TRADING CYBERSPACES:
A P/REVIEW OF THE SEASON IN CYBERLAW

27th Annual National Conference on Law and Higher Education
Stetson University College of Law

Steven J. McDonald
General Counsel
Rhode Island School of Design

It's been a momentous year in cyberlaw, with the promise (threat?) of much more still to come. Perhaps the greatest dramas on the "networks" this past year involved both those who make and distribute file sharing software and file sharing itself. It was a very bad year for the former, but, except in a small handful of instances, not so bad for the latter, as the law began, finally, to sort itself out in fairly clear, if not very enforceable, ways. Google's forays into the realm of publishing are developing into an "epic" worthy of the "sweeps". And the constant stream of new technologies continues to bewitch our students with new, often "unrated" opportunities for misconduct, bother the targets of that misconduct, and bewilder those of us who must deal with it.

Let's tune in and take a look:

I. The Biggest Loser: Grokster *and* Survivor: File Sharing

The issue of file sharing began its meteoric rise to the top of the ratings in 1999, when Northeastern University freshman Shawn Fanning first unleashed Napster upon the world. A software program that, for the first time, enabled computer users to share music with one another easily over the Internet, Napster quickly attracted the attention of college and university students, who had ready access to the substantial bandwidth required to operate the program; of college and university information technology offices, which saw their available bandwidth disappear virtually overnight; of the music industry, which (with considerable justification) feared lost sales and revenues – and, of course, of the lawyers, for whom copyright law, previously a sleepy backwater of the profession, soon became the Next New Thing.

Before long, the music industry and its lawyers succeeded in shutting down Napster *the company*, but Napster *the idea* proved to be a more elusive target. Almost as quickly as the first lawsuits were filed, numerous clones and variations of the Napster software appeared. These new programs exhibited an almost viral ability to replicate, to hide deep within the Internet while they gained strength, and to adapt themselves to the interstices of the various lower court rulings.

This past June, however, the Supreme Court largely settled the issue once and for all. In Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., 125 S. Ct. 2764 (2005), the Court *unanimously* held that a company that distributes a product or device capable of both noninfringing and infringing uses, and that not only knows that some of its customers will engage in infringement but also actively and "intentionally induces" them to do so, is contributorily liable for the resulting infringements. Under this standard, there was no real question but that Grokster and other producers of file sharing software, whose entire business models were expressly built on promoting and profiting from infringement by their users, were liable, and virtually all of them quickly shut down – at least at the *corporate* level.

While the "cancellation" of Grokster was not terribly surprising, it left open a significant, unresolved "cliffhanger": Where, between Grokster and more mainstream products and devices, does the liability line fall? Grokster could not have existed without computers and the Internet; should computer makers and Internet service providers therefore also be held liable? What about Apple Computer, whose initial advertising slogan for its popular iTunes software was "Rip. Mix. Burn."? Must the makers of digital cameras and digital video recorders – or even of VCRs and photocopiers – go into hiding? The Supreme Court noted only – and unhelpfully – that its holding was intended to "limi[t] liability to instances of more acute fault than the mere understanding that some of one's products will be misused", 125 S. Ct. at 2778, but its unanimity on this point then fractured into strong disagreement over what it actually meant.

Fortunately, the first case to apply the Grokster standard, Monotype Imaging, Inc. v. Bitstream Inc., 376 F. Supp. 2d 877 (N.D. Ill. 2005), suggests that the courts will take

a fairly common sense approach – or, at least, that discretion (on the part of potential defendants) remains the better part of valor. In that case, Monotype, the maker of font-generating software and owner of hundreds of copyrighted fonts, sued Bitstream, a competitor whose "TrueDoc" software allows the recipient of a document to view the fonts in the document even if they are not installed on the recipient's computer. The software works with all fonts, not just those created and owned by Bitstream. Moreover, Bitstream noted that fact in its advertising and undoubtedly must have known that some of its customers would use TrueDoc with unlicensed fonts. Nevertheless, the court held that Bitstream could not be held contributorily liable for any such infringements:

> Here, the most that Plaintiffs can point to are Bitstream's repeated advertisements that its TrueDoc software could be used with any fonts and did not infringe upon intellectual property rights. As several Bitstream witnesses credibly explained, however, the statement that the software could be used with any fonts referred to the fact that it could work with both Bitstream fonts, as well as fonts from other font distributors that had authorized the use of their fonts with TrueDoc. This differs substantially from the situation in Grokster where the defendants specifically targeted an audience that was seeking to download copyrighted material. Further, unlike in Grokster, here . . . Bitstream submitted evidence that it had taken steps to avoid the use of its TrueDoc with protected fonts of other companies. Lastly, unlike in Grokster, there is no evidence in the record to show that Bitstream's business was benefited by increasing the number of infringing uses of TrueDoc. Instead, the record shows that it was not in Bitstream's business interests to increase any infringement of other parties' fonts using TrueDoc. Rather, by distributing TrueDoc along with Bitstream's own fonts, Bitstream sought to increase sales of its fonts. Accordingly, there is no evidence in the record that supports that Bitstream acted with the requisite intent to make it liable under Grokster's intentional inducement of infringement cause of action.

Id. at 889.

While the legality of the actual *use* of file sharing software was not directly at issue in Grokster, the Court nevertheless expressed its opinion – quite clearly – both that "the vast majority of users' downloads are acts of infringement" and that the scope of such infringement is "staggering". 125 S. Ct. at 2772. Perhaps energized by this restatement of the obvious, the RIAA has since pursued its campaign against individual users with new vigor.

But while the RIAA has now filed lawsuits against more than 17,000 individual users, and has obtained several thousand settlements averaging $3,000 to $5,000, file sharing itself shows no signs of abating. In fact, by some estimates, file sharing traffic has doubled and the number of file sharers has nearly tripled in the two and a half years since the RIAA filed its first complaint. Electronic Frontier Foundation, RIAA v. The People (2005), available at <http://www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf>. Moreover, a small handful of the defendants in those cases are beginning to fight back.

BMG Music v. Gonzalez, 2005 U.S. Dist. Lexis 910 (N.D. Ill.), the first of the RIAA's cases to be litigated to judgment, strongly suggests that those defendants will not fare well. Defendant Cecilia Gonzalez, who admitted to having downloaded 30 songs, argued that doing so was "fair use", on the theory that she was "just sampling" music before deciding whether to purchase it, and that, in any event, she was an "innocent" infringer because she did not know that what she did was illegal. Unimpressed, the court granted summary judgment against her, holding that her fair use argument was "without merit" and that "ignorance is no defense to the law".[1] Id. at

[1] The desires of the music industry notwithstanding, however, fair use does have some application to "file sharing", broadly conceived. At this point, it generally is accepted – and rarely disputed even by the music industry – that making a copy of a song or CD that you already legitimately own, for your own personal use on your own MP3 player or computer, is a fair use and therefore not copyright infringement. Thus, to the extent that file-sharing software is used simply to effect such "space shifting", it raises few legal concerns. See, e.g., Recording Industry Ass'n of America v. Diamond Multimedia Systems, 180 F.3d 1072, 1079 (9th Cir. 1999) (copying one's own music to one's own MP3 player "is paradigmatic noncommercial personal use entirely consistent with the purposes of the [Copyright] Act"). See also In re Aimster Copyright Infringement Litigation, 334 F.3d 643, 652-53 (7th Cir. 2003), cert. denied sub. nom. Deep v. Recording Industry Ass'n of America, 540 U.S. 1107 (2004) (discussing with approval, though not expressly ruling upon, the "space shifting" rationale). In addition, under the "first sale" doctrine, it also is permissible to share a song or CD that you

*3 and *5. The court then proceeded to award damages in the amount of $22,500, the *minimum* statutory penalty of $750 per infringement multiplied by 30. (Looked at from another angle, that amount also represented approximately 500 times the cost of the roughly three CD's worth of songs she had downloaded – or more than three-fourths of her entire annual salary as a secretary before she was laid off, possibly as a result of her involvement in the case. See Bob Mehr, "Gnat, Meet Cannon", Chicago Reader, Feb. 4, 2005, available at <http://www.chicagoreader.com/TheMeter/050204.html>.) Her arguments fared even less well on appeal:

> Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying "fair use" if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute. Nor can she defend by observing that other persons were greater offenders; Gonzalez's theme that she obtained "only 30" . . . copyrighted songs is no more relevant than a thief's contention that he shoplifted "only 30" compact discs, planning to listen to them at home and pay later for any he liked.

2005 U.S. App. Lexis 26903 at *7-*8 (7th Cir.).

Other defendants are fighting back on other grounds, claiming misidentification or asserting antitrust, racketeering, and other counterclaims. See, generally, Ty Rogers and Ray Beckerman, Recording Industry vs. The People Blog, available online at <recordingindustryvspeople.blogspot.com>. Such approaches seem no more likely to succeed, however, and at least one of the cases should be filed under "be careful what you wish for". When Candy Chan was able to demonstrate that she was not responsible for the file sharing that had occurred on her computer, the recording industry dismissed its lawsuit against her only to refile it against her 14-year-old daughter. Id.

Stay tuned for next season's File Sharing SmackDown!

---

legitimately own by transferring physical possession of it (not a copy) to a friend, either

II. Who Wants to be a Millionaire?: Other Intellectual Property Developments

Three current copyright lawsuits involving Google could dramatically reshape the law of copyright as it applies to the Internet. In Agence France Presse v. Google, Inc., a case pending in the United States District Court for the District of Columbia, an international news agency is challenging Google News, a service that aggregates headlines, story leads, and photographs from online news services into a searchable index and provides links to the original source. In Perfect 10, Inc. v. Google, Inc., a case pending in the United States District Court for the Central District of California, a publisher of "adult" material is challenging the inclusion of its photographs in Google's Image Search, which indexes images on the web and shows thumbnails as a link to the original. And in Authors Guild v. Google, Inc., a case pending in the United States District Court for the Southern District of New York, a professional writers' organization and several individual authors have filed a class action against Google's Library Project, in which Google is attempting to digitize and make searchable the entire contents of several of the world's largest and most "storied" libraries, including those at Harvard, Stanford, and Oxford Universities, the University of Michigan, and the New York Public Library.

In each of these cases, Google is, unquestionably, reproducing and distributing copyrighted material without the express consent of the copyright owner. On the other hand, what Google is making available to the public in each of these cases is limited to snippets of the original written material and small, low-resolution copies of the original images, together with links to the originals (when they are already on the web elsewhere) or bibliographic information and links to online booksellers and libraries (when they are not). The ultimate question, then, is whether Google's actions qualify as fair use – a question for which there is for now no "final answer", let alone a lifeline or phone-a-friend.

Google would seem to have some strong arguments in its favor under the traditional fair use test. While it is a commercial enterprise (and a highly successful one at that), its uses of others' material is unquestionably "transformative", in that it is using

---

temporarily or permanently. 17 U.S.C. § 109(a).

those materials not for their original purposes, but, rather, to create an index "to organize the world's information and make it universally accessible and useful". Google Mission Statement, available at <http://www.google.com/intl/en/corporate/index.html>. Google does make complete copies of the works in its index, so that its index itself will be complete, but it does not provide those copies to the users of its search engine. Moreover, it seems highly unlikely that Google will displace sales of the original materials; indeed, if anything, it seems most likely to *increase* them, by increasing public awareness of them. See, generally, Kelly v. Arriba Soft Corp., 336 F.3d 811, 819 (9th Cir. 2003) ("This case involves more than merely a retransmission of Kelly's images in a different medium. Arriba's use of the images serves a different function than Kelly's use – improving access to information on the internet versus artistic expression. Furthermore, it would be unlikely that anyone would use Arriba's thumbnails for illustrative or aesthetic purposes because enlarging them sacrifices their clarity. Because Arriba's use is not superseding Kelly's use but, rather, has created a different purpose for the images, Arriba's use is transformative."). Still, a finding in Google's favor would deprive copyright holders of the potentially lucrative opportunity to try to license their materials to Google (and others like it) for such uses.

In the end, however, the decision in each of these cases is likely to turn on the courts' views as to whether what Google is doing is, on balance, an overall social good, rather than on a methodical analysis of the technical fair use factors. (Which, to be fair, would not distinguish these cases from many other fair use cases. The factors are highly malleable, and they frequently are used as the justification for an outcome rather than the means of reaching it.) That question may not be as easy as it seems, but the answer to it could well have far-reaching implications for the future shape of the Internet.

III. Temptation Island: Blogs, Facebook, and Other New Tools for Misconduct

For those of us 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,[2] dealing

[2] 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 may count themselves among this group.

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, Facebook, 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[3] or splintered into hodgepodges of individual policies specific to the web,[4] e-mail,[5] spam,[6] file sharing,[7] blogs,[8] and more.[9]

---

[3] See, e.g., Seattle University Computer Acceptable Use Policy, <http://www.seattleu.edu/it/policies/cupolicy.asp>.

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

[5] See, e.g., University of Texas System Administration Electronic Mail Policy, <http://www.utsystem.edu/utsysadminemailpolicy.htm>.

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

[7] See, e.g., Asuza Pacific Peer-to-Peer File Sharing Policy, <http://www.apu.edu/imt/policies/p2p.php>.

[8] See, e.g., Weblogs at Harvard Law, <http://blogs.law.harvard.edu/terms>; Williamette University Web Log Policy and Service Guidelines, <http://blog.willamette.edu/blog-policy.html>.

[9] 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>.

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.[10]

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!

---

[10] In the apt 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").

Your existing, generally applicable sexual harassment policy and (quite likely) your general code of student conduct already prohibit sexual harassment *regardless* of the means by which it is committed. Just as you unquestionably can address sexual harassment committed by means of a typewriter without a typewriter use policy,[11] you can address e-mail sexual harassment whether your computer use or e-mail policy references the subject or not – and, 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 is 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.

[11] 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.

So, do we need to constantly update our computer use (or e-mail, or file sharing, or blog, or . . .) policies 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 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. An example of one way of doing so is attached as Appendix A.)

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.[12]

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

[12] See, e.g., Pichelmann v. Madsen, 31 Fed. Appx. 322 (7th Cir. 2002) (even if university's e-mail system were 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); Faculty Rights Coalition v. de Mino, 2005 U.S. Dist. Lexis 16227 (S.D. Tex.) (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); 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).

unique to computer use, of which there are very few.[13] 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.

In short, don't worry (about computer technology), be happy.

[13] 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.

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