J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 6(3) 179-191, 1997-98

CYBERSMUT IN THE WORKPLACE: A NEW LEGAL MINEFIELD FOR EMPLOYERS

MICHAEL A. ZIGARELLI
Fairfield University, Connecticut

ABSTRACT

Because the Internet is rapidly becoming one of the most important business tools of the 1990s, employers are increasingly affording their workforces access to it. However, employee access to this technology has also presented human resource managers with yet another legal quagmire. In particular employee browsing of on-line pornographic materials on the job has implicated sexual harassment law, while proscribing such recreational use raises privacy and other legal concerns. This article identifies the legal pitfalls inherent in employee access to Internet pornography and in prohibition of such behavior. It also offers recommendations to human resource professionals for developing an Internet-access policy that both enables legitimate business use and insulates the organization from the liability associated with recreational use.

The Internet is, in all likelihood, the most powerful information vehicle in human history, currently linking approximately forty million people worldwide. With its virtually unlimited capability to cost-effectively reach the global marketplace, the Internet is also fast becoming an essential business tool. From marketing products, to furnishing customers with information, to recruiting, to research, organizations are increasingly going on-line to disseminate and collect information.

However, for many organizations in the United States, affording a workforce access to the Internet is manifesting itself as a double-edged sword. Although business-related use of the Internet may help employees work more efficiently and more productively, recreational use during work time has the opposite effect. One particular recreational use—accessing on-line pornography—was recently

doi: 10.2190/GD4W-2R1V-056W-9BQV
http://baywood.com

investigated by Nielsen Media Research, which found the on-line version of Penthouse Magazine is called up thousands of times each month by employees at IBM, Apple Computer, AT&T, NASA, and Hewlett-Packard [1].

Potentially lower productivity is but one problem that such Internet use poses for employers. Permitting access to Internet pornography in the workplace may, as is discussed in this article, expose employers to significant liability for sexual harassment. Moreover, designing and administering a policy to eradicate this problem is also replete with legal pitfalls that range from privacy concerns to, in light of the addictive nature of pornography, disability discrimination issues. After a brief primer on the Internet, this article details the legal implications of both employee access to Internet pornography and the prohibition of such access. It also offers recommendations to human resource professionals for developing an Internet-access policy that enables legitimate business use while insulating the organization from the liability associated with recreational use.

AN OVERVIEW OF THE INTERNET [2]

Before delving into the legal issues surrounding employee Internet use, it may be helpful to describe what is available on the Internet and how its information is accessed. The Internet is a vast network of smaller computer networks. Some of these smaller networks are "closed," meaning that access to the information on them is restricted to privileged users, whereas the overwhelming majority of these networks are "open" for public access.

The Internet is not administered by any one entity. There is no central storage facility or control point. Rather, its information is stored on the millions of linked computer networks around the world. An individual can access information on any of these open systems either through a terminal that is connected to one of these networks (e.g., in academic, government, and commercial institutions), or by using a personal computer and a modem to dial in to a network, such as an on-line service (e.g., America Online, Compuserve, Prodigy). Increasingly, employers are providing employees with terminal or modem access to the office network, and thus to the Internet [3].

Accessing and Exchanging Information

There are various methods of exchanging information on the Internet. The most common is electronic mail or "e-mail," which permits one individual to send a message to another individual anywhere in the world. One can also send a message to several people simultaneously through a "listserv," which essentially functions as a mailing list of persons who have similar interests in a particular topic. Every message sent to the listserv is received by every person who has "subscribed" to that mailing list. A third communication method is a "distributed

message database," the most common of which is a USENET newsgroup. Individuals can post messages to any of over 15,000 newsgroups and can read messages posted by other individuals. Some of these newsgroups are "moderated," meaning that someone screens all messages for content and determines whether the message is appropriate for the group, whereas others are unmoderated.

"Real-time communications" is a fourth communication method, substantially paralleling a telephone party line. Comments posted to the chat group are seen instantly by others who are currently on-line and who can respond immediately. A fifth method is "Telnet," which provides remote computer access to networks linked to the Internet. One might, for example, telnet into the Library of Congress' computerized card catalog to peruse what is available or into a university business school's network to seek information on its curriculum and faculty. To retrieve information from these networks, one has the option of using tools such as "gopher" or "file transfer protocol" (FTP); however, information access and retrieval is increasingly performed via the World Wide Web (the Web, WWW).

The Web is the most advanced information system on the Internet. Persons or organizations wishing to share text, images, or sounds can create what is called a "home page"—an information retrieval starting point. Using software such as Netscape or Mosaic, an individual can locate and visit a home page of interest and then access other parts of the website through what are called "hypertext links." To illustrate, if someone were seeking information about a particular corporation, he or she could connect directly to that corporation's home page, find general information about the business on this page, and find hypertext links to other information such as the company's history, its specific products and services, and how to place an order. Clicking on the link of interest transports (often immediately) the website visitor to the Internet location where the desired information exists.

Websites range from highly sophisticated corporate pages to pages by individuals that amount to little more than a personal newsletter. Some sites are restricted to authorized users, but others, indeed most websites, are open to the public. The information on the accessed site can be printed on one's personal or network printer or saved to a file on one's local computer.

What Is Available on the Internet

The content of the Internet is vast and diverse and defies simple classification. Newspapers and magazines are available for on-line reading, government publications can be retrieved, corporations provide product information, nonprofit organizations offer information of public interest, universities and municipalities put card catalogs on-line, professors put entire courses on the Web, and newsgroups and listservs exist for every imaginable topic. Such diversity of content is

possible because the Internet affords individuals and organizations an inexpensive vehicle to reach millions of people.

Not surprisingly, sexually explicit material ranging from modest to hard-core is also available and commonplace on the Internet. In fact, a study by a Carnegie Mellon University research team concluded that "one of the largest (if not the largest) recreational applications of users of computer networks [is] the distribution and consumption of sexually explicit imagery" [4, p. 1849]. These widely available text, picture, and sound files are transferable by e-mail, listservs, newsgroups FTP, gopher, and the Web, and many of these materials cost nothing to access or download. Additionally, several closed, commercial systems, including a multitude of "bulletin board systems" that operate much like newsgroups, permit paying customers to download pornographic materials.

PORNOGRAPHY AND SEXUAL HARASSMENT

Much of the traffic on the Internet's red-light district comes from individuals browsing these sites from their workplace, thus raising a new legal conundrum for human resource managers: can employee access to Internet pornography expose employers to sexual harassment liability? That is, can an aggrieved employee demonstrate a nexus between pornography in the workplace and the creation of a hostile work environment? Some courts that have considered these questions have either held or implied that the answer them is "yes."

The Pornography-Harassment Nexus

There is an abundance of academic literature that illustrates the pernicious effects of viewing pornography. The findings germane to the creation of a hostile work environment are briefly summarized here.

There appears to be substantial empirical support for a causal connection between an individual's exposure to pornography and adverse treatment of women by that individual [5]. In particular, viewing pornography has been linked to a variety of behaviors, including increased discussions about sex, greater acceptance of promiscuity and extramarital sex, callousness and insensitivity toward women, objectification and stereotyping of women, marital discord, child molestation, wife battering, incest, rape, and even murder [6-9]. A thorough review of the evidence on this subject led a 1986 Attorney General's Commission on Pornography to report that

> substantial exposure to materials of this type bears some causal relationship to the incidence of various non-violent forms of discrimination against women . . . To the extent that these materials create or reinforce the view that women's function is disproportionately to satisfy the sexual needs of men, then the material will have pervasive effects on the treatment of women in

> society far beyond the identifiable acts of rape or other sexual violence [10, p. 334].

The effects of pornography appears to progress through four distinctive stages: addiction to pornography, increased consumption of pornography, desensitization to previously shocking material, and tendency to act out activities that are witnessed [11]. In the workplace context, therefore, viewing pornography may culminate in both lower individual productivity (as one elects to feed his addiction rather than to work) and dehumanizing and harassing behavior toward female coworkers (as one seeks to act out what he has witnessed).

Judicial Treatment of the Pornography-Harassment Nexus

To date, only a few courts have scrutinized the above linkage and addressed whether the presence of pornography in the workplace is tantamount to sexual harassment. The most widely-cited case in this area is *Robinson v. Jacksonville Shipyards, Inc.* [12]. Here, a female welder, Lois Robinson, worked in a male-dominated environment where pin-ups, calendars, and posters of nude women were commonplace. Her complaints about the pictures met with managerial indifference and admonishments to simply look the other way if she were offended. The court, in evaluating Robinson's sexual harassment claim, concluded that because the presence of pornography at work reinforces sexual stereotypes and because this objectification burdens women with a condition of employment that men do not have, its presence created a hostile work environment within the meaning of Title VII. The academic evidence on the pornography-harassment nexus was found to not only be credible here, but determinative of the outcome [13].

Other courts have reached the opposite conclusion. In *Rabidue v. Osceola Refining Co.*, for example, the court held that

> 'Sexual jokes, sexual conversations and girlie magazines may abound [in some work environments]. Title VII was not meant to . . . change this.' . . . The sexually oriented poster displays had a de minimis effect on the plaintiff's work environment [17, at 620-22, quoting 18 at 419, 430].

Similarly, in *Johnson v. County of Los Angeles*, the court rejected a claim that reading *Playboy Magazine* in the privacy of one's office constitutes sexual harassment, ruling:

> [There is no precedent that] Title VII protects women from thoughts alone. Although Title VII would certainly prevent a male employee from manifesting sexually degrading thoughts in the form of sexually degrading comments or actions, until the thought is manifested, it is outside the scope of Title VII [19, at 1439-40].

Accordingly, in light of this paucity and inconsistency of case law, it is not known whether most jurisdictions would accept the existence of a pornography-harassment nexus. However, even if this linkage is not recognized by the courts, pornography in the workplace is still legally problematic for employers since its presence has been considered supporting evidence that a hostile work environment indeed exists (e.g., *Andrews v. City of Philadelphia* [20], *Waltman v. International Paper Co.* [21]). Accordingly, the most prudent course of action with respect to workplace pornography is to prohibit it altogether, whether in a hard-copy or electronic form. In doing so, an employer may decrease the likelihood that a hostile work environment will be created and may simultaneously eliminate a potential source of nonproductivity. Moreover, if the employer were sued for sexual harassment, such a policy, if enforced, would also serve as important evidence that the employer does not tolerate harassment and has sought to eradicate it.

LEGAL IMPLICATIONS OF PROHIBITING ACCESS TO INTERNET PORNOGRAPHY

Unfortunately, for employers seeking insulation from sexual harassment liability, the proscription of employee access to cybersmut will itself raise thorny legal issues. Employer attempts to implement and enforce such a ban implicate employee privacy concerns and possibly, given the addictive nature of pornography, accommodation under the American with Disabilities Act. Thus, human resource managers, when crafting employee Internet use policies, must also be cognizant of the potential liability associated with the policy's administration.

Common Law Privacy Issues

Once a ban on accessing Internet pornography is in place, it needs to be enforced. This, of course, entails some type of employee monitoring. The bad news for employers is that the law affords employees several vehicles for challenging monitoring: the good news is that the law and the courts clearly favor employers in this area.

First, in common law (judge-made law that varies by jurisdiction) there exists what is called an "invasion of privacy tort." One violates this privacy right, according to the Restatement (Second) of Torts, when one "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another [or] his personal affairs or concerns" and "is subject to liability to the other for invasion of privacy if the intrusion would be highly offensive to the reasonable person" [22]. Whereas workplace invasion of privacy suits were virtually nonexistent before 1980, such litigation accelerated and because commonplace over the next decade [23]. Today, employers are routinely required to answer allegations of invasions of privacy not only for monitoring and surveillance, but also for employee

searches, drug testing, electronic mail interception, phone-tapping, and inquiry into off-duty conduct.

Generally, when assessing an alleged privacy violation, a court will ask three specific questions:

1. did some type of intrusion occur?
2. did the employee have an expectation of privacy? and
3. was the intrusion "highly offensive to the reasonable person?"

With regard to monitoring, employees typically have little difficulty establishing that there was an intrusion. Clearly, the employer is watching them and that is why this issue is being litigated in the first place. The second question is a bit more involved. In the workplace, employees have every right to expect that some activities, such as use of the bathroom, will remain private, whereas other activities, such as interacting with coworkers in a work area, will not. One expects that articles kept in a desk or a locker are private, whereas articles stored in public view or carried across a room are not. In addressing this question of employee privacy expectations, the U.S. Supreme Court in *O'Connor v. Ortega* held that "not everything that passes through the confines of the business address can be considered in the workplace context" [24]. That is, some employee items and activities are beyond the scope of employer monitoring. Federal appellate courts have clarified that the contents of one's desk or locker are among these areas where employees have an expectation of privacy [25, 26]. However, neither common law or statutory law says that employees have any expectation of privacy in work areas, parking lots, lobbies, or just about any place at work other than a bathroom or changing room. Accordingly, employers may monitor employee activities in these areas.

Even where an employee does have an expectation of privacy, monitoring is not necessarily precluded. Criterion three above, examined only when a privacy expectation exists, recognizes there are degrees of offensiveness to employer intrusions. The reasonable person would not be "highly offended" by the monitoring of this person's cubicle, but would be "highly offended" by the monitoring of a changing room [27] or the search of a private locker where the individual's own lock was used to secure it [28]. Furthermore, legitimate business reasons for the monitoring may further reduce the offensiveness of the intrusion [29]. Where monitoring exists in support of a business objective (e.g., increasing productivity, assessing training needs, or curtailing on-site drug use), courts are less likely to conclude that the reasonable person would be highly offended by it.

Applying this analysis to the monitoring of Internet use, there is an employer intrusion, but if the computer is company property and is located in a work area, the employee has little expectation of privacy. This expectation could be further reduced, and probably eviscerated altogether, with a clear, well-circulated policy informing employees that Internet access is for business purposes only and that the employer reserves the right to monitor electronic transmissions. Lastly, even

if the invasion-of-privacy allegation were to survive this second step, the legitimate business reasons for the monitoring—productivity and minimizing sex discrimination—should surmount any claim of offensiveness to the reasonable person. Thus, in the current legal environment, monitoring employee internet use, if done properly, should not expose employers to liability for tortious invasion of privacy.

Statutory Law Privacy Issues

Employees may also attempt to challenge an employer ban on recreational use of the Internet through federal and state statutes. In particular, the federal Electronic Communications Privacy Act of 1986 (ECPA) [30] may be implicated by employer interception/monitoring of what employees are viewing on the Internet. The ECPA was written to protect the privacy of electronic messages but, at present, it is still not clear whether Internet activity and electronic mail interception is covered by the act. However, employers can insulate themselves from liability here if they take advantage of "business purpose" and "prior consent" exceptions in the law: electronic communications can be monitored by employers to the extent that such monitoring is a "necessary incident" to the provision of service or where an employee has consented to the monitoring [31]. This means employers can avoid liability under the ECPA if they own the computer being used, if they notify employees that company-owned computers are subject to inspection, and if they notify employees that Internet access is provided for business purposes only [32].

Many states have also passed laws regulating the interception of electronic communications, but most include the ECPA's business purpose and prior consent exceptions [29, 33]. Because some of these statutes are marginally more prohibitive than is the ECPA, the prudent employer may want to supplement the notification requirements above by mandating that employees sign an explicit consent form. Human resource managers should inquire with their state department of labor for specifics on an employer's obligation in their jurisdiction.

Constitutional Privacy Issues

The U.S. and state constitutions codify privacy rights that are broader than those available in common law. Thus, when attempting to implement and enforce Internet use policies, public employers (and some private employers, as detailed below) are subject to greater scrutiny than are their private sector counterparts.

The public employee's constitutional right to privacy at work is not absolute. Rather, in public employee privacy cases, courts seek to balance an employer's interest in supervision, control, and efficiency with an employee's expectation of privacy. Where legitimate interests exist on both sides, courts will often permit the privacy invasion if the monitoring or search is "reasonable." This is best exemplified by U.S. Supreme Court decisions involving public employee drug

testing [34, 35]. In these cases, the Court held that because searches of employee urine were performed under controlled, laboratory conditions and because test results were not used for criminal prosecution of employees, the search was deemed "reasonable" under the Fourth Amendment. Notwithstanding the clear employee expectation of privacy in something as private as one's bodily fluids, the employer's legitimate need to test in tandem with the reasonableness of the search rendered the drug test constitutionally permissible. Presumably, then, less intrusive measures such as computer monitoring should also withstand constitutional scrutiny provided the results are not used for prosecutorial purposes. Public employers who have a business need to monitor, who notify employees of the monitoring (thereby reducing their expectation of privacy), and whose remedy for policy violations does not extend beyond employee termination will thereby satisfy their constitutional obligations in this area [36].

Internet monitoring policies of private sector employers in California, New Jersey, and Massachusetts may also be scrutinized under this stricter public sector framework. Since 1976, protections of the California Constitution, including its privacy provisions, have been extended to private sector employees [37]. Similarly, the New Jersey Supreme Court has suggested that the privacy rights articulated in the state constitution may sometimes apply to private sector employees [38]. Also, the Massachusetts Civil Rights Act has created a cause of action for individuals whose constitutionally protected rights are infringed upon by any other individual, including private employers [39]. Accordingly, private sector employers in these three states should adhere to the more stringent public sector model in monitoring employees for recreational Internet use.

Disability Discrimination

Lastly, discipline or termination of an employee who violates the organization's no-pornography policy may implicate the Americans with Disabilities Act (ADA) and its state-level complements because of the addictive effects of viewing pornography. Consequently, human resource managers may need to consider possible accommodations for this "disability" before taking any adverse action against the policy offender.

A significant body of research has developed to demonstrate the addictive nature of pornography. Many of the central findings are summarized by McGaugh, who concluded that sexual arousal experiences become locked into the brain by the chemical epinephrine and become virtually impossible to erase [40]. Graphic and vivid memories are then replayed in the mind and call one back to view more pornography. Along these same lines, former Surgeon General C. Everett Koop noted in 1985 that pornography is a "serious contributing factor to certain disorders of human health" [41]. Seemingly, then, a case can be made that an employee who is accessing Internet pornography may be a disabled employee.

However, in light of an explicit exception in the ADA, it is not clear whether such an employee is protected under the Act. Among the many conditions specifically excluded from the definition of disability in the ADA [42] is "voyeurism," which may encompass addiction to pornography. To date, no court has reached this issue.

Of clearer concern to employers may be the state laws that parallel the ADA, since some of these laws do not enumerate such exceptions. One such example is Florida, where it was held in 1992 that transexuality, a condition specifically excluded by the ADA, constituted a disability under the Florida human rights law. In particular, the human rights commission in this administration decision stated that "transsexualism meets Florida's definition of handicap (since it is a) medically cognizable condition with a prescribed course of treatment" [43, p. A7]. No doubt the same could be said for addiction to pornography. Therefore, even if an employer is not obligated to seek an accommodation for Internet policy violators under the ADA, the employer may have an obligation under a more liberal state law. Human resource managers should consult their state human rights agency to ascertain the parameters of their responsibilities here.

CONCLUSION AND SUMMARY

The Internet is rapidly becoming one of the most important business tools of the 1990s, as it affords organizations almost limitless potential to gather and supply information. However, it has also presented human resource managers with yet another legal minefield to navigate. The following is a summary of how an organization can minimize the employee lawsuits and liability that accompany recreational use of this new technology.

First, organizations that furnish employees with access to the Internet should create an Internet-use policy stating that 1) the computers are owned by the organization and subject to inspection, 2) Internet access is restricted to business use only, and 3) recreational use is strictly prohibited.

Second, to avoid liability under state and federal communication interception statutes, employees should be required to sign a document that establishes their explicit consent for the employer to monitor electronic communications. Employers should also inquire with their state's department of labor regarding the specific boundaries of permissible communication interception in their jurisdiction.

Third employers should amend their sexual harassment policies to include among the proscribed activities viewing Internet or other pornography, using sexually explicit screen savers, and possession of any pornographic material.

Fourth, if an employee is found to have violated the Internet-use policy, investigate whether this employee may be addicted to pornography. If there is any evidence of an addiction, the employer may, under state or federal disability discrimination law, have an obligation to seek a reasonable accommodation

before taking any action against the offender. Employers should check with their state human rights agency to determine whether pornography addiction qualifies as a disability in their state.

Fifth, in light of constitutions and other statutes, public sector employers and private employers in California, New Jersey, and Massachusetts should not use results of any employee monitoring for prosecutorial purposes.

Lastly, employers may find it useful to purchase and install software that prevents Internet users from accessing sexually explicit material. Such software, originally designed for parents, generally sells for under $100. Among the more popular packages are Cyber Patrol, Surf Watch, CYBER Sitter, Net Nanny, Parental Guidance, Internet Filter, and Web Track.

* * *

Michael A. Zigarelli currently teaches courses in human resource management, labor relations, employment law, and quantitative methods at Fairfield University in Connecticut. His research primarily focuses on employee representation and he specializes in employment law and ethical treatment of workers. Dr. Zigarelli's articles have appeared in numerous professional journals. He is also the author a of book entitled *Can They Do That? A Guide To Your Rights On The Job.*

ENDNOTES

1. See, "New Workplace Issue: On-Line Sex Sites," *The New York Times*, June 27, 1996, p. C1.
2. This section is a synopsis of a much more detailed explanation written by district court judges Sloviter, Buckwalter and Dalzell in the case *American Civil Liberties Union v. Reno* 929 F.Supp. 824 (1996). In deciding whether the federal Communications Decency Act (CDA), an act regulating the content of the Internet, was constitutional, the court researched and wrote an extraordinary lay-language primer on the Internet as part of its decision to strike down the CDA.
3. An October 1995 Nielsen study of Internet use in the U.S. and Canada concluded that 54 percent of Internet users had connections at their workplace. An executive summary of this report, "The Commercenet/Nielsen Internet Demographics Survey," is available on-line at http://www.nielsenmedia.com/commercenet/exec_sum.html
4. M. Rimm, Marketing Pornography on the Information Superhighway, 83 *Georgetown Law Journal*, p. 1849, 1995.
5. F. M. Osanka and S. L. Johann, *Sourcebook on Pornography*, Lexington Books, Lexington, Massachusetts, 1989.
6. D. Zillman, Effects of Prolonged Consumption of Pornography, in *Report to the Surgeon General's Workshop on Pornography and Public Health*, E. P. Mulvey and J. H. Haugaard (eds.), U.S. Public Health Service and U.S. Department of Health and Human Services, Washington, D.C., 1986.
7. D. Scott, *Pornography—Its Effects on the Family, Community and Culture*, Free Congress Foundation, Washington, D.C., 1985.

8. D. Zillman and J. Bryant, Effects of Massive Exposure to Pornography, in *Pornography and Sexual Aggression*, N. M. Malamuth and E. Donnerstein (eds.), Academic Press, New York, 1984.
9. D. Zillman and J. Bryant, Pornography, Sexual Callousness, and the Trivialization of Rape, *Journal of Communication, 32*, pp. 10-21, Autumn 1982.
10. *Attorney General's Commission on Pornography, Final Report*, U.S. Department of Justice, Washington, D.C., 1986.
11. V. B. Cline, *The Effects of Pornography on Human Behavior*, Testimony before the Attorney General's Commission on Pornography, Houston, Texas, September 11, 1985.
12. *Robinson v. Jacksonville Shipyards, Inc.*, 760 F.Supp. 1486 (M.D. Fla. 1986).
13. A few cases not related to harassment also demonstrate that courts may accept the argument that pornography leads to discrimination. A federal appellate court, in its examination of an Indianapolis antipornography statute, acknowledged a linkage between pornography and harm to women, but still found the law to be unconstitutional (*American Booksellers Association v. Hudnut* [14]. Similarly, the Canadian Supreme Court in *Butler v. Her Majesty the Queen* [15] upheld Canada's anti-obscenity statute, concluding that pornography affects men's behavior and erodes women's self-esteem and integrity. Although the United States Supreme Court has not reached the question of this linkage, it has held that child pornography is harmful to children (*New York v. Ferber*) [16]. It would not be surprising, therefore, if it were to extend this logic to sexually explicit pictures of women.
14. *American Booksellers Association v. Hudnut* (771. F.2d 323 (7th cir. 1985), aff'd without opinion 475 U.S. 1001 (1986).
15. *Butler v. Her Majesty the Queen*, 1 S.C.R. 452 (1992 Canada).
16. *New York v. Ferber*, 458 U.S. 747 (1982).
17. *Rabidue v. Osceola Refining Co.*, 805 F.2d 611 (6th cir. 1986).
18. *Rabidue v. Osceola Refining Co.*, 584 F.Supp. 419 (E.D. Mich. 1984).
19. *Johnson v. County of Los Angeles*, 865 F.Supp. 1430 (C.D. Cal. 1994).
20. *Andrews v. City of Philadelphia*, 895 F.2d 1469 (3rd cir. 1990).
21. *Waltman v. International Paper Co.*, 875 F.2d 468 (5th cir. 1989).
22. Restatement (Second) of Torts § 652B (1977).
23. D. F. Linowes and R. C. Spencer, Privacy: The Workplace Issue of the '90s, Vol. 23 *John Marshall Law Review*, pp. 591-620, 1990.
24. *O'Connor v. Ortega*, 480 U.S. 709 (1987).
25. *Schowengerdt v. United States*, 944 F.2d 483 (9th cir. 1991) cert. denied 112 S.Ct. 1514 (1992).
26. *American Postal Workers Union v. U.S. Postal Service*, 871 F.2d 556 (6th cir. 1989).
27. *Doe v. B.P.S. Guard Services, Inc.*, 945 F.2d 1422 (8th cir. 1991).
28. *K-Mart v. Trotti*, 677 S.W.2d 632 (Tex. Ct. App. 1984).
29. L. T. Lee, Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop', 28 *John Marshall Law Review*, pp. 139-177, 1994.
30. 18 U.S.C. §§ 2510-2522 and 18 U.S.C. §§ 2701-2710.
31. 18 U.S.C. § 2511(2)(a)(i).
32. D. J. P. MacKensie, Commerce on the Net: Surfing through Cyberspace without Getting Wet, 14 *John Marshall Journal of Computer and Information Law* 247, 1996.

33. As of 1994, the following states had passed such laws: Arizona, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Louisiana, Maryland, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Virginia, West Virginia, Wisconsin, and Wyoming.
34. *National Treasury Employees Union v. Von Raab*, 109 S.Ct. 1384 (1989).
35. *Skinner v. Railway Labor Executives' Association*, 109 S.Ct. 1402 (1989).
36. M. A. Zigarelli, Random Drug Testing in the Public Sector: The Legal Parameters, *Employee Relations Law Journal, 17*:3, pp. 459-471, 1992.
37. *Porten v. University of San Francisco*, 139 Cal. Rptr. 839 (1976).
38. *Hennessey v. Coastal Eagle Point Oil Company*, 609 A.2d 1 (N.J. 1992).
39. Massachusetts Civil Rights Act, G.L. c.12 (1992).
40. J. L. McGaugh, Preserving the Presence of the Past: Hormonal Influence of Memory Storage, *American Psychologist, 38*, pp. 161-174, 1983.
41. C. Everett Koop, Remarks to the National Conference on Pornography, Denver, Colorado, May 31, 1985.
42. 29 C.F.R. § 1630.2g excludes from the definition of disability homosexuality, bisexuality, transvestism, transexuality, pedophilia, exhibitionism, voyeurism, gender identity disorders not resulting from physical impairments, other sexual behavior disorders, compulsive gambling, kleptomania, pyromania, and psychoactive substance abuse disorders resulting from current illegal drug use.
43. *Daily Labor Report*, Jacksonville, Fla. Approves Reinstatement of Fired Transsexual, March 8, 1993.

Direct reprint requests to:

Michael A. Zigarelli
School of Business
Fairfield University
Fairfield, CT 06430