AN OVERVIEW OF INTERNET LAW

Presenter:

STEVEN J. McDONALD
Associate Legal Counsel
The Ohio State University
Columbus, Ohio

Stetson University College of Law:

WORKSHOP: "VIRTUAL LEGALITY" Campus Electronic Communications Law and Policy
Clearwater Beach, Florida
February 16, 1997
AN OVERVIEW OF INTERNET LAW*

Steven J. McDonald
Associate Legal Counsel
The Ohio State University

I. Introduction

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. Not surprisingly, given these facts, the Internet also has a powerful and revolutionary potential for misuse. Judging from the pages of the Chronicle of Higher Education and other publications, such misuse is particularly prevalent on our campuses, where free access is often mistakenly thought to be the equivalent of "free speech," and where "free speech" is in turn often mistakenly thought to be defined by that which is technically possible. This outline addresses two legal questions that arise out of this situation: what are our responsibilities and liabilities, as service providers, when our systems are misused, and just what are the rules of the road of the Information Superhighway in the first place?

In seeking to answer the first of these questions, the most important thing to remember is that, while the Internet itself is new, it is, in this respect, still just another means of distributing information. This same question has arisen with every new communications medium, and a reasonably well-defined set of legal principles has evolved. There is little reason to believe that those principles are, or should be, any different in the Internet context.

In seeking to answer the second of these questions, the most important thing to remember is that the Internet is merely a tool. While having access to that tool may significantly multiply the opportunities for misbehavior, the source of the problem is the user who misuses the tool, not the tool itself. For this reason, Internet misuse raises few, if any, new legal issues and requires few, if any, new rules. The same laws and policies that apply to Internet users in other contexts can and do apply to them when they are "in" cyberspace. While it is impossible to catalog every area of the law that may conceivably apply in the Internet context -- which is to say every area of the law -- several of the most important and most frequently arising are discussed below.

II. General Standard of Liability for Internet Service Providers

Internet service providers have, quite quickly, become an indispensable part of the "free flow of information", though, at first glance, their role is not entirely clear. Unlike the traditional media, which generally disseminate their own message, and unlike mail and telephone services, which typically act as common carriers for the messages of others, Internet service providers both serve as a conduit for information created by others and deliver information of their own devising -- they are both medium and messenger. What, then, is their legal status for purposes of the libel, obscenities, invasions of privacy and other such misuses committed on their systems?

Traditionally, the standard of liability for such "publication torts" has depended largely upon the degree of editorial control and sponsorship that the defendant assumed and exercised over the publication that was the basis of a claim. The person or entity with the most responsibility was

* Portions of this outline are based on materials that I originally prepared for the General Counsel of CompuServe Incorporated in 1994. I wish to thank CompuServe for its permission to incorporate those materials into this outline.
the primary publisher, who created the relevant publication and put it out under the publisher's own name -- for example, a newspaper or television station reporting on a local matter. At common law, lack of knowledge and lack of fault were irrelevant; a publisher was typically strictly liable if its publication was false or obscene. See Bruce Sanford, Libel and Privacy § 8.2 (2d ed. 1993). (For a discussion of the constitutional abolishment of this doctrine, see § III(A), below.)

Distributors of the relevant publication that had no involvement in its actual creation, but that did have discretion to distribute it or not -- such as a bookstore, library or news vendor -- had considerably less liability than the publisher. Under the Restatement formulation for defamation, for example, “one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.” Restatement (Second) of Torts § 581(1). Moreover, as a general matter, such a distributor was under no duty to investigate the nature or contents of a publication before making it available. Id. at comments d-e.

Common carriers involved simply in the delivery of the publication at issue had virtually no responsibility. Even if they knew the publication to be false and defamatory, they were permitted to deliver it without liability unless they knew or had reason to know that the sender was not protected by any privilege. Restatement (Second) of Torts § 612(2). Moreover, they were entitled to “assume that the sender was privileged until [they had] some sufficient affirmative reason to know the contrary.” Id. at comment g.

Finally, those who simply made available the equipment by which the publication was created or distributed -- such as a printing press manufacturer or telephone company -- had no liability at all, regardless of the circumstances. “Since it is the user of a telephone rather than the telephone company who is treated as transmitting a telephone message . . . , the company is not subject to liability for a defamatory statement communicated by a customer.” Id. See also Restatement (Second) of Torts § 581 comment b; Anderson v. New York Telephone Co., 345 N.Y.S.2d 740 (App. Div. 1973), rev'd mem. on basis of dissent below, 361 N.Y.S.2d 913 (Ct. App. 1974).

These distinctions among publishers, distributors, common carriers and conduits, which are still part of the common law, have in recent years also been absorbed by constitutional doctrine. In Smith v. California, 361 U.S. 147 (1959), for example, the Supreme Court adopted a similar rationale as a matter of First Amendment law and used it to strike down a California statute that imposed strict criminal liability on bookstore owners who stocked “any obscene or indecent writing”:

[T]he constitutional guarantees of the freedom of speech and of the press stand in the way of imposing [this] requirement on the bookseller. By dispensing with any requirement of knowledge of the contents of the book on the part of the seller, the ordinance tends to impose a severe limitation on the public's access to constitutionally protected matter. For if the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected; and thus the State will have imposed a restriction upon the distribution of constitutionally protected as well as obscene literature. . . . And the bookseller's burden would become the public's burden, for by restricting him the public's access to reading matter would be restricted. If the contents of bookshops and periodical stands were restricted to material of which their proprietors had made an inspection, they might be depleted indeed. The bookseller's limitation in the amount of reading material with which he could familiarize himself, and his timidity in the face of his absolute criminal liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly. The bookseller's
self-censorship, compelled by the State, would be a censorship affecting the whole public, hardly less virulent for being privately administered. Through it, the distribution of all books, both obscene and not obscene, would be impeded.

Id. at 152-54 (footnote omitted).

Similarly, in Farmers Educational and Cooperative Union of America v. WDAY, Inc., 360 U.S. 525 (1959), the Supreme Court held that a radio and television station was immune from liability for defamatory statements made on the air by a political candidate who was exercising his statutory right of reply to statements made by his opponents. Noting "this country's tradition of free expression," id. at 529, and recognizing the extreme practical difficulties a station faced under such circumstances, the Court found, in effect, that the station was acting simply as a conduit:

The decision a broadcasting station would have to make in censoring libelous discussion by a candidate is far from easy. Whether a statement is defamatory is rarely clear. Whether such a statement is actionably libelous is an even more complex question, involving as it does, consideration of various legal defenses such as "truth" and the privilege of fair comment. Such issues have always troubled courts. Yet, under petitioner's view of the statute they would have to be resolved by an individual licensee during the stress of a political campaign, often, necessarily, without adequate consideration or basis for decision. Quite possibly, if a station were held responsible for the broadcast of libelous material, all remarks even faintly objectionable would be excluded out of an excess of caution. Moreover, if any censorship were permissible, a station so inclined could intentionally inhibit a candidate's legitimate presentation under the guise of lawful censorship of libelous matter. Because of the time limitation inherent in a political campaign, erroneous decisions by a station could not be corrected by the courts promptly enough to permit the candidate to bring improperly excluded matter before the public. It follows from all this that allowing censorship, even of the attenuated type advocated here, would almost inevitably force a candidate to avoid controversial issues during political debates over radio and television, and hence restrict the coverage of consideration relevant to intelligent political decision.

Id. at 530-31.

These same principles should afford a substantial measure of protection to colleges and universities that provide Internet services. With respect to the information that they (and their employees in the course of their employment) create and disseminate, they will, of course, be treated as traditional publishers. But in large part, college and university Internet providers act primarily as distributors of information created by others. Like any bookseller, library or news vendor, they stock their electronic "shelves" with a wide variety of materials from a wide variety of sources, and, as a practical matter, they cannot prescreen each of those materials and still perform their function of distributing information. Thus, at a minimum, college and university Internet providers should not be held liable for the content of such materials in the absence of a showing that they know or have reason to know that it is tortious or otherwise illegal in character. Moreover, in many cases -- such as e-mail, mailing lists, conferencing services and most student Internet uses -- such providers are more nearly like common carriers or conduits and should arguably be treated accordingly.

The fact that college and university Internet providers may have a right to control the content of their systems does not change this calculus. The same is true of any distributor of any type of information. For example, a bookstore may decline to carry a particular book, but its failure to do so does not automatically make it responsible for the book’s content.
More importantly, any such power of editorial control is largely theoretical. Given the vast quantity of information that flows through such systems -- increasingly, much of it encrypted -- and the speed with which it flows, a provider's editorial control is, as a practical matter, largely limited to the power to veto an information source on a wholesale basis, rather than to conduct any actual review or editing or to exercise any real control over specific content. Even if they could preview everything that flowed through their systems, public colleges and universities would face additional First Amendment restrictions on their ability to make content-based decisions about what they saw. And, to the extent that the Fourth Amendment, the Electronic Communications Privacy Act and similar state statutes (discussed in § IV(B), below) prohibit providers from reviewing communications made through their systems, colleges and universities have no editorial control at all. In short, college and university Internet providers actually have far less ability to control content than a bookseller, library or news vendor.

In reality, the imposition of any greater responsibility for publication torts would effectively require colleges and universities simply to turn off their systems. As the court held in a similar context in Aunvil v. CBS "60 Minutes", 800 F. Supp. 928, 931-32 (E.D. Wash. 1992), a $75,000,000 defamation case against several local TV stations based on a network broadcast that they had transmitted:

With the possible exception of re-run movies, the content of which is already widely known and/or catalogued, plaintiffs' construction would force the creation of full time editorial boards at local stations throughout the country which possess sufficient knowledge, legal acumen and access to experts to continually monitor incoming transmissions and exercise on-the-spot discretionary calls or face $75 million dollar lawsuits at every turn. That is not realistic.

***

More than merely unrealistic in economic terms, it is difficult to imagine a scenario more chilling on the media's right of expression and the public's right to know.

III. Libel

A. General Principles

At its most basic level, libel is the dissemination of a false statement of fact about a specific person that is sufficiently serious to damage that person's reputation. See generally Restatement (Second) of Torts § 558; Bruce Sanford, Libel and Privacy § 4.2 (2d ed. 1993). Significantly for Internet service providers, one who "republishes," or adopts and passes on, a libelous statement is ordinarily equally liable with the statement's originator. Restatement (Second) of Torts § 578. (This rule is qualified, however, by the rules governing distributors, common carriers and conduits discussed in § II, above.) Moreover, "[o]ne who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control" -- including, perhaps, publicly accessible web and Usenet servers or the like -- "is subject to liability for its continued publication." Restatement (Second) of Torts § 577. Cf. Fogg v. Boston & Lowell R.R., 20 N.E. 109 (Mass. 1889) (railroad company may be held liable for libel posted for 40 days on a bulletin board in its ticket office).

Over the years, numerous privileges and defenses have been established as limitations to these general rules. Most important of these has been the abolishment, as a constitutional matter, of strict liability. Under current doctrine, a libel defendant cannot be held liable in the absence of a showing of fault. See generally Restatement (Second) of Torts §§ 558(c), 580A and 580B; Bruce Sanford, Libel and Privacy, chapter 8 (2d ed. 1993).
The degree of fault necessary to establish liability depends upon the identity of the plaintiff. “Public officials” and “public figures” must prove that the defendant acted with “actual malice” -- that is, knowing that the relevant statement was false or having serious, subjective doubts about its truth, a standard similar to the common law standard for distributor liability. New York Times Co. v. Sullivan, 376 U.S. 254 (1964). See also St. Amant v. Thompson, 390 U.S. 727 (1968).


B. Discussion

Based on the cases to date, it appears that libel suits against the authors of libelous Internet communications will play out very much like libel suits involving more traditional means of communication. For example, in Rindos v. Hardwick, <http://www.jmls.edu/cyber/cases/rindos.html> (W. Austl. S.C. 1994), a professor who had been denied tenure sued another professor who, in a message posted to an electronic bulletin board available to academicians worldwide, implied that the reasons for the denial were that the plaintiff professor was incompetent and engaged in pedophilia. Applying garden variety libel principles, the court found that the message was libelous and awarded the plaintiff professor $40,000 in damages.

As for Internet and other online service providers that transmit such messages, however, the law is less clear; to date, only two reported decisions have addressed the liability of such service providers for the libels of their system users, and they appear, at least on their face, to conflict. In the first, Cubby, Inc. v. CompuServe Incorporated, 776 F. Supp. 135 (S.D.N.Y. 1991), the plaintiff sued CompuServe, a national online information service, on the basis of allegedly false and defamatory statements that were contained in an electronic newsletter available in CompuServe's Journalism Forum. The newsletter was published by a third party with no connection to CompuServe, and the Forum itself was moderated by an independent contractor who was responsible for its contents. As a practical matter, neither CompuServe nor the moderator had an opportunity to review the contents of the newsletter, which became available to Forum members as soon as the publisher uploaded it into CompuServe's computer system.

CompuServe sought summary judgment on the grounds that it was an electronic distributor, not the publisher, of the statements at issue; that it did not know or have any reason to know of the allegedly false and defamatory character of the statements when they were made available on its system; and that, as a matter of law, it therefore could not be held liable. The court agreed and granted CompuServe's motion:

[CompuServe] is in essence an electronic, for-profit library that carries a vast number of publications and collects usage and membership fees from its subscribers in return for access to the publications. CompuServe and companies like it are at the forefront of the information industry revolution. High technology has markedly increased the speed with which information is gathered and processed; it is now possible for an individual with a personal computer, modem, and telephone line to have instantaneous access to thousands of news publications from across the United States and around the world. While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents.

... CompuServe has no more editorial control over [the publication at issue] than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so....
Technology is rapidly transforming the information industry. A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory . . . statements.

Id. at 140-41.

By contrast, in Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 N.Y. Misc. LEXIS 229 (Sup. Ct. May 24, 1995), motion for rehearing denied, 24 Media L. Rep. (BNA) 1126 (Sup. Ct. 1995), the court held that another national online information service, Prodigy, was potentially liable as a publisher for a series of defamatory messages that an unidentified user had posted to its Money Talk bulletin board. Claiming to be "in full agreement with Cubby," the court noted a number of differences between the two cases. First, until just a few months before the defamatory postings, Prodigy employees had, in fact, prescreened all messages on its system before allowing them to be posted, though only for obscene, "insulting" or "harassing" language. Second, even after it had abandoned this practice, Prodigy still filtered all messages through its "George Carlin" software, which automatically rejected messages containing such language, and employed "board leaders" who had the power to delete messages that violated its guidelines. Perhaps most importantly, Prodigy had also frequently touted these practices and held itself out to the public as the "family network." In one nationally distributed article, for example, Prodigy stated that ""[c]ertainly no responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate."

Id. at *4.

Based on these facts, the court, in effect, took Prodigy at its word and found it to be a "publisher":

By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and "bad taste," for example, Prodigy is clearly making decisions as to content, and such decisions constitute editorial control. That such control is not complete and is enforced both as early as the notes arrive and as late as a complaint is made, does not minimize or eviscerate the simple fact that Prodigy has uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards. . . .

***

. . . Indeed, it could be said that Prodigy's current system of automatic scanning, Guidelines and Board Leaders may have a chilling effect on freedom of communication in Cyberspace, and it appears that this chilling effect is exactly what Prodigy wants, but for the legal liability that attaches to such censorship.

***

Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.

Id. at *10-*13 (citations omitted).

To the extent that the Prodigy decision hinges simply upon Prodigy's unique public relations campaign, it should make little difference to colleges and universities, which typically do
not claim to (and do not) exercise any significant editorial control over their systems. To the extent that the case holds that prescreening for obscene and offensive language and/or after-the-fact deletion of libelous messages is enough to make the provider the "publisher" of everything on its system, however, it marks a significant departure from past jurisprudence. Distributors frequently choose not to carry obscene or other materials, and they have always been required to remove libelous messages once they "have reason to know" of their existence, but neither practice has ever before been considered sufficient to turn them into "publishers" of all material that they carry. See, e.g., Spence v. Flynt, 647 F. Supp. 1266 (D. Wyo. 1986); Maynard v. Port Publications, Inc., 297 N.W.2d 500 (Wisc. 1980). Indeed, to hold otherwise would be, in effect, to eliminate the distributor category altogether.

Ironically, Prodigy might well have been found liable under traditional distributor liability principles. According to published reports about the case, Prodigy’s customer service department received a complaint about the defamatory postings a few days after they first appeared. Despite this notice, however, Prodigy made no effort to investigate the complaint or to remove the postings until several weeks later, after the lawsuit was filed. Alison Frankel, On-Line, On The Hook, American Lawyer, Oct. 1995, at 64. Because Prodigy thus "had reason to know" that libelous messages were allegedly on its system, its failure to take action would likely have been sufficient for it to have been found liable even as a distributor. Cf. Spence v. Flynt, 647 F. Supp at 1274 ("This was simply not a case of an innocent magazine seller unwittingly disseminating allegedly libelous material. Rather, we have a distributor who possessed detailed knowledge of the ongoing bitter battle between Hustler and Spence, and who, after receiving a complaint about the magazine, failed to investigate and continued to sell it . . . The Court finds that these constitute special circumstances and that Park Place Market has failed to show . . . that it is not liable for the alleged injury to the plaintiffs.").

Regardless of its merits, the Prodigy decision need no longer be of any significant concern. In an effort to encourage Internet service providers to screen out "indecent" material, Congress statutorily overruled Prodigy in a provision of the Communications Decency Act that has not been challenged. See § V(B), below.

What, precisely, these cases and the new statutory provision mean for college and university Internet providers is not entirely clear, but even Cubby should not be taken as the definitive answer for all providers in all contexts. What was an appropriate standard with respect to the proprietary portion of CompuServe’s system, in which CompuServe itself determined what materials to make available, may well be an overly burdensome and inappropriate standard in other contexts. For the reasons stated in § II, above, colleges and universities typically have, and typically exercise, less control over the content of their systems and, in many instances, do no more than make the system available for others’ use. In those instances, they arguably are mere "conduits" and should not be subject even to the "distributor" standard.

IV. Privacy and Related Issues

A. General Principles

What is commonly referred to as the common law “right of privacy” actually encompasses four distinct torts:

- **Intrusion:** “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement (Second) of Torts § 652B.
Misappropriation of Name or Likeness: “One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.” Restatement (Second) of Torts § 652C.

Public Disclosure of Private Facts: “One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” Restatement (Second) of Torts § 652D.

False Light: “One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.” Restatement (Second) of Torts § 652E.

A related tort is the “intentional infliction of emotional distress”: “One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.” Restatement (Second) of Torts § 46.

Many of the common law and constitutional privileges that have developed in the area of libel have been engrafted onto the law pertaining to these torts. For example, the protections accorded to common carriers and conduits in libel cases also extend to privacy cases. Restatement (Second) of Torts § 652G. Moreover, the First Amendment limitations on claims by public officials and public figures have also generally been applied. See, e.g., Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988) (actual malice standard applies to emotional distress claims brought by public figures and public officials). See also Florida Star v. B.J.F., 491 U.S. 524 (1989) (private facts claim cannot be based on information that is publicly available or of legitimate public concern); Time, Inc. v. Hill, 385 U.S. 374 (1967) (actual malice standard applies to false light claims based on reports concerning newsworthy persons or events).

A number of states have refused to recognize the false light tort altogether, finding it to be simply an attempt to evade constitutional protections in the libel area. See, e.g., M.J. DiCorpo, Inc. v. Sweeney, 69 Ohio St. 3d 497 (1994); Howell v. New York Post Co., 596 N.Y.S.2d 350 (N.Y. 1993); Renwick v. News and Observer Publishing Co., 312 S.E.2d 405 (N.C.), cert. denied, 469 U.S. 858 (1984). Similarly, misappropriation has largely been limited to instances involving advertising and other purely commercial contexts. See Restatement (Second) of Torts § 652C comment b. But cf. Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977) (“Wherever the line in particular situations is to be drawn between media reports that are protected and those that are not, we are quite sure that the First and Fourteenth Amendments do not immunize the media when they broadcast a performer’s entire act without his consent.”).

B. Discussion

As has been the case for the traditional media, privacy and related torts should generally not be of overwhelming concern to college and university Internet providers. The constitutional sensitivity for the free flow of information, coupled with the common law rules governing
distributors, common carriers and conduits and the inherent limitations of these torts, should provide a substantial measure of protection for good faith providers.

The effectiveness of these protections is perhaps best demonstrated by the fact that, to date, there have apparently been only two reported cases of any significance—both unsuccessful—involving a common law privacy claim against a computer communication service provider. In *Stern v. Delphi Internet Services Corp.*, 626 N.Y.S.2d 694 (Sup. Ct. 1995), radio personality Howard Stern sued Delphi under New York's version of the misappropriation theory when it published his bare-bottomed photograph in a newspaper ad promoting a newsgroup devoted to his ill-fated candidacy for governor. Citing *Cubby v. CompuServe*, the court held that Delphi was engaged in First Amendment-protected activity and rejected Stern's claim: 'Because Stern's name was used by Delphi to elicit public debate on Stern's candidacy, logically the subsequent use of Stern's name and likeness in the advertisement is afforded the same protection as would be afforded a more traditional news disseminator engaged in the advertisement of a newsworthy product. . . . The newsworthy use of a private person's name or photograph does not give rise to a cause of action under [New York misappropriation law] as long as the use is reasonably related to a matter of public interest.” *Id.* at 698-99.

In *Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), Smyth, an at-will employee, was fired after he allegedly sent an internal e-mail message to his supervisor threatening to "kill the backstabbing bastards" in the company's sales management and referring to the company's holiday party as the "Jim Jones Koolaid affair." Smyth then sued the company under the "intrusion" theory of invasion of privacy, arguing that the company had assured its employees that e-mail communications were confidential and would neither be intercepted nor used as a basis for discipline or termination. The court dismissed the complaint for failure to state a cognizable claim:

In the first instance, unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. . . . We find no privacy interests in such communications.

In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

*Id.* at 101.

Despite the dearth of common law cases, one statutory variant of the tort of intrusion is likely to receive increased attention as the use of e-mail and similar services continues to grow. In the Electronic Communications Privacy Act of 1986 (the "ECPA"), Congress extended the provisions of the Federal Wiretap Statute to "electronic communications," which it defined
generally as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

As thus revised, the Wiretap Statute, "which is famous (if not infamous) for its lack of clarity," Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994), now generally prohibits the actual or attempted "intentional" interception, disclosure or use of an electronic communication by "any person" -- including an "electronic communication service." 18 U.S.C. § 2511(1)(a)-(d).

There are, however, a number of exceptions to this general prohibition. Of most importance, an "electronic communication service" may intercept communications that flow through its system when:

♦ the "electronic communication system . . . is configured so that such electronic communication is readily accessible to the general public" -- as is the case with Usenet and most bulletin board and conferencing systems. 18 U.S.C. § 2511(2)(g)(i).

♦ "one of the parties to the communication has given prior consent to such interception[,] unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d). Note, however, that some state analogs to the Federal Wiretap Statute require both parties to a communication to consent before an "interception" may be made. E.g., Cal. Penal Code §§ 631-32.

♦ "an officer, employee, or agent of a provider of . . . electronic communication service, whose facilities are used in the transmission of a[n] . . . electronic communication, . . . [is acting] in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i). Such persons may also "disclose" and "use" the intercepted electronic communications under the same circumstances, id., and may "divulge the contents of any such communication . . . with the lawful consent of the originator or any addressee or intended recipient of such communication . . . [or] to a person employed or authorized, or whose facilities are used, to forward such communication to its destination." 18 U.S.C. § 2511(3)(b)(ii)-(iii).

The ECPA provides somewhat less protection to communications that are in "electronic storage," see 18 U.S.C. § 2510(17), rather than in actual transmission. For example, an electronic communications service provider is apparently free, at least as a statutory matter, to access (though not always to disclose) communications stored on its system. 18 U.S.C. § 2701(c)(1). See also Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) ("§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage.").

In addition, the ECPA draws a sharp distinction between the contents of an electronic communication and the log files that merely record its existence and transmission. Thus, for example, "a provider of electronic communication service [may] record the fact that a[n] . . . electronic communication was initiated or completed in order to protect such provider, another
provider furnishing service toward the completion of the . . . electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service." 18 U.S.C. § 2511(2)(h)(ii). Similarly, "a provider of electronic communication service . . . may disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by . . . this section) to any person other than a governmental entity." 18 U.S.C. § 2703(c)(1)(A).

While the scope of the ECPA is not yet entirely clear, it does appear that an “electronic communication service” may not routinely monitor all “electronic communications” that it carries, at least without its users’ consent. Well-drafted computer use policies and user notifications should prevent any misunderstandings in this regard.

Public colleges and universities must also consider Fourth Amendment issues, though, again, the case law is sparse. As with the ECPA, however, “reasonable expectations of privacy” appear to be the key. See generally O’Connor v. Ortega, 480 U.S. 709, 722-26 (1987) (“In our view, requiring [a government] employer to obtain a warrant whenever the employer wished to enter an employee’s office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. . . . [P]ublic employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.”). Compare Bohach v. City of Reno, 932 F. Supp at 1235 (no objectively reasonable expectation of privacy exists in a computer system that was “installed to allow communications among police personnel, and between police personnel and the press, about police matters; that it can be used to send private communications between police personnel is incidental to its primary function.”) with United States v. Maxwell, 42 M.J. 568, 576 (A.F.C.C.A. 1995) (“appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password”). Thus, the issue can likely be resolved in computer use policies and user notifications.

While privacy law need not be of major concern to good faith Internet service providers, there may well be a surge of privacy cases against system users as the Internet continues to grow, and the protections available to the media will not likely be available. For example, while the media are rarely, if ever, found liable for the public disclosure of private facts -- if an item appears in the press, it is, almost by definition, deemed to be of public concern -- courts will likely be less deferential to the "news judgment" of, say, the authors of Usenet messages concerning sensitive personal matters. Similarly, "fan" web pages, which are increasingly common, could become a fertile source of misappropriation cases, and the activities of hackers and crackers appear to constitute both intrusion and a violation of the ECPA.

V. Obscenity and Indecency

A. General Principles

The 1994 discovery of more than 90,000 hard-core pornographic images stored on a computer at the Lawrence Livermore nuclear weapons laboratory, see Reuter, Two Employees at Nuclear Lab Face Pornography Charges, Washington Post, August 19, 1994, at A20, highlighted the growing problem of -- and growing interest in -- computer pornography. Many of the most popular newsgroups and bulletin board services are devoted to sex, and it has become extraordinarily simple to digitize and transfer pornographic images. See, e.g., Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (copyright infringement case involving centerfolds that had been scanned onto a bulletin board system).
Virtually every state and municipality has a statute prohibiting the sale or distribution of obscenity, and the federal government prohibits its interstate transportation. Although these statutes have tended to be haphazardly enforced (except at election time), they pose a potential minefield for Internet service providers, which, like officials at Lawrence Livermore, will often have no idea that obscene material is on their systems.

The First Amendment again offers some protection. In Miller v. California, 413 U.S. 15 (1973), the Supreme Court significantly narrowed the permissible scope of obscenity statutes:

We acknowledge . . . the inherent dangers of undertaking to regulate any form of expression. State statutes designed to regulate obscene materials must be carefully limited. As a result, we now confine the permissible scope of such regulation to works which depict or describe sexual conduct. That conduct must be specifically defined by the applicable state law, as written or authoritatively construed. A state offense must also be limited to works which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value.

The basic guidelines for the trier of fact must be: (a) whether "the average person, applying contemporary community standards," would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id. at 23-24 (footnote and citations omitted). Moreover, in Smith v. California, 361 U.S. 147 (1959) (discussed in § II, above), the Court held that obscenity laws could not constitutionally be applied to an unknowing distributor of obscene materials.

B. Discussion

Unlike privacy, the issue of obscenity has been the focus of considerable litigation in the Internet context. Most prominently, the operators of the "Amateur Action" electronic bulletin board service were recently convicted, under federal law, of transmitting obscene images electronically from California to Memphis, Tennessee. The images on which the conviction was based were found to have violated the "contemporary community standards" of Memphis, although they apparently would have passed that test in California. United States v. Thomas, 74 F.3d 701, reh'g en banc denied, 1996 U.S. App. LEXIS 4529 (6th Cir.), cert. denied, 117 S. Ct. 74 (1996). Moreover, there have been numerous obscenity and child pornography "stings," and several convictions, in recent months. See, e.g., United States v. Delmarle, 99 F.3d 80 (2d Cir. 1996) (criminal conviction for computer transmission of child pornography); United States v. Maxwell, 42 M.J. 568 (A.F.C.C.A. 1995) (court martial for computer transmission of obscenity and child pornography); <http://www.iac.net/~ccc/> (web page devoted to a pending obscenity-related case in Cincinnati). Individuals who engage in the creation and dissemination of computer pornography should take note of these developments.

Given the holdings of Miller and Smith, however, obscenity statutes should not be a serious concern for college and university Internet providers, which, at least with respect to obscenity, typically act, at most, as distributors or conduits for materials created by others. Cf. generally Brian T. v. Pacific Bell, 258 Cal. Rptr. 707 (App.), review denied, 1989 Cal. LEXIS 4189 (1989) (common carrier could not be held liable in tort for damages resulting from
dial-a-porn services that it carried). They should, however, take prompt action to investigate and, if necessary, delete any obscene material on their system when it is brought to their attention.

The recently enacted Telecommunications Act of 1996, which includes a number of provisions designed to protect minors from computer “indecency,” will be of greater concern if it survives judicial scrutiny. The relevant provisions had their genesis in two competing bills: the Communications Decency Act, which sought essentially to ban all “indecent” material from the Internet, and the Online Family Empowerment Act, which sought instead to encourage technical, rather than legal, solutions to the problem. Apparently unable to reach an acceptable compromise, Congress simply passed both. Thus, the Telecommunications Act includes a Congressional finding that “[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation,” 47 U.S.C. § 230(a)(4), a statement that “[i]t is the policy of the United States to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation,” 47 U.S.C. § 230(b)(2), and the following new criminal provision:

(d) Whoever --

(1) in interstate or foreign communications knowingly --

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person’s control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

47 U.S.C. § 223(d).2

---

1 Within minutes after President Clinton signed the Telecommunications Act, the ACLU and 19 co-plaintiffs filed an action seeking to block enforcement of the “indecency” provisions of the Act, and at least one other, similar action was filed soon after by the publisher of an electronic newspaper. Both actions were heard by three-judge district court panels, pursuant to a special judicial review provision of the Act, and both resulted in unanimous, strongly worded decisions finding the “indecency” provisions to be unconstitutional. ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996). Anticipating the challenge, and apparently also the outcome, Congress also provided for a direct, expedited appeal to the Supreme Court. The government has appealed both cases, and a decision is likely sometime this spring.

2 The Act also provides that anyone who “by means of a telecommunications device knowingly (i) makes, creates, or solicits, and (ii) initiates the transmission of, any . . . communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age” or who “knowingly permits any telecommunications facility under his control to be used for any such communication may also be held criminally liable. 47 U.S.C. §§223(a)(1)(B) and 223(a)(2). Because the statutory definition of “telecommunications device”
Fortunately, however, the Act also contains a number of defenses that should significantly limit, though not entirely eliminate, college and university liability:

(e) In addition to any other defenses available by law:

(1) No person shall be held to have violated subsection . . . (d) solely for providing access or connection to or from a facility, system, or network not under that person’s control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.

(2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.

(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee’s or agent’s conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

(5) It is a defense to a prosecution under subsection . . . (d) . . . that a person --

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsection[], which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

47 U.S.C. § 223(e).

The legislative history of these provisions indicates that Congress was aiming primarily at those who create and actively disseminate “indecent” content, not at mere access providers. The conference report, for example, states that the “[d]efenses to violations of the new sections assure specifically excludes “interactive computer services,” however, see 47 U.S.C. § 223(h)(1)(B), and because the definition of “interactive computer service” appears to encompass most, if not all, of what college and university Internet service providers do, see 47 U.S.C. § 230(f)(2), it does not appear that section 223(a) will have any significant application. In any event, while they use different language, the two provisions are essentially identical in scope, and the same defenses are applicable to both.
that attention is focused on bad actors and not those who lack knowledge of a violation or whose actions are equivalent to those of common carriers. . . . [New section 223(e)(1)] is designed to target the criminal penalties . . . at content providers who violate this section and persons who conspire with such content providers, rather than entities that simply offer general access to the Internet and other online content. The conferees intend that this defense be construed broadly to avoid impairing the growth of online communications through a regime of vicarious liability.” 142 Cong. Rec. H1078, H1129 (daily ed. Jan. 31, 1996) (H.R. Rep. 104-458).

As a colloquy involving the prime sponsor of the legislation also indicates, however, colleges and universities may still be held liable for “indecent” material that is on their own computer systems unless, in accordance with new Section 223(e)(5), they take “good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors” to such material:

Mr. LEVIN. Mr. President, I would like to engage my colleague from Nebraska, the author of Title V of the telecommunications conference report, in a colloquy. I have a number of questions I hope you can answer to help clarify the intent of title V.

Is a company such as CompuServe which provides access to all mainframes on the Internet liable for anything on those mainframes which its users view?

Is a company like CompuServe which maintains its own mainframe and which allows people to post material on its mainframe liable for prohibited material that other people post there in the absence of an intent that it be used for a posting of prohibited material?

Is the entity that maintains a mainframe, such as a university, that allows a person to post material on its mainframe liable for prohibited material that other people post there in the absence of an intent that it be used for a posting of prohibited material?

Mr. EXON. I appreciate the questions raised by my colleague, Senator Levin. These questions are important and helpful. In general, the legislation is directed at the creators and senders of obscene and indecent information. For instance, new section 223(d)(1) holds liable those persons who knowingly use an interactive computer service to send indecent information or to display indecent information to persons under 18 years of age. You can't use a computer to give pornography to children.

The legislation generally does not hold liable any entity that acts like a common carrier without knowledge of messages it transmits or hold liable an entity which provides access to another system over which the access provider has no ownership of content. Just like in other pornography statutes, Congress does not hold the mailman liable for the mail that he/she delivers. Nothing in [the Act] repeals the protections of the Electronic [Communications] Privacy Act.

For instance, new section 223(e)(1) states that “no person shall be held to have violated subsection . . . (d) solely for providing access or connection to or from a facility, system, or network not under that person's control, * * * that does not include the creation of the content of the communication.” In other words, the telephone companies, the computer services such as CompuServe, universities that provide access to sites on Internet which they do not control, are not liable.
There are some circumstances, however, in which a computer service or telephone company or university could be held liable. If, for instance, the access provider . . . owns or controls a facility, system, or network engaged in providing that information (223(e)(3)), the access provider could potentially be held liable. Access providers are responsible for what's on their system. They are generally not responsible for what's on someone else's system.

Even in these cases, however, an access provider that is involved in providing access to minors can take advantage of an affirmative defense against any liability if the entity takes "good faith, reasonable, effective, and appropriate actions ** to restrict or prevent access by minors to such communications" (223(e)(5)). The Federal Communications Commission may describe procedures which would be taken as evidence of good faith. One such good faith method is set forth in the legislation itself — the access provider will not be liable if it has restricted access to such communications by requiring use of a verified credit card or adult access code (223(e)(5)(B)). This affirmative defense is similar to the defense provided under current law for so-called "dial-a-porn" providers.


While credit card restrictions and adult access codes may help commercial providers avoid liability, they are of little use to colleges and universities, and the Act offers no guidance as to what other measures will suffice under Section 223(e)(5). Colleges and universities can take some comfort in the conference report, which states that "[t]he word 'effective' is given its common meaning and does not require an absolute 100% restriction of access to be judged effective." 142 Cong. Rec. H1078, H1129 (daily ed. Jan. 31, 1996) (H.R. Rep. 104-458). Given the quantity of potentially "offensive" material on college and university systems, and given the number of college students who are under 18 and the number of other minors who have access to college and university systems through high school enrichment programs, freenets, K-12 access programs and other means, however, it appears that this defense will be the crux of the Act for college and university Internet providers.

Should a college or university choose to screen and eliminate all "indecent" materials from its system, it will at least no longer need to worry about the effect such measures may have on its potential liability for libel and other torts. Another provision of the Act specifies that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The conference report indicates that this provision was meant to overrule the Prodigy decision (discussed in § III(B), above), so that concerns about libel would not discourage Internet service providers from imposing such content-based restrictions. 142 Cong. Rec. H1078, H1130 (daily ed. Jan. 31, 1996) (H.R. Rep. 104-458) ("This section provides 'Good Samaritan' protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. One of the specific purposes of this section is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

VI. Sexual Harassment

A. General Principles

Under Title VII and Title IX, sexual harassment, including hostile environment sexual harassment, is prohibited, and colleges and universities have an obligation to maintain an
atmosphere free of such harassment. If the August 14, 1996, draft guidelines from the Office of Civil Rights of the Department of Education are formally adopted, we will be (if we are not already) liable even for peer harassment if we know or should know that it is occurring and fail to take “immediate and appropriate steps to remedy it.”

The standard for what constitutes hostile environment sexual harassment is, finally, becoming settled. As the Supreme Court stated in the employment context in *Harris v. Forklift Systems, Inc.*, 510 U.S. 17 (1993) (citations omitted):

> When the workplace is permeated with “discriminatory intimidation, ridicule, and insult” that is “sufficiently severe or pervasive to alter the conditions of the victim’s employment and create an abusive working environment,” Title VII is violated.

> This standard . . . takes a middle path between making actionable any conduct that is merely offensive and requiring the conduct to cause a tangible psychological injury. . . . “[M]ere utterance of an . . . epithet which engenders offensive feelings in an employee” does not sufficiently affect the conditions of employment to implicate Title VII. Conduct that is not severe or pervasive enough to create an objectively hostile or abusive work environment -- an environment that a reasonable person would find hostile or abusive -- is beyond Title VII’s purview. Likewise, if the victim does not subjectively perceive the environment to be abusive, the conduct has not actually altered the conditions of the victim’s employment, and there is no Title VII violation.

> But Title VII comes into play before the harassing conduct leads to a nervous breakdown. A discriminatorily abusive work environment, even one that does not seriously affect employees’ psychological well-being, can and often will detract from employees’ job performance, discourage employees from remaining on the job, or keep them from advancing in their careers. Moreover, even without regard to these tangible effects, the very fact that the discriminatory conduct was so severe or pervasive that it created a work environment abusive to employees because of their race, gender, religion, or national origin offends Title VII’s broad rule of workplace equality.

**B. Discussion**

The DOE standard for vicarious liability for sexual harassment appears to be similar to the distributor standard of liability for libel and related torts. Although there is, as of yet, no formal interpretation of, of experience under, that standard, it therefore appears that colleges and universities will not be liable for sexual harassment merely because it happens to have taken place on their computer systems.

It seems clear, however, that Internet communications can create or constitute part of a hostile environment. Under the *Harris* standard, an isolated, sexually oriented “flame” is, by itself, unlikely to constitute legally actionable sexual harassment, regardless of how offensive it may be. On the other hand, the constant display of pornographic images on the terminals in an institution’s only public computer lab, like the display of centerfolds on an office wall, may make some students sufficiently uncomfortable that they cannot remain in the lab to complete their own work. Similarly, repeated, sexually derogatory e-mail messages directed to a specific student, like a steady stream of sexist remarks and epithets from colleagues, could substantially impair that student’s learning environment.
The question, as in other contexts, is one of degree. The following are some of the cases in which the question has arisen in the Internet context:

1) The Santa Rosa case. In 1992, a journalism professor at Santa Rosa Junior College established a computer bulletin board on which his students could post messages in "conferences" devoted to various subject matters. In response to student requests, the professor created two gender-restricted conferences, one for male students only and one for female students only. He also established a rule requiring that messages posted to those conferences be kept confidential.

Following a controversy about a sexually suggestive ad in the campus newspaper, some of the participants in the male-only conference posted anatomically explicit and sexually derogatory messages about two women who had spoken out on the issue. Notwithstanding the confidentiality rule, another of the participants in the conference informed the women, and they obtained copies of the messages. They then complained to the college administration, which, upon investigation, found that they had not been subjected to a hostile educational environment, but did take steps to ensure that similar incidents would not happen in the future.

The women then took their complaint to OCR. Although the matter was ultimately settled, OCR did make preliminary findings on the issue of hostile environment. Applying Harris-like standards, OCR preliminarily determined that no such environment had been created as to one of the women, who, though initially frightened by the messages, stated that they had not directly impacted her ability to continue her studies. OCR did preliminarily determine, however, that such an environment had been created for the other woman, who had worked on the campus paper with the men, but was unable to continue to do so effectively after she learned of the messages.

OCR also preliminarily determined that the gender-restriction was itself a violation of 34 C.F.R. § 106.34, which prohibits a recipient of federal funds from carrying out educational programs or activities separately on the basis of sex.

2) Cornell and the "75 Reasons". In 1995, four freshman at Cornell composed and e-mailed to a few of their friends a list of "75 reasons why women (bitches) should not have freedom of speech." The list contained a number of sexist, derogatory and vulgar statements, such as, "If she can't speak, she can't cry rape." Unfortunately for the authors, their friends, who did not consider the list to be harassment, then disseminated it (complete with the authors' names and e-mail addresses) to others, who in turn disseminated it to still others, and so on, until it had made its way around the world. In response, Cornell was flooded with e-mail demands to punish the authors, as well as e-mail threats to "mailbomb" Cornell's computer system if it did. The authors themselves also received a flood of e-mail complaints, including a few death threats. Cornell's Judicial Administrator ultimately determined that the authors had not violated Cornell's sexual harassment policy, since they were not responsible for its distribution to those who considered it harassment. (In fact, most of the list's wide distribution had been effected by those who were offended by it.) The students did, however, voluntarily apologize for the effect that their actions had had on the Cornell community.

3) Knox v. Indiana, 93 F.3d 1327 (7th Cir. 1996). Kristi Knox, a correctional officer at a state prison in Indiana, sued the state under Title VII for sexual harassment committed by her supervisor, Robert Stewart. The basis for her complaint was a lengthy course of misconduct by Stewart that included numerous e-mail messages asking her for sex or an "HGTWM," by which he meant a "horizontal good time with me." Although the court considered Stewart's actions to constitute "blatant sexual harassment," the jury found
for the state on Knox’s quid pro quo and hostile environment claims, apparently on the
ground that the state had not known of Stewart’s actions at the time and had responded
adequately when it learned of them. The jury did, however, award her $40,000 on her
retaliation claim, apparently on the ground that the state did not properly respond to the
actions taken against Knox by co-employees in retaliation for her complaint.

African-American, sued her employer for both sexual and racial harassment following a
series of incidents involving her co-workers. One of the incidents involved an e-mail
message in which a supervisor allegedly addressed her as “Dear Brown Sugar.” The court
found that the message, while offensive to Harley, was not, taken alone, sufficient to create
an objectively hostile environment.

Blaber, a student at the University of Victoria in British Columbia, was found to be in
violation of the harassment provision of the university’s computer use policy, and various
sanctions were imposed upon him, after he posted the following “open letter” to another
student on an electronic newsgroup:

Dear Miss Hardy,

Since being elected to the Board of Governors, I charge that you
have done virtually nothing to benefit the student body other than to create
an atmosphere of gender hatred.

You have not used this medium, the internet to inform we the
students of UVic of any of your sundry albeit useless exploits in the realm
of student politics.

I charge that you are not only incompetent as a member of the board
of governors, but a waste of space on the ballot. It sickens me to think that
you will use this position on your resume without explaining how inept you
actually were.

Pheh!

Robyn Blaber

“And I will execute great vengeance upon them with furious rebukes, and
they shall know that I am the LORD, when I shall lay my vengeance upon
them.” Ezekiel 25:17

Blaber then sued the university, arguing that its actions violated Canada’s Charter
of Rights and Freedoms. The court dismissed his claim upon what appear to be primarily
procedural grounds. In the course of its ruling, however, the court noted that the wording
of the university’s policy “does appear to fall outside the ambit of constitutionally
acceptable infringements of Charter rights.”