A CYBERSPACE UPDATE I: STUDENT ISSUES*

Privacy

2002 National Conference on Law and Higher Education

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 at only 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. Most Internet users, however, do not realize that that is what they are doing – let alone their legal responsibilities for such matters as invasion of others' privacy in doing so.

Most Internet users also do not realize the extraordinary impact that the Internet can have on their *own* privacy. With every move, Internet users create and leave behind a set of virtually indelible electronic "fingerprints", including "clickstreams", "cookies", "caches", "metadata", and more. Such information can be of great interest to employers, marketers, investigators, and others — and of great detriment to the users who created it. Here, too, the law has much to say, though little of it clearly. This outline addresses the major legal principles governing privacy in cyberspace, primarily from the perspective of colleges and universities in their role as Internet service providers.

---

* Portions of this outline are based on materials I originally prepared for the General Counsel of CompuServe Incorporated. I wish to thank CompuServe for its permission to incorporate those materials into this outline.

II. The Law of Privacy

A. The Common Law of Privacy

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 people or events). See generally Bartnicki v. Vopper, 532 U.S. 514 (2001) (publisher cannot be penalized, consistent with First Amendment, for publishing truthful information of public concern that it acquired lawfully, even though the publisher's source obtained it unlawfully).

A number of states have refused to recognize the false light tort altogether, concluding that it is in essence little more than an attempt to evade constitutional protections in the libel area. See, e.g., M.J. DiCorpo, Inc. v. Sweeney, 634 N.E.2d 203 (Ohio 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" in a news program.).

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 been few reported cases of any significance – and apparently no successful ones – 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), for example, 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 Incorporated, 776 F. Supp. 135 (S.D.N.Y. 1991), 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's misappropriation law] as long as the use is reasonably related to a matter of public interest." Id. at 698-99. See also Leary v. Punzi, 687 N.Y.S.2d 551 (Sup. Ct. 1999) (online listing of name of former employee as "contact person" for arts organization is not misappropriation).

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.

More recently, in McLaren v. Microsoft Corp., 1999 Tex. App. Lexis 4103, a terminated employee of Microsoft (a company well known for its interest in privacy issues) sued the company for invasion of privacy after it accessed a folder marked "personal" on "his" office computer during an investigation of sexual harassment charges against him. The court quickly disposed of the claim:

> McLaren's workstation was provided to him by Microsoft so that he could perform the functions of his job. In connection with that purpose and as alleged in McLaren's petition, part of his workstation included a company-owned computer that gave McLaren the ability to send and receive e-mail messages. Thus, contrary to his argument on appeal, the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment. . . . [W]e cannot conclude that McLaren, even by creating a personal password, manifested – and Microsoft recognized – a reasonable expectation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages.

Id. at *11-*12.

The often secretive, apparently extensive, and increasingly intrusive tracking and profiling practices of some online services, however, have resulted in a number of recent lawsuits and calls for legislative action – and may result in enhanced legal protections for privacy as well. See, e.g., In re DoubleClick Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (noting, but not deciding, state law claim for invasion of privacy based on DoubleClick's use of cookies); In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) (same); In re Toys R Us Privacy Litigation, 2001 U.S. Dist. Lexis 16947 (N.D. Cal.) (same); Electronic Information Privacy Center Bill Track, <http://www.epic.org/privacy/bill_track.html>.

In addition, 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 likely will be less deferential to the "news judgment" of, say, the authors of bulletin board postings concerning sensitive personal matters. Similarly, "fan" and "revenge" web pages, which are increasingly common, could become a fertile source of misappropriation cases.

A recent case in the higher education setting illustrates the possibilities. In Felsher v. University of Evansville, 755 N.E.2d 589 (Ind. 2001), a professor who had been terminated from the University of Evansville created e-mail accounts intended to appear to belong to the president and other administrators of the university and then used the accounts to send messages nominating the administrators for numerous positions at other universities. The court, noting that "common law precepts seem to serve surprisingly well in this dramatic new environment", id. at 591, found that the professor had committed misappropriation. See also Aware Woman Center for Choice v. Raney, Case No. 99-5-CV-ORL-19C (M.D. Fla.) (pending case, based in part on private facts theory, brought by an abortion clinic against various Internet service providers that provided anti-abortion activists with access to databases containing personal information); Louder v. CompuServe Incorporated, Case No. BC153274 (Cal.

Super. Ct.) (pending misappropriation case brought by a class of "aspiring and beginning models" whose photographs were made available in a collection of "California Girls" images available in a CompuServe forum).

B. Statutory Privacy

Despite the dearth of common law cases in this area, one statutory variant of the tort of intrusion is receiving increased attention as the use of e-mail and similar services continues to grow. In the Electronic Communications Privacy Act of 1986 ("ECPA"), Congress extended the provisions of the Federal Wiretap Statute to "electronic communications," which are 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). Congress made numerous additional amendments in the recent USA PATRIOT Act.

As it currently stands, ECPA, "which is famous (if not infamous) for its lack of clarity," Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994)[1], 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 a communication that flows through its system when:

---

[1] "[T]he Fifth Circuit . . . might have put the matter too mildly." U.S. v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998), cert. denied, 525 U.S. 1071 (1999). In a subsequent case that proves the point, the Ninth Circuit reaffirmed its agreement with Steve Jackson Games on ECPA's impenetrability, but disagreed with the latter case's substantive holding – a holding that the Ninth Circuit had followed in Smith – only to withdraw its opinion without explanation! Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, op. withdrawn, 262 F.3d 972 (9th Cir. 2001).

- the "electronic communication system . . . is configured so that such electronic communication is readily accessible to the general public" – as is the case with the Web, 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).

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 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."). Moreover, while ECPA prohibits providers of electronic communication service to the general public from disclosing the content of stored communications, see 18 U.S.C. § 2702(a)(1), it contains no such restriction on "proprietary" providers, see Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) – a category that seems to include college and university providers.

In addition, 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 to the public"[2] may disclose "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . .) to any person other than a governmental entity". 18 U.S.C. § 2702(c)(5). See U.S. v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999), aff'd mem., 225 F.3d 656 (4th Cir. 2000), cert. denied, 531 U.S. 1099 (2001) ("ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn . . . transactional records over to nongovermental entities."). Accord Hill v. WorldCom Communications, Inc., 120 F. Supp. 2d 1194 (S.D. Iowa 2000); Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998). In addition, a provider apparently may disclose both transaction records and message contents to governmental entities, on the provider's own initiative, to "protect[] [the provider's] rights or property", 18 U.S.C. § 2702(b)(5) and § 2702(c)(3), but it generally may not do so in response to an informal governmental request, see McVeigh

[2] While ECPA contains no similar express authorization for "proprietary" providers – again, seemingly including colleges and universities – they apparently are considered to have inherent authority to disclose such records, at least insofar as ECPA is concerned.

v. Cohen, 983 F. Supp. 215 (D.D.C. 1998) (depending upon the circumstances, a governmental entity may obtain access to such records only with a search warrant; court order; or administrative, grand jury, or trial subpoena or with subscriber consent). See also FTC v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000) (a governmental entity may not obtain subscriber information by means of a pre-trial discovery subpoena).

While the USA PATRIOT Act's efforts to simplify and clarify ECPA were not entirely successful, it did succeed in its efforts to significantly broaden government access to electronic communications. For example, a provider of "electronic communication service to the public" may now disclose subscriber information to any "governmental entity" if "the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information", 18 U.S.C. § 2702(c)(4), and may also disclose communication contents to "a law enforcement agency" if "the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay", 18 U.S.C. § 2702(b)(6)(C). Moreover, the types of subscriber information that the government may compel a provider to disclose by means of an administrative subpoena has been expanded to include "records of session times and durations"; "any temporarily assigned network address", including the IP address assigned to the subscriber; the "length of service (including start date) and types of service utilized"; and the "means and source of payment for such service (including any credit card or bank number)", in addition to the subscriber's name, address, and "subscriber number or identity" authorized under prior law. 18 U.S.C. § 2703(c)(2). See generally 18 U.S.C. § 2703 (requirements for compelled disclosure to the government).

While the scope of ECPA is still not entirely clear,[3] it does appear that an "electronic communication service" may not routinely monitor all "electronic

[3] For the latest "official" word on ECPA and related privacy issues, see the Department of Justice's manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, <http://www.cybercrime.gov/searchmanual.htm> (2001), and its most recent update, Field Guidance on New Authorities that Relate to

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.

C. Constitutional Privacy

Public colleges and universities must also consider Fourth Amendment issues, though, again, the case law is sparse. As with 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 U.S. v. Maxwell, 45 M.J. 406 (C.M.A. 1996) ("While implicit promises or contractual guarantees of privacy by commercial entities do not guarantee a constitutional expectation of privacy, we conclude that under the circumstances here appellant possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL."), U.S. v. Monroe, 50 M.J. 550, 558 (A.F.C.C.A. 1999), aff'd, 52 M.J. 326 (C.A.A.F. 2000) ("In Maxwell, the Court held that a

---

Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001, <http://www.cybercrime.gov/PatriotAct.htm> (2001). The "Quick Reference Guide" portion of Searching and Seizing Computers, a chart summarizing the principal ECPA provisions governing disclosure to law enforcement authorities, is particularly helpful (though it must be read in conjunction with the update). It is available at <http://www.cybercrime.gov/searchmanual.htm#IIIf>.

subscriber has a reasonable expectation of privacy in an e-mail box which can be overcome only by a warrant issued upon probable cause. That holding, however, was confined specifically to a commercial, contractual scenario . . . . In the instant case, we are faced with the insular setting of a government system which acted as a gateway between its users and the internet and which had known specific limitations on use. . . . In view of the fact that the mailbox was issued to appellant via official channels for performance of his official duties, and restricted unofficial personal use, his electronic mailbox was akin to other types of government property routinely designated for or assigned to military personnel for performance of their official duties. One does not acquire a reasonable expectation of privacy in government property designated or assigned under these circumstances."), and U.S. v. Butler, 151 F. Supp. 2d 82 (D. Maine 2001) ("What [the] objectively reasonable expectation is for computers, under circumstances of shared usage, presents questions of some difficulty in today's environment of rapidly changing technology and provisions of service. I do not have to confront these difficult issues because the defendant has made not even a minimal showing that he had a reasonable expectation of privacy in either his session logs or the hard drives of these University-owned computers. Session logs are obviously maintained for the benefit of the University and therefore not suppressible on the defendant/student's motion. . . . As for the hard drives, the defendant has pointed to no computer privacy policies in effect at the University, no statements or representations made to him as a user of the computers in this [public] lab, no practices concerning access to and retention of the contents of hard drives, not even password requirements. From all that appears, he, along with other students, was simply using the University computers under circumstances where images on the monitor were visible to others (as occurred here), and no commitments were made as to the privacy of hard drives.").

To a large degree, the ambiguities and uncertainties inherent in the fact-intensive, case-by-case Fourth Amendment analysis can be eliminated by establishing, in computer use policies and user notifications, what expectations are reasonable for a given system. In U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000), for example, an employee of the CIA's Foreign Bureau of Information Services was charged with having viewed and stored child pornography on his office computer. The court rejected his

motion to suppress the results of a search of that computer, relying on FBIS policy that expressly authorized such searches:

> Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use.

Id. at 398 (footnotes and citations omitted). Cf. Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (holding that state employee had a Fourth Amendment expectation of privacy in a computer assigned exclusively to him when his department had not "placed [him] on notice that he should have no expectation of privacy in the contents of his office computer" and did not have "a general practice of routinely conducting searches of office computers"); Adams v. City of Battle Creek, 250 F.3d 980, rehearing denied, 2001 U.S. App. Lexis 16099 (6th Cir. 2001) (holding that a "general policy of the [police] department that department-issued equipment . . . was not to be 'converted to personal use' cannot provide the necessary notice" to make an expectation of privacy unreasonable). But see U.S. v. Butler, 151 F. Supp. 2d 82 (D. Maine 2001) (finding no expectation of privacy in a shared computer in a public computing lab in the absence of a privacy policy).

Public institutions must also consider whether the information they are collecting and disseminating over the Internet is subject to a constitutional right of informational privacy. See Whalen v. Roe, 429 U.S. 589, 605-06 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a

proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data -- whether intentional or unintentional -- or by a system that did not contain comparable security provisions."); Nixon v. Administrator of General Services, 433 U.S. 425, 457-59 (1977).

Early indications suggest that any such restrictions will be slight. In Akella v. Michigan Dept. of State Police, 67 F. Supp. 2d 716 (E.D. Mich. 1999), several persons required to register as sex offenders under Michigan's version of "Megan's Law" challenged Michigan's decision to make their registration information available on the Internet, in part on common law invasion of privacy grounds. The court made quick work of the claim, holding that "plaintiffs do not have a 'legitimate privacy interest in preventing compilation and dissemination of truthful information that is already, albeit less conveniently, a matter of public record.' . . . [T]he Court concludes that dissemination of sex offender registration materials [over the Internet] does not violate any constitutionally protected privacy interest of plaintiffs." Id. at 729 (citation omitted). Accord State v. Stevens, 992 P.2d 1244, 1249 (Kan. App. 1999), review denied, 2000 Kan. Lexis 52 ("[W]e conclude that the placing of offender registration information on the internet does not impinge on Stevens' constitutional right of privacy. A strong argument can be made for requiring a court to determine a level of risk involved on a case-by-case basis and then determining to what degree the State is allowed to impinge on an individual's right of privacy to better ensure public safety. We can assume here that the legislature carefully studied such a proposal and rejected it."); U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999), cert. denied, 530 U.S. 1213 (2000) (FCC regulation requiring telephone companies to obtain customer consent before disclosing their telephone records for marketing purposes violates the First Amendment). But see Condon v. Reno, 528 U.S. 141 (1999) (Congress may prohibit disclosure and resale of personal information contained in the records of state motor vehicles departments); Los Angeles Police Dept. v. United Reporting Publishing Corp., 528 U.S. 32 (1999) (First Amendment does not require a state to disclose personal information in arrest records); A.A. v. New Jersey, 2001 U.S. Dist Lexis 20350 (D.N.J.) (convicted sex-offenders' "privacy interests in controlling the disclosure of their home addresses, while limited, are

nevertheless entitled to constitutional protection against 'willy-nilly' disclosure to the general public" over the Internet; however, "information regarding an individual's criminal history, as well as the basic identifying information accompanying it, is not constitutionally entitled to privacy protection"); Kirkland v. Sheehan, <http://www.justicefiles.org/Court%20Oders/Court%20Order%20May%2010th%202001.htm> (Wash. Super. Ct. 2001) (granting injunction requiring removal of police officer Social Security Numbers from publicly accessible web site).

D. FERPA

Although it was enacted long before the prevalence of electronic records and was not specifically written with them in mind, the Family Educational Rights and Privacy Act nevertheless applies to student records that are maintained electronically equally with those maintained on paper. FERPA defines its key term, "education records", to mean "those records that are: (1) [d]irectly related to a student; and (2) [m]aintained by an educational agency or institution or by a party acting for the agency or institution", and further defines "record" to include "*any* information recorded in *any* way, including, but not limited to, handwriting, print, *computer media*, video or audio tape, film, microfilm, and microfiche". 34 C.F.R. § 99.3 (emphasis added). See also 61 Fed. Reg. 10663, 10664 (Mar. 14, 1996) (noting that "computer media" was included in the definition "to reflect changing technology and changing modes of maintaining information").

Thus, for example, student e-mail messages are, when in the possession of an educational institution, generally protected from disclosure without the student's consent. See, e.g., President and Trustees of Bates College v. Congregation Beth Abraham, 2001 Me. Super. Lexis 22 (2001) ("The e-mail messages here were generated by students and directed to the[ir] faculty advisor . . . . The records directly related to the named students and sought the advice and assistance of a person acting for the college. Although the e-mail correspondence may be of a different character than most records, files and documents maintained by an educational institution, [FERPA] does not limit the definition of [education records]. As such that term ought to

be liberally construed to be inclusive rather than exclusive to carry out the Act's purpose and intent for the protection of the students.")

On the other hand, FERPA now specifically authorizes educational institutions to include e-mail addresses in their definitions of "directory information". 34 C.F.R. § 99.3. See also 65 Fed. Reg. 41852, 41855 (July 6, 2000) ("[A]s methods of communication and record management continue to evolve, it is useful to list additional categories of information that we believe are directory information, such as a student's e-mail address . . . . We do not believe that the disclosure of student e-mail addresses will generally be considered harmful or an invasion of privacy. We think that a student's e-mail address is analogous to a student's mailing address, an item already included as directory information.")

For an excellent resource on building electronic student records systems consistently with FERPA and related privacy principles, see Privacy and the Handling of Student Information in the Electronic Networked Environments of Colleges and Universities, <http://www.educause.edu/ir/library/pdf/PUB3102.pdf>, a white paper developed jointly by CAUSE and AACRAO in 1996.

E. FOIA and Public Records Statutes

Finally, in addition to the numerous privacy protections for electronic records, public colleges and universities must also grapple with the equally confusing, and often seemingly conflicting, requirements imposed upon them by applicable freedom of information and public records statutes. These statutes, which exist in every state, typically apply to *all* records *regardless* of their form; it generally is the *substance* of a record that governs its status as public or not. See, e.g., State, ex rel. Wilson-Simmons v. Lake County Sheriff's Dept., 693 N.E.2d 789, 793 n.1 (Ohio 1998) ("In . . . holding [that a particular e-mail message is not subject to Ohio's public records statute], we reject the sheriff's department's broader assertion that no public office e-mail would ever be public records . . . . [I]t is unnecessary for an expression to be in a particular medium for it to be a public record.") However, while legislatures and courts have had little trouble determining that electronic records are subject to these statutes in general,

they have had considerable trouble determining just what constitutes an electronic record in particular. The cases are just beginning to consider whether "cookies", "metadata", and other such "extra-textual" materials should be considered part of the public record, and it likely will be years before all of the policy and practical issues are sorted out. See, e.g., Public Citizen v. Carlin, 184 F.3d 900, 910 (D.C. Cir. 1999), cert. denied, 529 U.S. 1003 (2000) ("a paper printout of an electronic mail record is not an "extra copy" within the meaning of [the Federal Records Act] if it does not include transmission data, such as the names and addresses of both the recipient and the author and the date the message was sent – the electronic equivalents of the address, return address, and date on correspondence sent by conventional mail"); Putnam Pit, Inc. v. City of Cookeville, 23 F. Supp. 2d 822 (M.D. Tenn. 1998), aff'd in part and rev'd in part, 221 F.3d 834 (6th Cir. 2000) (considering, but not deciding, whether "cookies" are subject to Tennessee's public records statute).