small handful of hits, most of which deal only with who is eligible to use typewriters in public libraries.

should come as no great surprise, as computer users generally have not been required to undergo "driver training" or to be tested on the "rules of the road" before setting out on the Information Superhighway. But if lack of awareness is the real problem, it also should come as no great surprise that it will not be solved with ever more elaborate policies and procedures.

Rather, the better solution is to educate our computer users about the generally applicable laws, policies, and procedures that already exist. Here are the three most fundamental principles they need to know:

1. Cyberspace is not a separate, law-free jurisdiction. Conduct that is illegal or in violation of institutional policy in other contexts is just as illegal or in violation of institutional policy and will result in the invocation of the same procedures and the imposition of the same consequences when it occurs on-line. (Of course, in addition to this general point, it is helpful, even critical, to provide some explanation of what the relevant laws, policies, and procedures are and what they mean in this context.)

2. What is technologically possible is not the same as what is legally permissible, let alone the same as what is ethically advisable. While technology certainly has legal implications, it does not define the outer limits of the law. Computers are no more designed to prevent you from violating relevant laws and policies than cars are designed to prevent you from speeding or guns are designed to prevent you from committing murder. "Can," "may," and "should" are entirely different concepts.

3. Free *access* is not the same thing as free *speech*, nor is *free* speech the same thing as *unfettered* speech. The First Amendment does not restrict private institutions from regulating speech at all, and even public institutions, which are subject to First Amendment restrictions, have leeway to set some limits. For example, it would be perfectly legal (if not necessarily advisable or practically enforceable) for a college or university to prohibit all personal use of its computers, just as it could (and probably does) prohibit personal use of its letterhead, envelopes, stamps, and photocopiers.[11]

[11] See, e.g., Pichelmann v. Madsen, 31 Fed. Appx. 322 (7th Cir. 2002) (even if university's e-mail system was a limited public forum, which "[w]e doubt," university could, consistently with the First Amendment, require an employee to remove a "vulgar" tagline from her e-mail signature, as it was not a matter of public concern and university was not engaged in viewpoint discrimination); Loving v. Boren, 956 F. Supp. 953 (W.D. Okla. 1997), aff'd on other grounds, 133 F.3d 771 (10th Cir. 1998) (state university could limit the use of its computer systems to "academic and research purposes" and was not constitutionally required to provide unrestricted access to the Internet); Faculty Rights Coalition v. de Mino, 2005 U.S. Dist. Lexis 16227 (S.D. Tex.), aff'd, 204 Fed. Appx. 416 (5th Cir. 2006) (university e-mail system was not a public forum, and, in any event, it was not a First Amendment violation for the university to employ spam filters, impose limits on the quantity of stored e-mail, and deactivate e-mail accounts of adjunct faculty during semesters when they were not teaching).

If you follow this approach, your baseline computer use policy can – and in my view should – look a lot like your typewriter use policy, which is to say at most short and sweet. The only issues such policies really do need to cover are those that truly are unique to computer use, of which there are very few.[12] The remainder can largely be simply an incorporation (and reminder) of your other existing policies and procedures. You can then – much more profitably – devote your time to educating your computer users about their responsibilities *generally*, and applying your existing policies and procedures in this context just as you always have in others.

A significant and beneficial byproduct of such brevity is that your policy likely will be sufficiently flexible to withstand future developments in technology and the endless creativity of its misusers without constant updates and amendments. When I was at Ohio State, for example, we thought of our policy as a sort of constitution, setting forth broad, general principles that could be interpreted and fleshed out over time, as new situations arose, through a sort of "common law" method. The resulting "gloss" would then be captured not in the policy itself, but in an associated F.A.Q, which would not bear the label "policy" and therefore would not require the same sort of elaborate development and approval process. To further facilitate education and awareness, we posted both documents to the web, along with "Virtual Legality," a brief description of libel, copyright, privacy, and other relevant laws, and hyperlinked them all back and forth.[13] Let's take a look at how it worked:

[12] One issue in particular that merits attention is the privacy of user accounts. You probably don't have a truly general policy on the privacy of information, and the jumble of FERPA, public records laws, the Fourth Amendment, the Electronic Communications Privacy Act, and so forth aren't much help, so it is useful to set out a policy of what is and isn't private on your system and under what circumstances privacy can be breached. You may also wish to address such computer-specific technical issues as disk storage quotas or prohibitions against personal wireless networks (such as Apple Airport networks), if you impose such limits generally on your campus. Other computer-related issues that involve only specific, limited categories of users – rules governing access to student information databases, say – are best left to separate and more targeted policies.

[13] See <http://cio.osu.edu/policies/responsible_use.html>

Policy on Responsible Use of University Computing Resources at The Ohio State University

General Statement

Comment: Much as with a student code, a computer use policy can benefit from a brief introductory discussion of the institutional culture and values that underlie the policy's general approach and specific provisions. At Ohio State, we emphasized that we view this medium of communication as an important part of the "free exchange of ideas" and encourage its use for such purposes. We also took the opportunity to start off with a bit of education, noting that academic freedom involves both rights and *responsibilities, which are no different in this context than in any other.*

As a part of the physical and social learning infrastructure, The Ohio State University acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for university-related purposes, including direct and indirect support of the university's instruction, research, and service missions; of university administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the university community and between the university community and the wider local, national, and world communities.

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of university computing resources, like the use of any other university-provided resource and like any other university-related activity, is subject to the normal requirements of legal and ethical behavior within the university community. Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Applicability

Comment: To whom and what should the policy apply? We viewed this policy as the "baseline" policy applicable to all use and all users of university computers and networks, and we therefore defined applicability broadly. Other institutions may wish to have separate policies for different protocols (for example, e-mail versus web) or for different classes of users (for example, people with access to specific databases), but we felt that there are certain fundamentals that apply across all boards. We also noted, however, that there may be additional policies applicable only in specific contexts and to specific sets of users.

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the university or to uses within specific units. Consult the operators

or managers of the specific computer, computer system, or network in which you are interested or the management of the unit for further information.

Policy

All users of university computing resources must:

Comment: If there is one sentence that captures the entire essence of Ohio State's policy, the following one is it. Recognizing that its meaning would not be immediately obvious to most users, we elaborated at some length both here and in the "Virtual Legality" educational piece, to which we hyperlinked the web version of the policy (and a copy of which is reproduced at the end of this outline). Much of the rest of the policy is really just a further educational elaboration of this principle.

- **Comply with all federal, Ohio, and other applicable law; all generally applicable university rules and policies; and all applicable contracts and licenses.** Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the university's code of student conduct; the university's sexual harassment policy; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

Comment: Picking up on the last sentence of the prior section, and repeating a theme that appears throughout, we reiterated in the next two paragraphs that neither technical ability nor legal ignorance is a legitimate excuse for computer misconduct.

- **Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university.

- **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

Comment: Setting "speed limits" such as disk quotas or restrictions on bandwidth usage can be an important part of maintaining overall system efficiency and usability. (Among other things, such limits may have the effect of reducing the strain that file sharing can impose on a system.) Because the technology evolves and advances so rapidly, however, they can be quite difficult to

set. We chose to acknowledge the need for restraint but to set forth only a general principle, leaving the specifics for administrative determination and implementation.

- **Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.** Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of university computing resources, the university may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

Comment: One of the most important policy choices an institution must make in this context is whether to limit the use of its computing resources to "institutional" purposes or, rather, to tolerate personal use. This choice is particularly important for public institutions, which need not operate their systems as First Amendment "public forums," but which also must take care not to do so inadvertently. Of course, the line between what is and isn't "institution-related" is much fuzzier in a college or university than it is in, say, a law firm or corporation. A student viewing the Playboy web page, for example, may (possibly even legitimately) claim to be studying the human form for a drawing class or the objectification of women for a class on the politics of sexuality. Moreover, an absolute ban on personal use is essentially impossible to enforce and, according to at least some research, is actually likely to result in de*creased productivity. For these reasons, we, like many institutions, provided that we would permit "incidental" personal use within certain specified parameters. We elaborated on the parameters at some length in the F.A.Q., to which we hyperlinked the web version of the policy (and a copy of which follows).*

- **Refrain from using those resources for personal commercial purposes or for personal financial or other gain.** Personal use of university computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

Comment: Given the relatively common misperception that every single e-mail message that emanates from an institutional e-mail system is an official, authorized, and fully endorsed statement of that institution, and the equally common misperception that the Infinitely Wise and Powerful Persons who created the Internet wouldn't have made it so easy to "right click" and copy an image of a college mascot or logo into an e-mail message or onto a web page if it weren't permissible – even obligatory – to do so, we thought it appropriate to include a brief statement addressed to both constituencies. It is modeled, in part, on the concepts expressed in the AAUP's 1940 Statement of Principles on Academic Freedom and Tenure.

- **Refrain from stating or implying that they speak on behalf of the university and from using university trademarks and logos without authorization to do so.** Affiliation with the university does not, by itself, imply authorization to speak on behalf of the university. Authorization to use university trademarks and logos on university computing resources may

be granted only by the Office of University Communications or The Office of Trademarks and Licensing, as appropriate. The use of suitable disclaimers is encouraged.

Enforcement

Comment: Just as we already have generally applicable substantive rules that cover most of the misconduct that is committed by means of computers, we also have generally applicable procedural rules for dealing with that misconduct. IT staff can be endlessly helpful in figuring out the technical facts of the situation, but they typically are not trained to handle disciplinary proceedings, and it really is not their job to do so. Rather, as we stated here, computer misconduct complaints normally (barring an emergency) should be dealt with under the same judicial affairs and employee discipline processes as are applicable to students and employees generally. The fact that computers were involved in the misconduct is almost never dispositive or even particularly relevant, other than as background.

Users who violate this policy may be denied access to university computing resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Violations will normally be handled through the university disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Judicial Affairs. However, the university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

Comment: From a legal perspective, privacy is one of the most difficult issues to deal with when it comes to computers. People tend to have an intensely personal relationship with "their" computers, even when those computers were supplied by the institution and bear prominent institutional inventory tags. At the same time, because of the way computers and the Internet work, they can be an extraordinarily fruitful (and even frightening) source of information on what their users have been up to.

There is a body of generally applicable privacy law governing whether and when we can look at that information, but, simply put, it's a complete mess. It comes from a variety of different, usually complex, and often conflicting sources – the Fourth Amendment, the Electronic Communications Privacy Act, the common law of privacy, state freedom of information and public records statutes, and FERPA, to name just some – and it frequently hinges upon a case-by-case analysis of the users' "reasonable expectations of privacy" under "all of the facts and circumstances." Only the Supreme Court can tell for sure – and only because it gets the last word – whether you've made the right call in sorting all of that out.

Fortunately, what expectations are reasonable can be established by express policy, and consent is always a defense to any claim of invasion of privacy. Thus, it is possible to bypass this mess by creating your own privacy policy – in effect, your own private law of privacy – and making

use of your system subject to it. From a legal standpoint, that policy can fall pretty much anywhere in the range from absolute privacy to no privacy whatever,[14] as long as it is clear and your users have notice of it (and, of course, you follow it once it's in place).

At Ohio State, we chose a middle ground, creating a system that is similar to, though much simpler than, the Fourth Amendment search warrant process. The system consists of two basic elements: First, recognizing that our users have a legitimate desire *for privacy (particularly because we do allow incidental personal use) and that we normally have no need to compromise that desire, we set forth a list of the reasons we considered legitimate for "looking." The list is reasonably broad, but it certainly is not open-ended and does not include mere curiosity. Second, we provided that the only person who could authorize "looking" was our CIO or someone designated by the CIO. The idea was not to limit the authority to a single person; we anticipated that at least each college within the university would eventually have a designee, though no one ever asked for one, and the sole designee remains the CIO's policy advisor. What we wanted to make clear, however, was that no one had the inherent authority to "look" simply by virtue of position or technical ability. As is explained in greater detail in the F.A.Q., we also wanted to ensure that the designees would be people with appreciation for privacy issues and that the policy would be applied consistently across campus.*

One question that arose almost immediately was whether the restriction on "monitoring" prohibited a supervisor or co-worker from accessing an employee's computer files for noninvestigatory, work-related purposes. In accordance with our "constitutional" approach, we dealt with that not in the policy itself, but by including a discussion in the F.A.Q.

The university employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the university cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should also be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The university may also specifically monitor the activity and accounts of individual users of university computing resources, including individual login sessions and communications, without notice, when (a) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this policy; (d) an account appears to be engaged in unusual or unusually excessive

[14] For an example of a university policy following the latter approach, which certainly is easy to administer, see U.S. v. Angevine, 281 F.3d 1130 (10th Cir. 2002).

activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring, other than that specified in "(a)," required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designees.

The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings. Communications made by means of university computing resources are also generally subject to Ohio's Public Records Statute to the same extent as they would be if made on paper**.**

Frequently Asked Questions
about the
Policy on Responsible Use of University Computing Resources

Why doesn't the policy prohibit <u>all</u> personal use of university computing resources? Why doesn't the policy permit <u>unrestricted</u> personal use of university computing resources?

The general guiding principle behind the policy is that "cyberspace is not a separate legal jurisdiction"; that existing, generally applicable laws, rules, and policies therefore already apply equally to the use of university computing resources; and that new rules and policies are therefore necessary only in those rare instances when the use of university computing resources implicates unique new issues. In accordance with that principle, the provisions concerning personal use of university computing resources are intended to mirror existing policies and practices concerning personal use of other university resources. Thus, the policy provides that university-provided computing resources, like university-provided telephones, typewriters, photocopiers, stationery, office supplies, tools, and so forth, are provided for "university-related purposes."

Use of such resources for personal commercial purposes or for personal financial or other gain is clearly improper and, under some circumstances, may be illegal. Recognizing, however, the difficulty of drawing a bright line between other types of personal uses and "university-related" uses, the minimal costs typically associated with occasional personal use, the typically inordinate costs associated with attempting to enforce a flat prohibition, and the benefits that may accrue to the university from increased experience and familiarity of its users with available computing resources, the policy also provides that "incidental" personal use of university computing resources is, in general, permitted – just as it typically is with other types of university resources. "Incidental" uses of university computing resources are defined as uses that do not consume a significant amount of those resources, do not interfere with the performance of the user's job or other university responsibilities, are not made for personal commercial purposes or for personal financial or other gain, and are otherwise in compliance with applicable laws, rules, policies, contracts, and licenses.

Also recognizing, however, that circumstances vary among the different administrative units of the university, the personal use provisions of the policy are set forth simply as a "default" rule. The policy expressly provides that further limits may be imposed upon personal use in accordance with normal supervisory procedures. Thus, individual administrative units of the university may, if they deem it appropriate, impose additional use restrictions on, or prohibit all personal use of, the university-provided computing resources under their control.

Does the restriction on use of university computing resources for personal commercial purposes or personal financial or other gain prohibit faculty from using such resources in connection with their consulting work?

Faculty use of university resources, including university computing resources, is governed by the university's Policy on Paid External Consulting, which recognizes that appropriate professional service by faculty outside the university is both part of the university's mission and is of benefit to the university as well. Accordingly, use of university computing resources in connection with such consulting is not considered "personal" in the sense intended by the Policy on Responsible Use of University Computing Resources and is therefore not within the scope of the prohibition.

In accordance with the Policy on Paid External Consulting, however, the use of university resources in connection with consulting work, and the consulting work itself, must be approved, in advance, by the relevant department chair and dean, and arrangements must be made to compensate the university if the use of its resources will be significant. Use of university computing resources in connection with consulting that has not been approved in accordance with this procedure is prohibited.

In short, the use of university computing resources in connection with consulting work is subject to the same requirements and limitations as is the use of any other university resources in connection with consulting work.

Why must monitoring be authorized by the Chief Information Officer or designee? When and how may a designee be appointed?

The purpose of the advance authorization provision of the policy is to make clear that authority to engage in investigatory monitoring of university computing resources is not implied or inherent in any job position, to ensure consistency in the development and application of the standards for monitoring, and to enable the university to monitor the effectiveness of the policy itself, not to require that all authorizations be made by a single person. It is expected that most major administrative units within the university will want and will have their own designees.

Vice Presidents, Deans, and Directors may request the Chief Information Officer to designate a specified individual to handle authorization requests within their respective administrative units. Designees should be familiar both with the technology and with general university policy and procedures, but ordinarily should not be technical staff members who would conduct or supervise any monitoring that is authorized or persons who would be responsible for the determination or imposition of any disciplinary action that may result. Designees will be expected to report and be responsible to the Chief Information Officer concerning their activities as designees.

Does the restriction on individualized monitoring prohibit a supervisor or co-worker from accessing an employee's computer files for work-related purposes?

The policy's provisions on monitoring govern only the monitoring and investigation of actual or suspected misconduct or misuse of university computing resources, not the ordinary, everyday functioning of an office. Thus, for example, to the extent that a PC or network server serves as the functional equivalent of a desk drawer or file cabinet, supervisors and co-workers continue to have the same access to it for normal, noninvestigatory, work-related purposes – for example, to retrieve a file or document needed while the employee who maintains the file or document is away from the office – as they always have. Obtaining such access is not considered "monitoring" for purposes of the policy and does not require the advance authorization of the Chief Information Officer or designee.

If, however, a supervisor or co-worker discovers evidence of possible misconduct or misuse while accessing university computing resources under the control of another for normal, noninvestigatory, work-related purposes, further monitoring or investigation of those computing resources for purposes of dealing with the suspected misconduct or misuse does require the advance authorization of the Chief Information Officer or designee, unless the monitoring is required by law or is necessary to respond to perceived emergency situations. Evidence discovered in the course of normal, noninvestigatory, work-related activity may be used as a basis for seeking such authorization.

Does the policy prohibit "spam"?

The problem of "spam" is an extraordinarily complicated one. Few people would agree on a definition of exactly what constitutes "spam"; technical restrictions against it are therefore necessarily imprecise, as well as easily evaded; and the university's legal ability to deal with that indefinable and technically insoluble problem is further complicated by the university's status as a public institution subject to the restrictions of the First Amendment. For all of these reasons, the policy does not prohibit "spam" per se.

The policy does, however, prohibit the use of university computing resources for personal commercial purposes or for personal financial or other gain, and it also prohibits uses that consume an unreasonable quantity of those resources or that unreasonably interfere with the activity of other users. Most of what most people consider to be "spam" falls within either or both of these categories and thus is prohibited by the policy. In addition, "spammers" who refuse to honor a recipient's request to be removed from the "spammers'" mailing lists are engaged in what the university considers to be harassment. Under any of these circumstances, the university may attempt to block further incoming messages from persons outside the university who engage in such activities and may restrict or terminate the computing privileges of persons inside the university who engage in such activities. In addition, University Technology Services can assist individual members of the university community in establishing individual mechanisms to filter out "spam."

What "additional policies" may individual administrative units adopt for the computing resources under their control?

The policy is intended to serve both as an "umbrella" policy and as a "threshold" policy applicable to all university computing resources. It is expected that many units will find that no further policies are necessary. Individual administrative units may, however, supplement the policy with additional, complementary rules for the computing resources under their control, but they may not "lower the threshold" or override the policy. Thus, for example, an individual administrative unit may impose additional restrictions on personal use appropriate for that unit or address other, unit-specific issues not covered by the policy, but may not authorize the use of its computing resources for personal commercial gain or authorize individual monitoring in the absence of the required designation by the CIO.

VIRTUAL LEGALITY
An Overview of Your Rights and Responsibilities in Cyberspace*

Steven J. McDonald
Associate Legal Counsel
The Ohio State University

The Internet is a powerful and revolutionary tool for communication – powerful in its ability to reach a global audience and revolutionary in its accessibility to those who formerly were only at the receiving end of mass communications. With access to the Internet, *anyone* – even a preschool child – can now effectively be an international publisher and broadcaster. By posting to Usenet or establishing a web page, for example, an Internet user can speak to a larger and wider audience than does the New York Times, NBC, or National Public Radio. Many Internet users, however, do not realize that that is what they are doing.

Not surprisingly, given these facts, the Internet also has a powerful and revolutionary potential for misuse. Such misuse is particularly prevalent on college and university campuses, where free *access* to computing resources is often mistakenly thought to be the equivalent of free *speech*, and where free speech rights are in turn often mistakenly thought to include the right to do whatever is technically possible.

The rights of academic freedom and freedom of expression *do* apply to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with those rights. Thus, legitimate use of university computing resources does *not* extend to whatever is technically possible. In addition, while some restrictions are built into the university's computer operating systems and networks, those restrictions are not the only restrictions on what is permissible. Users of university computing resources must abide by *all* applicable restrictions, *whether or not* they are built into the operating system or network and *whether or not* they can be circumvented by technical means. Moreover, it is not the responsibility of the university to prevent computer users from exceeding those restrictions; rather, it is the computer user's responsibility to know and comply with them. When you're pulled over to the side of the Information Superhighway, "I'm sorry officer – I didn't realize I was over the speed limit" is *not* a valid defense.

So just what *are* the applicable restrictions? The same laws and policies that apply in every other context. "Cyberspace" is not a separate legal jurisdiction, and it is not exempt from the normal requirements of legal and ethical behavior within the university community. **A good rule of thumb to keep in mind is that conduct that would be illegal or a violation of university policy in the "offline" world will still be illegal or a violation of university policy when it occurs online.** Remember, too, that the online world is not limited to The Ohio State University, to the State of Ohio, or even to the United States. **Computer users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks.**

It is impossible to list and describe every law and policy that applies to the use of university computing resources and the Internet – since, by and large, they all do – but the following are some of the ones that most frequently cause problems:

* The resolution of specific legal issues requires an analysis of all the facts and circumstances; the general guidelines in this document do not constitute, and should not be relied upon as, specific legal advice.

Copyright

Copyright law generally gives authors, artists, composers, and other such creators the *exclusive* right to copy, distribute, modify, and display their works or to authorize other people to do so. Moreover, their works are protected by copyright law from the very moment that they are created – *regardless* of whether they are registered with the Copyright Office and *regardless* of whether they are marked with a copyright notice or symbol (©). That means that virtually every e-mail message, Usenet posting, web page, or other computer work you have ever created – or seen – is copyrighted. That also means that, if you are not the copyright owner of a particular e-mail message, Usenet posting, web page, or other computer work, you *may not* copy, distribute, modify, or display it *unless:*

- Its copyright owner has given you permission to do so; *or*
- It is in the "public domain"; *or*
- Doing so would constitute "fair use"; *or*
- You have an "implied license" to do so.

If none of these exceptions applies, your use of the work constitutes copyright infringement, and you could be liable for as much as $150,000 in damages for *each* use. In addition, if you reproduce or distribute copies of a copyrighted work having a total retail value of at least $1,000 (which could include, for example, posting a $50 software program on a web page or newsgroup from which it is downloaded 20 times), your actions may also be *criminal* – even if you do it for free.

It's usually easy to tell whether you have permission to make a particular use of a work – the copyright owner will have told you so expressly, either in writing or orally – but it's not always so easy to tell whether the work is in the public domain or whether what you want to do constitutes fair use or is covered by an implied license.

Placing a work on the Internet is *not* the same thing as granting that work to the public domain. Generally speaking, a work found on the Internet, like a work found anywhere else, is in the public domain only if (a) its creator has *expressly* disclaimed any copyright interest in the work, *or* (b) it was created by the federal government, *or* (c) it is very old. Unfortunately, just *how* old a particular work must be to be in the public domain depends in part upon when the work was created, in part upon whether and when it was formally published, in part upon whether and when its creator died, and in part on still other factors, so there is no one specific cutoff date that you can use for all works to determine whether or not they are in the public domain. As a rule of thumb, however, works that were created *and published* before 1923 are now in the public domain. Works that were created in or after 1923, works that were created before 1923 but published in or after 1923, and works that have never been published *might* be in the public domain, but, if you don't know for sure, it's best to assume that they are not.

In very general terms, a particular use of a work is "fair" if it involves only a relatively small portion of the work, is for educational or other noncommercial purposes, and is unlikely to interfere with the copyright owner's ability to market the original work. A classic example is quoting a few sentences or paragraphs of a book in a class paper. Other uses may also be fair, but it is *almost never* fair to use an entire work, and it is *not* enough that you aren't charging anyone for your particular use. It also is not enough simply to cite your source (though it may be plagiarism if you don't).

An implied license may exist if the copyright owner has acted in such a way that it is reasonable for you to assume that you may make a particular use. For example, if you are the moderator of a mailing list and someone sends you a message for that list, it's reasonable to assume that you may post the message to the list, even if its author didn't expressly say that you may do so. The copyright owner can always "revoke" an

implied license, however, simply by saying that further use is prohibited.

In addition, facts and ideas *cannot* be copyrighted. Copyright law protects only the *expression* of the creator's idea – the specific words or notes or brushstrokes or computer code that the creator used – and not the underlying idea itself. Thus, for example, it is not copyright infringement to state in a history paper that the Declaration of Independence was actually signed on August 2, 1776, or to argue in an English paper that Francis Bacon is the real author of Shakespeare's plays, even though someone else has already done so, as long as you use your own words. (Again, however, if you don't cite your sources, it may still be plagiarism even if you paraphrase.)

Exactly how copyright law applies to the Internet is still not entirely clear, but there are some rules of thumb:

- You *may* look at another person's web page, even though your computer makes a temporary copy when you do so, but you *may not* redistribute it or incorporate it into your own web page without permission, except as fair use may allow.

- You *probably may* quote all or part of another person's Usenet or listserv message in your response to that message, unless the original message says that copying is prohibited.

- You *probably may not* copy and redistribute a private e-mail message you have received without the author's permission, except as fair use may allow.

- You *probably may* print out a single copy of a web page or of a Usenet, listserv, or private e-mail message for your own, personal, noncommercial use.

- You *may not* post another person's book, article, graphic, image, music, or other such material on your web page or use them in your Usenet, listserv, or private e-mail messages without permission, except as fair use may allow.

- You *may not* download materials from Lexis-Nexis, the Clarinet news service, or other such services and copy or redistribute them without permission, unless the applicable license agreement expressly permits you to do so or unless your particular use would constitute fair use.

- You *may not* copy or redistribute software without permission, unless the applicable license agreement expressly permits you to do so.

Libel

Libel is the "publication" of a false statement of fact that harms another person's reputation – for example, saying that "John beat up his roommate" or "Mary is a thief" if it isn't true. If a statement doesn't harm the other person's reputation – for example, "Joe got an 'A' on the test" – it's not libel even if it's false. In addition, a statement of *pure* opinion cannot be libelous – for example, "I don't like John" – but you can't turn a statement of fact into an opinion simply by adding "I think" or "in my opinion" to it. "IMHO, John beat up his roommate" is still libelous if John didn't beat up his roommate. If you honestly believed that what you said was true, however, you *might* not be liable if it later turns out that you were wrong.

A libel is "published" whenever it is communicated to a third person. In other words, if you say "Mary is a thief" to anyone other than Mary, you have "published" that libel. That means that almost anything you post or send on the Internet, except an e-mail that you send only to the person about whom you are talking, is "published" for purposes of libel law.

A person who has been libeled can sue for whatever damages are caused by the publication of the libel. Since a libel on the Internet could potentially reach millions of people, the damages could be quite large.

A good rule of thumb to follow: If you would be upset if someone else made the same statement about you, think carefully before you send or post that statement to the Internet, because it might be libelous.

Invasion of Privacy

There are a number of different laws that protect the "right to privacy" in a number of different ways. For example, under the Electronic Communications Privacy Act, a federal statute, it generally is a *crime* to intercept someone else's private e-mail message or to look into someone else's private computer account without appropriate authorization. The fact that you may have the technical ability to do so, or that the other person may not have properly safeguarded his or her account, does *not* mean that you have authorization. If you don't know for sure whether you have authorization, you probably don't.

Invasion of privacy, like libel, is also a "tort," which means that you can also be sued for monetary damages. In addition to the sorts of things prohibited by the Electronic Communications Privacy Act, it can be an invasion of privacy to disclose intensely personal information about another person that that person has chosen not to make public and that the public has no legitimate need or reason to know – for example, the fact that someone has AIDS, if he or she has not revealed that information publicly. Unlike with libel, a statement can be an invasion of privacy even if it is true.

Obscenity, Child Pornography and "Indecency"

Under both state and federal law, it is a *crime* to publish, sell, distribute, display, or, in some cases, merely to possess obscene materials or child pornography. These laws also apply equally to the Internet, and a number of people have been prosecuted and convicted for violating them in that context.

The line between what is obscene and what is not is hard to draw with any precision – as one Supreme Court Justice said, "I could never succeed in intelligibly" defining obscenity, "[b]ut I know it when I see it" – but the term basically means hard-core pornography that has no literary, artistic, political, or other socially redeeming value. One reason that it is so hard to define obscenity is that it depends in part on local community standards; what is considered obscene in one community may not be considered obscene in another. That makes it particularly difficult to determine whether materials on the Internet are obscene, since such materials are, in a sense, everywhere, and it is therefore not enough that the materials are legal wherever *you* are. In one case, the operators of a bulletin board service in California posted materials that were not considered obscene there, but were convicted of violating the obscenity statutes in Tennessee when the materials were downloaded there.

Child pornography is the visual depiction of minors engaged in sexually explicit activity. Unlike obscenity, child pornography is illegal *regardless* of whether it has any literary, artistic, political, or other socially redeeming value.

Sexually oriented materials that do not constitute either obscenity or child pornography *generally* are legal. Still, it is illegal in most cases to provide such materials to minors, and displaying or sending such materials to people who do not wish to see

them may be a violation of the university's Sexual Harassment Policy.

"Hacking," "Cracking" and Similar Activities

Under the federal Computer Fraud and Abuse Act, and under a variety of similar other state and federal statutes, it can also be a *crime* to access or use a computer without authorization, to alter data in a computer without authorization, to transmit computer viruses and "worms" over computer networks, to conduct "e-mail bombing," and to engage in other such activities. Engaging in such activities can also make you liable for monetary damages to any person who is harmed by your activities. Again, the fact that you may have the technical ability to do any of these things, or that another computer owner may not have properly safeguarded his or her computer, does *not* mean that you have authorization. If you don't know for sure whether you have authorization, you probably don't.

University Policies

Use of university computing resources is also subject to the university's Code of Student Conduct, the university's Policy on Academic Misconduct, the university's Sexual Harassment Policy, and all other generally applicable university policies. In addition, the following prohibitions apply specifically to the use of university computing resources:

- University computer accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university – even family and friends. Users are responsible for all use of their accounts.

- Users must limit their use of university computing resources so as not to consume an unreasonable amount of those resources or to interfere with the activity of other users.

- University computing resources are intended for university-related use and therefore may not be used for personal commercial or business purposes or for other personal gain. Personal use of university computing resources for *other* purposes will generally be permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other university responsibilities, and is otherwise in compliance with university policies.

- Users of university computing resources may not state or imply that they are speaking on behalf of the university and may not use university trademarks and logos in connection with their use of those resources without specific authorization to do so.

For Further Information

If you have questions about the legality of your use of university computing resources, it's best to ask before proceeding. You can get general advice (but not specific legal advice) from your UVC advisor, from any of the computer lab site managers, or from the UTS Technology Support Center (688-HELP).

In addition, you can find more information on these and related topics at the following web sites:

- Cyberspace Law for Non-Lawyers
- 10 Big Myths About Copyright Explained
- "Copying is Theft," and Other Legal Myths in the Looming Battle over Peer-to-Peer