WHOSE COMPUTER IS IT, ANYWAY?

Presenter:

STEVEN J. McDONALD
Associate Legal Counsel
The Ohio State University
Columbus, Ohio
WHOSE COMPUTER IS IT, ANYWAY?  
(THE "LONG FORM" VERSION)*

Stetson University College of Law  
20th Annual 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 only at the receiving end of mass communications. With access to the Internet, anyone — even a preschool child — can now effectively be an international publisher and broadcaster. By posting to Usenet or establishing a web page, for example, an Internet user can speak to a larger and wider audience than does the New York Times, NBC, or National Public Radio. 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", 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.

* 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.
This outline addresses in depth the major legal principles governing privacy in cyberspace, primarily from the perspective of colleges and universities in their role as Internet service providers. Other materials in this package include a copy of the presentation for this session (the "short form" version), a sample Internet privacy policy, and a bibliography of privacy-related resources available on the Internet.

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 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.").

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, 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 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.

While common law privacy principles 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, cf. 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). A number of such cases have been filed, and many of them have been settled on undisclosed terms.

B. Statutory Privacy

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 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).
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). See McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998) (a governmental entity may obtain access to such records only with a specified warrant, court order, or subpoena or with subscriber consent).

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.

**C. Constitutional Privacy**

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, 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."). Thus, the issue can likely be resolved in computer use policies and user notifications.
Whose Computer Is It, Anyway?

Steven J. McDonald
Associate Legal Counsel
The Ohio State University

20th Annual National Conference on
Law and Higher Education

The Key to Handling On-Line
Privacy Issues Successfully

But First, Let's Invade
A Little Privacy

- AnyWho
  - http://www.anywho.com
- FECinfo
  - http://www.fec.com/lodinfo
- Franklin County Property Records
  - http://www.co.franklin.oh.us/auditor
- DejaNews
  - http://www.dejanews.com
- Magellan Veyeur
  - http://veyeur.magellan.com/cgi-bin/veyeur.cgi
- Showmeit
  - http://www.showmeit.com
- Coches, Cookies, and History Files
What is Privacy?

"The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people."

Justice Louis Brandeis
Olmstead v. U.S. (1928)

The Legal Basis for Privacy:
A Patchwork Quilt

• U.S. and State Constitutions
  – But no explicit reference in U.S. Constitution
  – Fourth Amendment (and State versions)
• Statutory Privacy
  – Electronic Communications Privacy Act (and State versions)
  – But also FERPA, State open records laws, and discovery rules
  – And much, much more
• The Common Law of Privacy

The Fourth Amendment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Publics are Private, 
Privates are Not

"Although individuals have a right under the 
Fourth Amendment of the United States 
Constitution to be free from unreasonable 
searches and seizures by the Government, 
private searches are not subject to constitutional 
restrictions."

U.S. v. Hall (7th Cir. 1998)

O'Connor v. Ortega (S.C. 1987)

"Fourth Amendment rights are implicated only 
if the conduct of the [government] officials at 
issue ... infringe[s] 'an expectation of privacy 
that society is prepared to consider reasonable.'

... Given the great variety of work 
environments in the public sector, the question 
whether an employee has a reasonable 
expectation of privacy must be addressed on a 
case-by-case basis."

O'Connor v. Ortega

"We hold ... that public 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. 
Under this reasonableness standard, both the 
inception and the scope of the intrusion must be 
reasonable."
O'Connor v. Ortega

"Ordinarily, a search of an employee's office by a supervisor will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file... The search will be permissible in its scope when 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of... the nature of the [misconduct].'

The Fourth Amendment in Cyberspace

"We are satisfied that the Constitution requires that the FBI and other police agencies establish probable cause to enter into a personal and private computer. However, when an individual sends or mails letters, messages, or other information on the computer, that Fourth Amendment expectation of privacy diminishes incrementally."

U.S. v. Maxwell (C.M.A. 1996)

Reasonable Expectations in Cyberspace

• Who owns the system?
• Who has access to the system?
• How does the system work?
• How was the system used?
• Is the system password-protected?
• What policies apply to the system?
• What is the ordinary practice?
The Electronic Communications Privacy Act (ECPA)

- Enacted in 1986 as a revision of the Federal Wiretap Statute.
- "[A] statute . . . which is famous (if not infamous) for its lack of clarity"—Steve Jackson Games, Inc. v. United States Secret Service (9th Cir. 1994)

ECPA Prohibitions

- Generally illegal to:
  - Intercept an electronic communication while it is in transmission
  - Disclose the contents of an electronic communication that has been illegally intercepted
  - Use the contents of an electronic communication that has been illegally intercepted

ECPA Exceptions

- A provider of electronic communication service may intercept an electronic communication, or disclose or use an intercepted communication, "while engaged in any activity which is a necessary incident to the rendition of [its] service or to the protection of [its] rights or property"
ECPA Exceptions

- A party to an electronic communication, or a person to whom a party to an electronic communication has given consent, may intercept the communication "unless such communication is intercepted for the purpose of committing any criminal or tortious act"
  - An exception to the exception: Some states require that all parties consent

More ECPA Prohibitions and Exceptions

- Generally illegal to access an electronic communication while it is in electronic storage
  - But a provider of electronic communication service has apparently unlimited authority to access stored communications on its system
- But a provider of electronic communication service to the public generally may not divulge the contents of a stored communication
  - But any provider may divulge the contents of a stored communication with consent or as a necessary incident to the rendition of service or to protect its rights or property

Law Enforcement Access

- Voluntary or at government request?
- Obtained inadvertently or intentionally?
- In transmission or in storage?
  - In storage more than 180 days?
- Contents or log files?
- With consent of user or without?
- With notice to user or without?
Common Law
Invasion of Privacy

"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

Smyth v. The Pillsbury Co.
(E.D. Pa. 1996)

"[E]ven 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. ... [I]n 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."

FERPA, Open Records and Discovery

• Substance generally governs over form
  – So student e-mail will generally be protected by FERPA
  – But public employee e-mail may be a public record
  – And everyone's e-mail will generally be discoverable in litigation
• Not much case law yet
Untangling the Privacy Mess

- Ignore the law
- Establish — and follow — a policy
  - What expectations are reasonable?
  - Consent
- Options:
  - No privacy
  - Total privacy
  - Somewhere in between
Policy on Responsible Use of University Computing Resources
The Ohio State University

General Statement

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

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

Applicability

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of the university or to uses within specific units. Consult the operators or managers of the specific computer, computer system, or network in which you are interested or the management of the unit for further information.

Policy

All users of university computing resources must:

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

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

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

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

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

- **Refrain from stating or implying that they speak on behalf of the university and from using university trademarks and logos without authorization to do so.** Affiliation with the university does not, by itself, imply authorization to speak on behalf of the university. Authorization to use university trademarks and logos on university computing resources may be granted only by the Office of University Communications or The Office of Trademarks and Licensing, as appropriate. The use of suitable disclaimers is encouraged.

**Enforcement**

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

Security and Privacy

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

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

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

Cyberspace Law for Non-Lawyers

An excellent, plain-English discussion of basic privacy (and other) law as it applies in the online world

Lost and Found in Cyberspace
http://www.info-law.com/lost.html

A more detailed law review article about online privacy law

Cyberspace Law Index: Privacy
http://www.jmls.edu/cyber/index/privacy.html

A collection of important cyberspace-related privacy cases, law review articles, and other materials, in full text

Department of Justice Computer Crime and Intellectual Property Section
http://www.usdoj.gov/criminal/cybercrime/index.html

Information on search and seizure in cyberspace

Federal Trade Commission Privacy Page
http://www.ftc.gov/privacy/index.html

National Telecommunications and Information Administration Privacy Page
http://www.ntia.doc.gov/ntiahome/privacy/index.html

Extensive information on federal government reviews and initiatives

The Privacy Page
http://www.privacy.org

Privacy Rights Clearinghouse
http://www.privacyrights.org

Electronic Privacy Information center
http://www.epic.org

Online Privacy Alliance
http://www.privacyalliance.org

The home pages of several advocacy groups interested in electronic privacy issues
Dejanews
http://www.dejanews.com

AnyWho
http://www.anywho.com/resq.html

FECInfo
http://www.tray.com/fecinfo

Daily Usenet Usage Report
http://globe.acs.ohio-state.edu/reports/newsdata

Magellan Voyeur
http://voyeur.mckinley.com/cgi-bin/voyeur.cgi

Showstat
http://www.showstat.com

Engage Technologies
http://www.engage.com

The Stalker's Homepage
http://www.glr.com/ stalk.html

Cookie Central
http://www.cookiecentral.com

Junkbusters Cookie Demonstration

The Anonymizer
http://www.anonymizer.com/cgi-bin/snoop.pl

Several interesting, and often revealing, demonstrations and collections of materials about online privacy