



OKLAHOMA CITY UNIVERSITY LAW REVIEW

VOLUME 29

NUMBER 1

SPRING 2004

DEDICATION

IN MEMORIAM OF SILAS ROBERT (BOB) LYMAN I

Professor Emeritus Silas Robert (Bob) Lyman I 1932-2004
Memorial to Bob Lyman
In Memoriam: Silas Robert Lyman I
Fond Memories of Bob Lyman
A Tribute for Silas R. (Bob) Lyman I

Vicki Lawrence MacDougall
Dean Lawrence K. Hellman
Dennis W. Arrow
Daniel Morgan
Vicki Lawrence MacDougall

EMPLOYMENT AND LABOR LAW

The Workplace Privacy Myth: Why Electronic Monitoring Is Here to Stay

Leonard Court
Courtney Warmington

Gratz v. Grutter: Lessons for Pursuing Diversity in the Workplace

Allan G. King
Jeremy W. Hawpe

Split Decisions: The Lack of Consensus on Disparate Impact Claims Under the Age Discrimination in Employment Act

Joel S. Allen
Melissa M. Hensley
Scott Sherman

Three Steps Forward in the Continuing Search for the Parameters of the Public Policy Exception to the At-Will Employment Doctrine in Oklahoma: *Wilburn v. Mid-South Health Development, Inc.*, *Barker v. State Insurance Fund*, and *Crain v. National American Insurance Co.*

David W. Lee

In Search of *Wiley*: Struggling to Bind Successor Corporations to Their Predecessor's Collective Bargaining Agreement

Jared S. Gross

Culture Shock in the Workplace: The Legal Treatment of Cultural Behavior Under Title VII

Darryll M. Halcomb Lewis
James R. Jones

ARTICLES

September Eleventh, The ABC's of a Citizen's Responses: Explorations

George Anastaplo

The Trillion-Round Revolver: Problems in the Scope and Limit of Substance, Likelihood and Probability in Contemporary Reckless Homicide Law

Rhys Brendan Cartwright-Jones

Mitigation of Psychological Damages: An Economic Analysis of the Avoidable Consequences Doctrine and Its Applicability to Emotional Distress Injuries

Kevin C. Klein
G. Nicole Hinger

VIGNETTE

Vignette

Von Russell Creel

SPEECHES

The Power of Words

Hon. Nancy L. Coats

Oklahoma City University Law School May 11, 2003 Commencement Address

Hon. Lee R. West

COMMENT

Andrade v. Attorney General of California: Gross Disproportionality in Sentencing – A Standard for Reviewing Eighth Amendment Challenges on Cruel and Unusual Punishments

Michael A. Trevino

OKLAHOMA CITY UNIVERSITY LAW REVIEW

VOLUME 29

SPRING 2004

NUMBER 1

EMPLOYMENT AND LABOR LAW

THE WORKPLACE PRIVACY MYTH: WHY ELECTRONIC MONITORING IS HERE TO STAY

LEONARD COURT*
COURTNEY WARMINGTON**

I. INTRODUCTION

Vast numbers of employers across the country admit to having some form of employee monitoring. To understand why, one need only look at the statistics of Internet and e-mail misuse by workers and the liability it is creating. Yet the topic continually sparks a debate about the privacy rights of employees, who often mistakenly believe the web sites they visit and the e-mail messages they send and receive are confidential. The line separating the purely private conduct of employees from the conduct that employers have legitimate grounds to monitor and regulate is, through developing technology and case law, shifting day-by-day.

This article examines several aspects of the legal challenges involved in monitoring employees' use of computers. First, this article examines why employers are monitoring, including an overview of the types of cases being brought against employers, as well as issues surrounding employee productivity. Second, it discusses the privacy laws implicated by monitoring and proposed legislation which would offer greater protection to employees. Third, this article gives guidelines on how employers can safely implement procedures that balance their monitoring needs with their employees' expectation of privacy. Finally, this article addresses emerging issues involving e-mail in the labor union context.

* Leonard Court is a graduate of Oklahoma State University (B.A., 1969) and Harvard Law School (J.D., 1972) and joined Crowe & Dunlevy Law Firm in Oklahoma City, Oklahoma, in 1972. Mr. Court is chairman of the Firm's Labor and Employment Law Section. He is a past Chairman of the Labor and Employment Law Section of the

II. WHY EMPLOYERS MONITOR

A. Internet and E-mail Abuse

A two-year study by Alexa Research demonstrated that "sex" was the most popular search term on the Internet.¹ "Porn" was the fourth

Oklahoma Bar Association, and is currently a member of the Equal Employment Opportunity Committee Section on Labor and Employment Law. Mr. Court has served as a member of the United States Chamber of Commerce Labor Relations Committee since 1997. In 1999, he was appointed chairman of the Wage, Hour and Leave Subcommittee and is a member of the steering committee of the Labor Relations Committee of the United States Chamber of Commerce. Mr. Court is a Fellow of the American College of Labor and Employment Lawyers. He serves as an adjunct professor of labor law at the University of Oklahoma Law School and Oklahoma City University School of Law. He is a former president of the Oklahoma State University Alumni Association. He received that organization's Distinguished Alumni Award in 1998.

Mr. Court has served as Chairman of the board of elders and member of the Memorial Christian Church, Oklahoma City, 1980-2000; co-chairman of sustaining fund raising drive for Oklahoma City downtown YMCA, 1989, member of board of management, 1994-96; participant of Leadership Oklahoma City, 1987-88; Oklahoma City Ronald McDonald House, 1990-93, member executive committee 1991-93; co-chairman of the annual teleparty fund raising drive American Heart Assn., Oklahoma City, 1996-98, board of directors 1996-98; Oklahoma State University Alumni Association Board of Directors 1992-present, president 1995-1996; Oklahoma State University Foundation Board of Governors, 1990-2002.

Mr. Court is listed in *Who's Who in America*, *Who's Who in American Law*, *Guide to Leading U.S. Labor and Employment Lawyers* and *The Best Lawyers in America* (Labor and Employment Law).

Mr. Court is listed in the "star" category among management labor and employment lawyers as listed in *Chambers, USA America's Leading Business Lawyers 2003-2004*.

** Courtney Warmington is a graduate of Oklahoma State University (B.A. in Public Relations, 1995) and Oklahoma City University School of Law (J.D., magna cum laude, 1999). She joined the law firm of Crowe & Dunlevy in Oklahoma City, Oklahoma, in 1999. While attending law school, she was a member of Phi Delta Phi, Order of the Barristers, Moot Court Honors Board, was the Merit Scholars Organization President and also served as Articles Editor of the Oklahoma City University Law Review. Ms. Warmington was the recipient of many awards and honors, including: the CALI Award for Legal Research and Writing I; Oklahoma City University Intramural Moot Court Competition Best Oralist, 1998; and the Hatton Summers Foundation Academic Scholarship. She is currently a member of the Labor and Employment Law Section of the Oklahoma Bar Association and serves on the Board of the Oklahoma City University School of Law Alumni Association as well as the Central Oklahoma Chapter of the Oklahoma State University Alumni Association. She has previously served as Secretary for the Board of the Young Lawyers Division of the Oklahoma County Bar Association, and has previously served on the Oklahoma Bar Association Ethics Committee. Ms. Warmington focuses her practice in the areas of litigation and labor and employment law.

1. *Alexa Research Finds Many People Inefficient at Reaching Their Online*

most-searched term, followed by "Nude," "XXX," "Playboy," and "Erotic Stories," all of which were in the top twenty most-searched list.² Think these terms are being searched in the privacy of one's home? Think again. According to Websense Enterprise, an Internet management business, 70% of all Internet porn traffic occurs during the 9:00 a.m. to 5:00 p.m. workday.³ In one survey, more than 60% of companies report having disciplined employees, and more than 30% having terminated employees, for inappropriate use of the Internet.⁴ Some employee misuse makes headlines, such as the firing of fifty workers and the suspension of 200 more at Dow Chemical Company for sending and storing pornographic and/or violent e-mail messages.⁵ In December 1999, the New York Times terminated over twenty employees for sending inappropriate and offensive e-mail messages.⁶ The *Wall Street Journal* reports that employees of IBM, Apple Computer, and AT&T were among the most frequent visitors to *Penthouse Magazine's* website, spending the equivalent of over 347 eight-hour days in a single month.⁷

Internet misuse is not, of course, limited to the private sector. A study by the Internal Revenue Service revealed that many of its employees viewed sexually explicit websites.⁸ Internet misuse by employees was uncovered at the Departments of Commerce and Housing and Urban Development and even former White House administrations.⁹ In fact, Internet misuse is becoming so commonplace that many psychologists are specifically devoted to helping persons overcome web addictions.¹⁰

Destinations at <http://www.internetindustry.com/News/Archives/February01/21401> (February 14, 2001).

2. *Id.*

3. Surprising Internet Statistics, available at <http://www.websense.com/company/news/stats.cfm> (last visited Jan. 12, 2003).

4. *Internet Usage In The Workplace*, at <http://www.n2h2.com/pdf/usagestats.pdf> (last visited Jan. 13, 2003).

5. *Dow Chemical Fires 50, Suspend 200 Workers for Sending, Storing Offensive E-Mail Messages*, 51 BNA, Inc. Bulletin to Management 243 (Aug. 3, 2000).

6. Matthew H. Meade, *I've Got My Eye on You: Workplace Privacy in the Electronic Age*, 632 P.L.I./PAT 459, 462 (2001).

7. *United States v. Rowland*, 145 F.3d 1194, 1217, n.7 (10th Cir. 1998).

8. *Significant Misuse of Internet Found at IRS*, at <http://hpl.blr.com/Article.cmf/Nav/5.0.0.0.27706> (last visited Jan. 12, 2003).

9. Paul Sperry, *Cyberporn Scandal Hits Commerce Department, Personnel Security Officer Suspended; Follows HUD, White House Abuses*, at http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=20766 (Sept. 27, 2000).

10. See, e.g., The Center for Online Addiction, at <http://www.netaddiction>.

B. Productivity Issues

Even if employees are not viewing inappropriate or offensive websites at work, they are likely spending time looking at other non-work related sites. According to a survey by Vault.com, 25.1% of employees admitted to spending ten to thirty minutes a day surfing non-work-related sites, 11.9% admitted to spending one to two hours a day, and an astonishing 12.6% spent over two hours a day surfing non-work-related sites.¹¹ Many employees report using the Internet to read the news each day, make travel arrangements, check stocks, and to shop for gifts.¹² Indeed, according to a survey conducted in November of 2000, respondents admitted to spending between a half day to two days per week shopping on the Internet for holiday gifts.¹³ E-mail is also a productivity culprit, with half of the employees surveyed admitting to sending and/or receiving one to five non-work-related e-mails each workday.¹⁴ The impact on businesses can be enormous. It has been estimated that a company with 500 Internet users could lose almost a million dollars in productivity annually from just a half hour of daily Internet surfing by employees.¹⁵

C. Employer Liability

A survey recently reported, of those employers who monitor employees' e-mail and Internet use, 68% cite legal liability as their

com/workplace (last visited May 14, 2004).

11. *Results of Vault.com Survey of Internet Use in the Workplace*, Fall 2000, at <http://www.vault.com/surveys/internetuse2000/results2000.jsp;jsessionid=C1EF7C8DD006DFF050F4ED89B2D7B236?results=2&image=employee> (last visited May 15, 2004).

12. *Results of Vault.com Survey of Internet Use in the Workplace*, Fall 2000, at <http://www.vault.com/surveys/internetuse2000/results2000.jsp;jsessionid=C1EF7C8DD006DFF050F4ED89B2D7B236?results=12&image=employee> (last visited May 15, 2004).

13. Denise F. VanHouten, *Surfing and Shopping on Company Time*, 20 *Employment Alert* No. 5, 5 (February 27, 2003).

14. *Results of Vault.com Survey of Internet Use in the Workplace*, Fall 2000, at <http://www.vault.com/surveys/internetuse2000/results2000.jsp;jsessionid=C1EF7C8DD006DFF050F4ED89B2D7B236?results=3&image=employee> (last visited May 15, 2004); *Results of Vault.com Survey of Internet Use in the Workplace*, Fall 2000, at <http://www.vault.com/surveys/internetuse2000/results2000.jsp;jsessionid=C1EF7C8DD006DFF050F4ED89B2D7B236?results=4&image=employee> (last visited May 15, 2004).

15. See Productivity Chart, 8e6 Technologies, at http://xstop.com/prod_calc.htm (figures were calculated based on an average salary of \$25,000 per year) (last visited August 9, 2004).

primary motivation.¹⁶ While no court has ever ruled that an employer must monitor electronic communications, several have indicated that such monitoring would be wise. Indeed, one federal circuit court judge recently opined that “the abuse of access to workplace computers is so common . . . that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.”¹⁷ The rise in the number of lawsuits against employers for employee misuse of the Internet and e-mail only furthers this point. One of the most costly examples of employer liability was a reported \$2.2 million settlement by Chevron of a sexual harassment lawsuit involving, in part, an Internet message entitled “Why Beer Is Better Than Women.”¹⁸ However, sexual harassment lawsuits are not the only concern. Other types of “cyberliability” have arisen, including racial and other forms of discrimination. The following cases illustrate this point.

In *Blakey v. Continental Airlines*, the New Jersey Supreme Court confronted the issue of whether an employer could be held liable for sexual harassment that occurs via communications made through the Internet.¹⁹ At issue was the “Crew Members Forum,” an on-line electronic bulletin board which was used by Continental pilots and crews to post messages and communicate with one another.²⁰ The plaintiff, a female pilot for Continental, alleged that the Forum had been used to publish derogatory gender-based messages about her in the middle of a federal lawsuit she had filed against the airline involving claims of sexual discrimination.²¹ When the on-line messages were discovered, the

16. 2001 AMA SURVEY, WORKPLACE MONITORING & SURVEILLANCE: POLICIES AND PRACTICES (AMERICAN MANAGEMENT ASSOC. 2001), at http://www.amanet.org/research/pdfs/emsfu_short.pdf.

17. *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002). The Tenth Circuit Court of Appeals has likewise said “[w]ith the advent of the ‘information superhighway,’ companies are faced with the dilemma created by Internet access for their employees: Companies must balance the beneficial access to data with the detrimental and suspect access to pornography or other inappropriate personal uses.” *United States v. Rowland*, 145 F.3d 1194, 1217 n.7 (10th Cir. 1998).

18. See Mark S. Dichter & Michael S. Burkhardt, *Electronic Monitoring in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, 42 (June 1999) at http://www.morganlewis.com/pubs/A5C845ED-575B-4ADC-8A47F280IDC3594C_Publications.pdf.

19. *Blakey v. Continental Airlines, Inc.*, 751 A.2d 538 (N.J. 2000).

20. *Id.* at 544.

21. *Id.* The allegations of sex discrimination in the federal lawsuit included claims that the plaintiff was subjected to pornographic photographs and vulgar gender-based comments in violation of Title VII. *Id.* at 543-44. Plaintiff also asserted a claim of retaliation. *Id.* at 543-44.

plaintiff brought a state court action against her co-employees for defamation, as well as against the airline for a hostile work environment arising from the allegedly defamatory statements.²²

The trial court granted Continental's motions to dismiss and for summary judgment, and the plaintiff appealed.²³ The appeals court affirmed, finding that Continental "was not vicariously liable for defamatory statements by . . . [Continental] pilots."²⁴ It further found that because Continental did not require employees to access the bulletin board, and because employees bore the cost of using the board, Continental was not liable under the doctrine of respondeat superior.²⁵

The New Jersey Supreme Court reversed and remanded, holding that although employers are not specifically required to monitor their employees' communications, employers do have a duty to try to stop employee harassment when the employer knows or has reason to know that such harassment is occurring in the workplace.²⁶ One wonders, was this alleged harassment over the Internet "in the workplace?" The evidence established that the only way pilots were able to access the electronic bulletin board was through a personal computer and modem accessed through the airline's contracted Internet service provider, CompuServe.²⁷ Nevertheless, the court found no difference between a "bulletin board" on the Internet and an actual bulletin board in the pilot's lounge. The court noted:

the fact that the electronic bulletin board may be located outside of the workplace (although not as closely affiliated with the workplace as was the cockpit in which similar harassing conduct occurred), does not mean that an employer has no duty to correct off-site harassment by co-employees. Conduct that takes place outside the workplace has a tendency to permeate the workplace.²⁸

However, the court stated that it was unclear in this case whether the Forum "was such an integral part of the workplace that harassment on the Crew Members Forum should be regarded as a continuation or

22. *Id.* at 547.

23. *Id.*

24. *Id.* at 548.

25. *Id.*

26. *Id.* at 552.

27. *Id.* at 544-45.

28. *Id.* at 549.

extension of the pattern of harassment that existed in the Continental workplace."²⁹ The court remanded this issue to the lower court.³⁰ The court suggested that the trial court should first determine whether Continental obtained a substantial workplace benefit from the overall relationship with CompuServe (noting that the record did not contain Continental's contract with CompuServe), the number of current users of CompuServe services, and whether Continental sought the inclusion of the Forum in the services provided by CompuServe.³¹

Employers may face liability not only for what is said over the Internet, but also for what is seen. For example, in May of 2001, the Equal Employment Opportunity Commission determined that Minneapolis public librarians were subjected to a sexually hostile work environment when they were exposed to hard-core pornography left on the computers by library patrons.³² In another instance, a female employee sued her employer for allegedly creating a "hostile work environment by, among other things, forcing her to look at sexually explicit materials on the Internet."³³ Many other examples of this type of liability exist.³⁴

An example of potential liability for racial discrimination arising from workplace e-mail was illustrated by *Owens v. Morgan Stanley & Co., Inc.*³⁵ In *Owens*, two African American employees of Morgan Stanley brought suit for racial discrimination, and retaliation based upon the company's alleged treatment of them after they complained about an

29. *Id.* at 550.

30. *Id.* at 558-59.

31. *Id.* at 551-52.

32. Nancy Montwieler, *EEOC Finds Minneapolis Librarians Faced Hostile Environment Because of Internet Porn*, BNA, Inc., Daily Labor Report at A-9 (May 29, 2001).

33. Meade, *supra* note 6, at 462.

34. See e.g., *Autoliv ASP, Inc. v. Dept. of Workforce Servs.*, 29 P.3d 7, 12 (Utah Ct. App. 2001) (noting that potential employer liability for employee misuse of Internet and e-mail is increased by the fact that this type of material can be viewed inadvertently by others as it is displayed on a computer screen); see also *Dichter & Burkhardt*, *supra* note 18, at 42 (citing *Trout v. City of Akron*, No. 97-115879 (Dec. 15, 1998) (Ohio Ct. of Comm. Pleas) (noting that an Ohio jury "found that a female employee was sexually harassed . . . because she could see pornographic pictures that her male co-worker had downloaded off the Internet"); *Luttrell v. O'Connor Chevrolet, Inc.*, No. 01 C 979 2002, WL 1263990, at *4 (N.D. Ill. June 5, 2002) (denying summary judgment on sexual harassment claim where employees testified as having been continually exposed to, among other things, pornography on their co-worker's computer).

35. No. 96 CIV. 9747, 1997 WL 793004 (S.D.N.Y. Dec. 24, 1997).

e-mail message containing racist jokes.³⁶ The employees claimed that after complaining internally about the offending e-mail, they were professionally isolated, threatened with termination if they filed a legal complaint, and passed over for promotions.³⁷ The *Owens* case was ultimately settled after the federal court judge ruled that the amended employment discrimination claims could proceed.³⁸ Similar claims were raised against Citibank in *Curtis v. DiMaio*, a lawsuit involving a Polish joke and a joke about Ebonics.³⁹ Although *Curtis* was dismissed under the particular facts of the case, it serves as another reminder of the potential liability that exists.⁴⁰

III. THE STATE OF THE LAW GOVERNING E-MAIL AND INTERNET PRIVACY

When defining the contours of an employee's right to privacy in the workplace, it must first be determined whether the employer is a government agency or a privately owned operation. As discussed below, when the government employs, it must honor the constitutional rights to privacy enjoyed by its employees when searching employee work space or taking other actions which may infringe upon its employees' constitutional rights to privacy, such as monitoring e-mail and Internet usage. In contrast, neither the United States Constitution nor most state constitutions establishes rights of privacy for employees of private employers.⁴¹

36. *Id.* at *1.

37. *Id.*

38. See Dichter & Burkhardt, *supra* note 18, at 41.

39. *Curtis v. DiMaio*, 46 F. Supp. 2d 206 (E.D.N.Y. 1999).

40. *Id.* at 213. See also, *Daniels v. WorldCom Corp.*, No. CIV. A-3:97-CV-0721-P.1, 1998 WL 91261 (N.D. Tex. Feb. 23, 1998), a lawsuit involving claims of racially discriminatory e-mails. The case was ultimately dismissed for failure to exhaust administrative remedies. *Id.* at *3-4.

41. *O'Connor v. Ortega*, 480 U.S. 709, 719 (1997) ("the Fourth Amendment applies to searches conducted by [public employers]"); *Gilmore vs. Enogex, Inc.*, 878 P.2d 360, 365 (Okla. 1994) ("[t]he constitutional right of privacy affords protection against governmental intrusions and is not enforceable against private individuals or corporations . . ."). However, it is important to note that the Fourth Amendment may be implicated for private employers who search pursuant to governmental regulations or essentially act as governmental bodies. See Dichter & Burkhardt, *supra* note 18, at 19 (citing *Skinner v. Ry. Labor Executives Ass'n.*, 489 U.S. 602, 614-16 (1989) (holding Fourth Amendment applicable to company that complied with government drug testing regulations) and *Marsh v. Alabama*, 326 U.S. 501, 508-10 (1946) (finding private corporation which acted essentially as a municipality in a company-owned town was a state actor).

A. Constitutional Protections

The Fourth and Fourteenth Amendments to the United States Constitution protect government employees from unlawful searches and seizures by the federal and state governments.⁴² Before a governmental employer may lawfully intrude upon an employee's privacy, the employer's intrusion must be reasonable.⁴³ A search is reasonable if it does not infringe upon an employee's reasonable expectation of privacy in the property searched.⁴⁴

Whether a search intrudes upon an employee's reasonable expectation of privacy must be determined on a case-by-case basis.⁴⁵ In other words, it is impossible to say that an employee's computer, desk, credenza, or other work space, may or may not be searched under any circumstances. The constitutionality of each search depends on the circumstances surrounding it.⁴⁶ When determining the constitutionality of any intrusion into employee privacy by a governmental employer, it is helpful to envision the reasons for and against the search on a large scale. Courts balance the employer's justification for the search, which may include the need for supervision, control, and the efficient operation of the workplace, against the employee's legitimate expectations of privacy in the property searched.⁴⁷ If the employer's needs for the search outweigh the employee's reasonable expectations of privacy in the property searched, then the search will be upheld as constitutional.⁴⁸ Whether an employee has a reasonable expectation of privacy in certain property, or certain areas of work space, may depend upon whether or not the work area in question is given over to the "employee's exclusive use . . . the extent to which others had access to the work space . . . the nature of the employment . . . and whether office regulations placed employees on notice that certain areas were subject to employer intrusions."⁴⁹

Under these principles, the Fourth Amendment has historically provided only limited privacy protection to governmental employees.

42. *O'Connor*, 480 U.S. at 714.

43. *Id.*

44. *Id.*

45. *Id.* at 714, 718.

46. *Id.*

47. *Id.* at 719-20.

48. *Id.*

49. *Vega-Rodriguez v. P. R. Tel. Co.*, 110 F.3d 174, 179 (1st Cir. 1997). *See also O'Connor*, 480 U.S. at 718-19.

Courts routinely give public employers discretion to search employee computers and other work areas, so long as the employer can articulate a legitimate justification for the search and show that the employee had no reasonable expectation of privacy.⁵⁰ For example, in *Bohach v. City of Reno*, the plaintiffs claimed that the City of Reno, Nevada, violated their constitutional right to privacy by intercepting messages sent between officers from their squad cars over a computerized communications system similar to e-mail.⁵¹ The court held that the officers' constitutional rights to privacy were not violated by the interception of their messages because they did not have an objectively reasonable expectation that their messages were protected from employer monitoring.⁵² Due to the manner in which the e-mail system was designed, all messages were received and stored in a central computer before being forwarded.⁵³ Thus, all messages were accessible to the employer at the central computer. Moreover, the officers could not have a reasonable expectation that their messages would remain private because the police chief had notified all e-mail users that their messages were "logged on the network" and that some messages (e.g. those violating the department's anti-discrimination policy) were banned.⁵⁴ The officers therefore, were on notice from their employer that their messages were not private.⁵⁵

Some states have constitutional provisions which also provide some privacy protection.⁵⁶ To date, only California has attempted to extend this protection to private sector employees.⁵⁷ However, this move has been called into doubt by an unpublished California Superior Court opinion, which refused to recognize constitutional protection from e-mail monitoring by private employers.⁵⁸

50. See Dichter & Burkhardt, *supra* note 18, at 17 (citing cases therein).

51. *Bohach v. City of Reno*, 932 F.Supp. 1232, 1233 (D. Nev. 1996).

52. *Id.* at 1234-35.

53. *Id.* at 1234.

54. *Id.* at 1235.

55. *Id.* at 1234-35; accord *Williams v. Philadelphia Hous. Auth.*, 826 F. Supp. 952, 954 (E.D. Pa. 1993) (employee failed to state a claim against government employer for invasion of constitutional right to privacy, when employer reviewed the contents of a computer disk left behind by former employee, since employer searched disk in pursuit of "maintaining efficiency and productivity in the workplace").

56. Lynne Bernabei, *Ethical and Legal Issues of Workplace Monitoring of Employee Communications*, April 10-11, 2003, 2003 WL 22002093, at *4.

57. *Id.*

58. *Id.*

B. Statutory Protections

1. The Electronic Communications Privacy Act

Prior to 1986, laws existed to protect the privacy of mail and voice communications,⁵⁹ but no laws existed to protect the privacy interests of persons communicating through the burgeoning use of telecommunications and computer technology.⁶⁰ To alleviate what lawmakers called a “gap” resulting in legal uncertainty, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986, to provide protection for electronic communications.⁶¹ Title I of that Act amended the Federal Wiretap Act (which previously addressed only wire and oral communications) to protect against unauthorized interception of “electronic communications.”⁶² Title II of the ECPA created the Stored Communications Act, which protects against unauthorized “access” to electronic communication while it is in electronic storage.⁶³ Civil and criminal penalties are both provided for in the Act. A successful civil plaintiff may recover the greater of either: 1) actual damages suffered and any profits made by the violator, or 2) statutory damages (the greater of \$100 a day for each day of the violation or \$10,000).⁶⁴ Attorney’s fees and costs may also be awarded.⁶⁵ Criminally, a violator may be punished with up to five years imprisonment and fines up to \$5000.⁶⁶

Despite Congress’ best efforts to catch up with technology, the ECPA is criticized for its ambiguity.⁶⁷ Part of the difficulty is attributed

59. See S. REP. NO. 99-541, at 5 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3559. The Senate Report notes that mail sent through the United States Postal Service is protected by a “combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations.” S. REP. NO. 99-541, at 5. Voice communications are protected by Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968. S. REP. NO. 99-541, at 5.

60. S. REP. NO. 99-541, at 5.

61. 18 U.S.C. §§ 2510 - 2522; 2701 - 2711 (2000).

62. S. REP. NO. 99-541, at 3.

63. 18 U.S.C. § 2701 (2000). The Wiretap Act and the Stored Communications Act have since been amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (U.S.A. Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

64. 18 U.S.C. § 2520(c)(2).

65. 18 U.S.C. § 2520(a)(3).

66. 18 U.S.C. § 2511(4)(a)-(b).

67. See *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001) (additional citations omitted). Indeed, it has been called “a complex, often convoluted, area of the law.” *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

to the fact that the Act was written prior to the advent of the Internet. Adding to the confusion is the absence of specific provisions relating to e-mail, which is transmitted and stored in much more complex ways than other forms of communication. Indeed, although the legislative history makes clear that Congress intended the Act to cover e-mail, the term "e-mail" appears nowhere in the Act. Nevertheless, courts began to apply the ECPA to monitoring in the workplace, thus seeming, at first glance, to give workers the privacy protections Congress desired. As discussed below, however, the exceptions to the Act nearly swallow the rule, making any expectation of privacy illusory under most circumstances.

2. Analysis of the ECPA and Its Exceptions

a. Interception Versus Storage

As discussed above, the ECPA has a dual role of providing protection against unauthorized interception of communications, as well as protection against unauthorized access to stored communications. The procedural and substantive requirements for each are markedly different.⁶⁸ The first question, therefore, is whether the provider has in fact "intercepted" an electronic communication. The question is not easily answered because electronic communication, such as e-mail, goes through various stages of transmittal, sometimes remaining in "intermediate storage" before it reaches the intended recipient.⁶⁹ Communications posted to electronic bulletin boards are also hard to fit neatly into the language of the Act. Despite struggling with the statute, every circuit court to consider the issue has ruled that an "interception" of electronic communication will only be found to have occurred if it takes place contemporaneously with transmission.⁷⁰ For example, two courts have held that an interception did not occur where e-mail was stored on an electronic bulletin board, even though it had not yet been read by the intended recipient.⁷¹ In another case, a court found no

68. See *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (noting that stored communications are subject to less burdensome procedures).

69. For a more detailed explanation of transmittal and storage of e-mail, see the district court's opinion in *Fraser*, 135 F. Supp. 2d at 633-34.

70. See *Fraser*, 2003 WL 22904302, at *6 (citing *Steiger*, 318 F.3d at 1048-49; *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 459-62 (5th Cir.1994); see also *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), *summarily aff'd*, 172 F.3d 861 (3d Cir. 1998).

71. See *Steve Jackson Games*, 38 F.3d at 460-61; *Konop*, 302 F.3d at 877-80.

interception when the company accessed e-mails from the company's central file server, because the access did not occur at the time of the initial transmission.⁷² Indeed, one commentator noted that when it comes to e-mail, an "interception" seldom occurs unless the provider has some type of automatic routing software, that automatically forwarded all e-mails to another person for review.⁷³

Although such instances may be rare, they are not impossible. The Court of Appeals for the First Circuit recently found a web-monitoring company in violation of the ECPA for intercepting information about Internet users contemporaneously with their web use, and thereafter forwarding such information to other interested parties.⁷⁴ In so holding, the court noted that the system used by the web-monitoring company was, in effect, an automatic routing program.⁷⁵

Both the Federal Wiretap Act and the Stored Communications Act of the ECPA contain exceptions, which, when used properly by employers, allow for monitoring in the workplace. Little case law exists interpreting the effect of the ECPA upon e-mail, but the exceptions have been interpreted by courts examining analogous forms of communication.

b. Consent Exception

The first exception is the "consent" exception, which applies when one party to the communication has given prior consent to the interception or access.⁷⁶ This exception will not apply if the interception is accomplished for a criminal or tortious purpose.⁷⁷ The requisite consent may be either actual or implied, but may not be constructive.⁷⁸ Courts generally find implied consent when the employee knew or should have known of a policy of constantly monitoring calls, or when

72. See *Fraser*, 323 F.3d at 115.

73. *Steiger*, 318 F.3d at 1050 (quoting J.J. White, *Email@work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1083 (1997)).

74. *In re Pharmatrack, Inc.*, 329 F.3d 9, 22 (1st Cir. 2003).

75. *Id.*

76. 18 U.S.C. § 2511(2)(d) (2000) and § 2702(b)(3) (2000).

77. 18 U.S.C. § 2511(2)(d).

78. Compare *Griggs-Ryan v. Smith*, 904 F.2d, 112, 117 (1st Cir. 1990) (noting that consent may be "inferred from 'surrounding circumstances' indicating the . . . [parties] knowingly agreed to the surveillance"), and *In re Pharmatrack, Inc.*, 329 F.3d at 19-20 (holding that consent under the ECPA may be explicit or implied, but must be actual rather than constructive), with *Watkins v. LM Berry & Co.*, 704 F.2d 577, 581-82 (11th Cir. 1983) (holding that mere knowledge of employer's capacity to monitor could not be considered consent).

the employee conducts a personal conversation over a line that is explicitly reserved for business purposes. For example, in *Griggs-Ryan v. Smith*,⁷⁹ the Court of Appeals for the First Circuit held that a tenant had consented to his landlord's interception of incoming phone calls when he had been told on a number of occasions that all such calls would be recorded.⁸⁰ In *Jandak v. Village of Brookfield*, a federal district court likewise found that a police officer consented to interception of his phone calls where he knew or should have known that the phone line he was using was constantly taped for police purposes, and because he was provided an unmonitored line for personal use.⁸¹ However, courts may decline to imply consent by an employee if the employer indicated only that it might be forced to monitor phone conversations to determine the number of personal calls made by employees.⁸²

Importantly, courts have held that consent is not an all-or-nothing proposition. Employees can consent to monitoring of only part of a communication or to only a subset of communications.⁸³ Therefore, employers must be cautious in drafting policies that specifically identify the types of communications being monitored and monitor only within the limits set in that policy. If such a policy is in place, any continued use of the e-mail system by an employee will presumably be done with the implied consent to allow interceptions of work-related communications and personal messages, at least to the extent needed to determine if the communication is business or personal.

c. Provider Exception

The second general exception is the "provider" exception, which covers employers who own and provide their company e-mail

79. 904 F.2d 112 (1st Cir. 1990).

80. *Griggs-Ryan*, 904 F.2d at 118-19.

81. *Jandak v. Village of Brookfield*, 520 F. Supp. 815, 824-25 (N.D. Ill. 1981); see also *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 393-94, 396 (10th Cir. 1979) (finding consent where the plaintiff made a personal call on a phone which was to be used exclusively for business purposes and which he knew was regularly monitored, instead of other phones that were specifically provided for personal calls).

82. See *Deal v. Spears*, 980 F.2d 1153, 1155-57 (8th Cir. 1992) (finding no implied consent where the employee was only notified that the employer "might" monitor to cut down on the number of personal phone calls).

83. See *In re Pharmatrack, Inc.*, 329 F.3d at 19 (explaining that a court must inquire into the "dimensions of the consent" and then determine whether the interception exceeded those boundaries); *Watkins*, 704 F.2d at 581 (employee consented to interception of business calls, but not personal calls).

networks.⁸⁴ Less clear is whether the exception applies to employers who provide e-mail capabilities through common carriers such as Prodigy or CompuServe.⁸⁵ The cases discussing the provider exception primarily concern telephone use, but one federal circuit court recently discussed the exception in the context of e-mail. Affirming the district court on different grounds, the Court of Appeals for the Third Circuit in *Fraser v. Nationwide Mutual*⁸⁶ held that access to an insurance agent's stored e-mail is exempt from the ECPA because the e-mail is stored on the insurance company's system, which the company administered as a provider.⁸⁷ In so holding, the court relied on *Bohach v. City of Reno*,⁸⁸ in which a district court similarly held that the retrieval of alphanumeric pages stored on the police department's computer system was not a violation of the ECPA, noting that when it comes to accessing communications in storage, service providers may "do as they wish."⁸⁹

Both *Fraser* and *Bohach* involved access to stored communications, and were governed by the less restrictive Stored Communications Act, which simply gives a wholesale exclusion to anyone who is a provider of an electronic communications service.⁹⁰ If, however, the provider is *intercepting* communications, additional requirements must be met under the Wiretap Act. Specifically, the provider must be able to show that the interception occurred in the normal course of employment while engaged in an activity that is either "necessary incident to the rendition of his service or to the protection of the rights or property of the provider of

84. See 18 U.S.C. § 2511(2)(a)(i) (2000) of the Wiretap Act which authorizes:

[A]n officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication 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

Id. See also 18 U.S.C. § 2701(c)(1)-(2) (2000) of the Stored Communications Act which likewise exempts person or entities providing a wire or electronic communications service.

85. See Kevin P. Kopp, *Electronic Communications in the Workplace: E-Mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861, 871 (1998) (citing Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 360 (1995)).

86. 352 F.3d 107 (2d Cir. 2003).

87. *Id.* at 115.

88. 932 F. Supp. 1232 (D. Nev. 1996).

89. *Id.* at 1236.

90. 18 U.S.C. § 2701(c)(1) (2000).

that service."⁹¹ The few cases discussing the interception of communications by providers indicate, however, that these additional requirements are not hard to meet. For example, in *United States v. Mullins*,⁹² the Court of Appeals for the Ninth Circuit found that American Airlines acted lawfully in monitoring a travel agent's computer reservations because American, as the provider of the computer reservation system, was monitoring to uncover suspected fraud.⁹³ The court found that the airline security chief who monitored the travel agent's computer was doing so "within the scope of her employment" and "to protect the rights and property of her employer."⁹⁴ Therefore, no liability existed under the ECPA.

d. Ordinary Course of Business Exception

In order to find liability under the ECPA, the violator must intercept the communication with an "electronic, mechanical or other device."⁹⁵ The phrase "electronic, mechanical or other device" excludes from its definition any "telephone or telegraph instrument, equipment or facility, or any component thereof," which is used by a provider of wire or electronic communication service "in the ordinary course of its business."⁹⁶ To date, this exception has only been applied to telephone monitoring and has not been extended to the monitoring of e-mail.⁹⁷ Commentators disagree about whether this exception will ever be applied to e-mail, since such monitoring is arguably not accomplished with a "telephone or telegraph instrument" as set forth by the statute.⁹⁸

91. *Id.* at § 2511(2)(a)(i) (2000).

92. 992 F.2d 1472 (9th Cir. 1992).

93. *Id.* at 1478.

94. *Id.*

95. 18 U.S.C. § 2510(4) (2000) (defining the term "intercept" under the Act).

96. *Id.* at § 2510(5)(a)(i-ii).

97. Dichter & Burkhardt, *supra* note 18, at 31; Sara DiLuzio, *Workplace E-mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741, 747 (2000); Kopp, *supra* note 85, at 874.

98. Compare Dichter & Burkhardt, *supra* note 18, at 31-32 (noting that e-mail does travel over telephone lines, but questioning whether e-mail is intercepted by use of telephone equipment as defined by the statute), and Patrice S. Arend & Kathleen M. Holper, *Monitoring E-Mail in the Workplace: Employee Privacy and Employer Liability*, 87 ILL. B.J. 314, 316 (June, 1999) (arguing that the exception is unlikely to apply to e-mail), with DiLuzio, *supra* note 97, at 747; (noting that the business exception may well provide another shield for employers who monitor e-mail), and Kopp, *supra* note 85, at 874-81 (noting only that the legislative history is silent as to how the exception may apply to e-mails, but analyzing how it might be applied under such a scenario).

Assuming that the exception extends to e-mail monitoring, whether an employer can successfully use this exception depends on whether the court follows the context or content approach.⁹⁹ A court using the context approach focuses on the employer's motive for the monitoring and whether "it had a legitimate business justification in doing so."¹⁰⁰ For example, courts using this approach have upheld monitoring where an employer had reason to believe that an employee was disclosing confidential information in violation of a loyalty agreement,¹⁰¹ and where employees' telephone calls were being monitored for quality control.¹⁰²

Conversely, a court using the content approach focuses not on the employer's business justification for monitoring, but on whether the monitored communication is business or personal.¹⁰³ For example, in *Watkins v. L.M. Berry & Co.*, all employees were aware of the employer monitoring employees' phone calls pursuant to an established policy.¹⁰⁴ The plaintiff sued under the ECPA after discovering that the company had monitored a personal phone call in which she discussed an interview she had with another company.¹⁰⁵ The Court of Appeals for the Eleventh Circuit held that while business calls are necessarily monitored in the normal course of business, personal calls cannot be intercepted in the ordinary course of business except to the extent necessary to determine that they are in fact personal calls.¹⁰⁶ Another court using the content approach found that a call was not of a personal nature, and therefore validly monitored, where it occurred during office hours, between co-employees concerning their supervisors.¹⁰⁷

Many states have enacted their own statutes regarding interception of electronic communication.¹⁰⁸ While most state statutes mirror the ECPA, there are some notable exceptions. For example, several states require the consent of both parties to a conversation before monitoring can occur.¹⁰⁹ In addition, at least two states, Connecticut and Delaware,

99. See DiLuzio, *supra* note 97, at 747, at n.39 (and authorities cited therein).

100. *Id.*

101. *Briggs v. American Air Filter Co., Inc.*, 455 F. Supp. 179, 180-82 (N.D. Ga. 1978), *aff'd*, 630 F.2d 414 (5th Cir. 1980).

102. *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).

103. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582-84 (11th Cir. 1983).

104. *Id.* at 579.

105. *Id.*

106. *Id.* at 583.

107. *Epps v. St. Mary's Hosp. of Athens, Inc.*, 802 F.2d 412, 416-17 (11th Cir. 1986).

108. See *Bartnicki v. Vopper*, 532 U.S. 514, 541-42, n.1 (2001) (Rehnquist, C.J., dissenting) (collecting statutes).

109. These states include California, Florida, Illinois, Maryland, Massachusetts,

"require advance notice of any electronic monitoring . . ." ¹¹⁰ Therefore, even if an employer meets one of the above exceptions under the ECPA, the employer must also closely check relevant state law.

3. Proposed Legislation

As far back as 1993, Congress has unsuccessfully tried to introduce legislation which would provide more protection for employees that are monitored in the workplace. The first such legislation was the Privacy for Consumers and Workers Act, introduced in the House of Representatives by Representative Pat Williams.¹¹¹ Under this proposed legislation, electronic monitoring of employees could only occur if the employer complied with specific notice requirements.¹¹² Employers would have been required to not only post an electronic monitoring notice in conspicuous places on the premises, but also would have to "notify . . . prospective employees . . . at the first personal interview of existing forms of electronic monitoring conducted by the employer."¹¹³ No random or periodic electronic monitoring would have been allowed, except for random monitoring of employees who had worked less than five years with the employer.¹¹⁴ The only exception to the notice requirements was "if an employer had a reasonable suspicion that any employee [was] engaged in conduct which violated criminal or civil law or constituted willful gross misconduct" and if such misconduct adversely affected "the employer's interests or the interests of other employees."¹¹⁵ In such a case, the employer would still have to execute a statement describing the conduct which was being monitored and the basis for the monitoring. Furthermore, the employer would need to identify the specific economic loss or injury to the business of the employer resulting from such conduct or the injury to the interests of

Michigan, New Hampshire, Pennsylvania, and Washington. See Bernabei, *supra* note 56, at *2.

110. *Id.*

111. Privacy for Consumers and Workers Act, H.R. 1900, 103rd Congress (1993), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=103_cong_bills&docid=fi1900ihtxt.pdf (last visited May 15, 2004).

112. H.R. 1900 § 4.

113. H.R. 1900 § 4.

114. H.R. 1900 § 5. Even in such a scenario, the monitoring would only be lawful if it was of a work group of employees who were provided notice "at least 24 hours but not more than 72 hours before the monitoring occurs." H.R. 1900 § 5 (B)(2).

115. H.R. 1900 § 5(C)(1).

such employer's employees."¹¹⁶ The employer would have to keep this statement for three years from the date the monitoring began, or until judgment was rendered in an action brought under the Act, whichever occurs later.¹¹⁷ This bill never made it out of the committee hearings.¹¹⁸

In July of 2000, Clinton administration officials announced that they would be seeking new legislation to address the protection of e-mail, including workplace e-mail, because of a belief that the ECPA was outdated.¹¹⁹ Shortly thereafter, Senator Charles Schumer and Representatives Charles Canady and Bob Barr jointly proposed the Notice of Electronic Monitoring Act, which would have required companies to notify workers if their e-mail messages, Internet usage, or phone usage was being monitored by the company.¹²⁰ Under that proposed legislation, an employer would not have to give prior notice of monitoring "if the employer had reasonable grounds to believe that . . . [the] employee 'was engaged' in conduct that violates the legal rights of the employer or another person, that such activity involves significant harm to the employer or such other person, and the electronic monitoring will produce evidence of such conduct."¹²¹ Violators would have been subject to actual and punitive damages, not to exceed \$500,000.00.¹²² Like the previous legislation, the bill never moved beyond the committee stage.¹²³

C. Common Law Protections

Lacking adequate protection under constitutional or statutory law, many employees turn to common law causes of action when challenging employer monitoring. The most commonly asserted privacy claim is known as "intrusion upon seclusion." The Restatement (Second) of Torts § 652(B) defines intrusion upon seclusion, providing that:

116. H.R. 1900 § 5(2)(B).

117. H.R. 1900 § 5(C)(2).

118. See status of bill located at <http://thomas.loc.gov/cgi-bin/bdquery/z?d103:HR01900:@@L&summ2=m&> (last visited May 15, 2004).

119. Meade, *supra* note 6, at 462.

120. Notice of Electronic Monitoring Act, H.R. 4908, 106th Congress (2000), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cog_bills&docid=fi4908ih.txt.pdf (last visited May 15, 2004).

121. H.R. 4908 § 2711(c).

122. H.R. 4908 § 2711(d).

123. See status of bill located at <http://thomas.loc.gov/cgi-bin/bdquery/D?d106:1:/temp/>.

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 the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.¹²⁴

The seminal case discussing common law privacy is *Smyth v. Pillsbury Co.*¹²⁵ In *Smyth*, the Pillsbury Company fired one of its regional operations managers for sending what the company "deemed to be inappropriate and unprofessional comments over . . . [the company's] e-mail system."¹²⁶ The manager made threats against sales management to "kill the backstabbing bastards" and referred to the planned Holiday party as the "Jim Jones Kool-Aid affair" when replying to e-mail messages from his supervisor over the company's e-mail system.¹²⁷ Although the manager sent the messages via company e-mail, he did so from his personal computer at home, and did so based upon the company's assurances that "all e-mail communications would remain confidential and privileged."¹²⁸ Upon his termination, the manager sued the company for wrongful discharge, claiming that his termination violated Pennsylvania's public policy against terminating at-will employees after violating their right to privacy.¹²⁹

Applying a balancing test not unlike the invasion of privacy analyzed under constitutional law discussed above in Section III.A, the court balanced the company's reasons to intercept the manager's e-mail with the manager's reasonable expectations that the e-mail would remain private. The court held that the manager had no "reasonable expectation of privacy in e-mail communications voluntarily made . . . over the company e-mail system notwithstanding any assurances that such communications would not be intercepted."¹³⁰ The court explained that once the manager made comments over "an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost."¹³¹ The court took the position, which appears to be fatal for employees wishing to bring privacy claims based upon e-mail

124. RESTATEMENT (SECOND) OF TORTS § 652(B) (2000).

125. *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

126. *Id.* at 98-99.

127. *Id.* at n.1.

128. *Id.* at 98-99.

129. *Id.* at 100.

130. *Id.* at 101.

131. *Id.*

monitoring in Pennsylvania, that there are “no privacy interests in . . . [e-mail] communications.”¹³²

The court went on to hold that even if the manager could have had a reasonable expectation of privacy to the content of his e-mail messages, the company did not commit a “substantial or highly offensive invasion” of the manager’s privacy by reading his messages.¹³³ The court based its holding upon the fact that, unlike a compulsory employee drug or alcohol test conducted by the employer, the company merely monitored e-mail messages that the manager voluntarily sent over the company e-mail system.¹³⁴ More importantly, however, the company’s interest in monitoring e-mails to prevent inappropriate and unprofessional comments, or even illegal activity over its e-mail system, outweighed any privacy interest the manager could have had in his comments.¹³⁵

Recent cases have applied these principles to monitoring of e-mail. For example, in *McLaren v. Microsoft Corp.*,¹³⁶ the Texas Court of Appeals held that an employee did not have a legitimate expectation of privacy in the contents of stored e-mail messages, despite the fact that they were stored in “personal” folders under a private password.¹³⁷ The court noted that the e-mails were stored on a company computer given to the plaintiff to perform the functions of his job, and as such, were an “inherent part of the office environment,” and not the employee’s personal property.¹³⁸ The court additionally pointed out that although the e-mails were stored in password-protected folders, they were initially sent over the network and were at some point accessible by another individual.¹³⁹ Even if the employee had some expectation of privacy in the e-mail messages, the court found that a reasonable person would not find the search a “highly offensive invasion.”¹⁴⁰ In so holding, the court noted that the plaintiff was on leave pending a sexual harassment investigation at the time the e-mails were accessed and that some of the e-mails were indeed relevant.¹⁴¹ The court held that the company’s interest in preventing inappropriate, or even unlawful conduct,

132. *Id.* (emphasis added).

133. *Id.*

134. *Id.*

135. *Id.*

136. 1999 WL 339015 (Tex. Ct. App. 1999).

137. *Id.* at *4-5.

138. *Id.* at *4.

139. *Id.*

140. *Id.* at *5.

141. *Id.*

outweighed any claimed privacy interest in those communications.¹⁴² Other courts have likewise found no reasonable expectation of privacy under similar circumstances.¹⁴³

IV. GUIDELINES FOR DEVELOPING POLICIES GOVERNING E-MAIL AND INTERNET USAGE

As reflected by the cases discussed above, although not yet required by law, the best way for employers to avoid constitutional, statutory, or common law privacy claims is to implement e-mail and Internet usage policies which educate their employees about the lack of privacy in on-line activities while at work and, at the same time, operate as consent in the event an employer chooses to monitor those activities. In drafting and implementing such policies, employers should consider the following:

A. Formulate and Adopt Written E-Mail and Internet Policies That Clearly Define the Employees' Reasonable Expectations of Privacy to E-Mail and Internet Usage

After determining the stance the company intends to take with regard to e-mail and Internet monitoring, the company should adopt written policies, acknowledged in writing by employees, that define the company's monitoring practice. Some companies have even installed programs that alert employees each time they log in that computer usage is not private. As shown by the cases discussed above, such measures diminish any expectation on the part of employees that computer usage at work is private.

Indeed, e-mail is not necessarily private—even from persons other than the employer. E-mail is routinely discoverable in litigation, and may prove to offer fruitful evidence for persons suing a company. As such, employees should be told to take great care in ensuring that e-mail messages are drafted in a professional manner.

142. *Id.*

143. *See* Garrity v. John Hancock Mutual Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002) (finding that even if plaintiffs had a reasonable expectation of privacy in their password-protected e-mails, the employer's legitimate business interest in protecting employees from sexual harassment outweighed those privacy interests).

B. Harmonize E-Mail and Internet Policies with Policies Prohibiting Workplace Discrimination and Violence

Because employers may be held vicariously liable for failing to discover discriminatory or threatening e-mails sent over company computer systems which should have been detected, anti-discrimination policies should blend readily with e-mail and Internet policies. Therefore, companies may wish to reiterate their policies prohibiting discrimination and violence in the workplace when formulating e-mail and Internet policies.

C. Suggested Language to Include in E-Mail/Internet Policies

While all employers have differing needs, and should adopt an e-mail/Internet policy that meets their particular circumstances, employers may wish to consider the following sample language for inclusion in e-mail and Internet policies:

- (1) All e-mail messages and information stored on computer files are company property. As such, employees should not consider e-mail messages private. Management can and will access such communications at any time if warranted under the circumstances;
- (2) Deleting an e-mail message does not mean that it has been erased from the computer system. The company retains backup of certain media, including e-mail communications, in the normal course of management of the system;
- (3) All e-mail should be drafted with the understanding that messages and files will be read by someone else. Users should exercise restraint in language and terminology, and the same decorum used in printed memoranda and mail should be followed;
- (4) Employees should not use the system to communicate any obscene, derogatory, defamatory or other inappropriate messages. Employees are also strictly prohibited from viewing or downloading from the Internet anything of a harassing, intimidating, offensive, or discriminatory nature. The guidelines set forth in the company's Sexual Harassment Policy are equally applicable to e-mail and Internet use;

(5) Employees should not consider their Internet use private. Information as to the sites visited and the times when such usage occurs will be available for reference. Employees are strictly prohibited from sending chain letters, gambling, or engaging in any other activity in violation of state and/or federal law. The company will monitor Internet usage to ensure compliance with this policy;

(6) All improper uses of e-mail, Internet, and computer files can result in disciplinary action up to, and including, termination from employment.

Employers should provide employees with copies of the written policy, refer to it in any employee training that is given, and thereafter provide periodic reminders.

V. EMERGING LABOR ISSUES

Any discussion of e-mail policies and practices is incomplete without mention of special concerns regarding the potential for unfair labor practice charges. Problems can occur where employers enforce their e-mail policies in a discriminatory manner, allowing employees to use e-mail to distribute a wide variety of material on various subjects which have little relevance, if any, to the employer's business,¹⁴⁴ but then prohibit the use of the e-mail system for union organizing. In one such case, the National Labor Relations Board (NLRB) upheld a ruling by an administrative law judge that such actions violate employee rights under Section 7 of the National Labor Relations Act (NLRA).¹⁴⁵ Based on this holding, it appears that if a corporation allows its employees regularly to use e-mail for personal purposes, the company may be hard pressed to justify a ban on pro-union messages.

It would appear that an employer would be wise to simply adopt and enforce an e-mail policy which prohibits all non-business use of e-mail. Yet this too can create problems. In a 1998 case, the NLRB General Counsel took the position that a policy prohibiting all personal messages

144. Common examples include selling tickets to various sporting or other events and school fundraisers.

145. See *E.I. DuPont DeNemours & Co.*, 311 N.L.R.B. 893, 898 n.4 (1993). For the administrative law judge's opinion, see *id.* at 904.

from the e-mail system was overly broad and illegal.¹⁴⁶ In doing so, the General Counsel noted that some e-mail communication is akin to oral solicitation, which, under NLRB rules, cannot be prohibited during non-work time.¹⁴⁷ At least one NLRB Administrative Law Judge has agreed.¹⁴⁸

The General Counsel's opinion left open the question whether some e-mail might also be treated as "distribution" of union material, rather than solicitation. Courts and commentators alike have suggested that this might be the case since e-mail can be printed and saved for reading or re-reading, like written literature.¹⁴⁹ If this is true, an employer would be permitted to limit such e-mail to nonworking areas during nonworking time.¹⁵⁰ However, determining what constitutes a "work area" in cyberspace may prove difficult. The General Counsel has stated that computers themselves might constitute work areas if the employees' use is found to be substantial.¹⁵¹ The NLRB, however, has yet to reach that conclusion.¹⁵² Until further opinions address the issue, it will remain an uncertainty for employers.

Finally, employers must always remember that communication via e-mail or the Internet can constitute protected activity under the NLRA. For example, in *Timekeeping Systems, Inc.*, an employer was found to have violated Section 8 of the NLRA after terminating an employee who had e-mailed the company protesting changes to employee benefits.¹⁵³ The NLRB found that in sending the e-mail, the employee was seeking to enlist the support of fellow employees for his position with respect to the proposed changes.¹⁵⁴ Thus, the employee was engaged in a concerted activity that was entitled to protection.¹⁵⁵

146. See Report of the NLRB General Counsel, at <http://www.lawmemo.com/emp/nlrb/gcreport.htm>.

147. See *id.* Non-work time includes time such as lunch and breaks.

148. See *Prudential Ins. Co. of Am.*, 2002 WL 31493320 (N.L.R.B. Div. of Judges, Nov. 1, 2002); but see *Guard Publish. Co.*, 2002 WL 336963 (N.L.R.B. Div. of Judges, Feb. 21, 2002) (noting that the NLRB has yet to hold that an e-mail system constitutes a workplace where an employer is prohibited from limiting all solicitation).

149. *Prudential*, 2002 WL 31493320; *Dichter & Burkhardt*, *supra* note 18, at 66.

150. For general rules on solicitation and distribution under the NLRA, see *Stoddard-Quirk Manuf. Co.*, 138 N.L.R.B. 615, 619-21 (1962).

151. See *Dichter & Burkhardt*, *supra* note 18, at 67.

152. *Guard Publish. Co.*, 2002 WL 336963.

153. *Timekeeping Systems, Inc.*, 323 N.L.R.B. 244 (1997).

154. See *id.*

155. See *id.*

Like many other areas of the law, the NLRA has not yet caught up completely to the electronic communication age. What can be discerned from the few cases that do exist, however, is that employers who try to completely control all information communicated by employees on company computer systems may find themselves at odds with the Act. Employers must avoid limiting e-mail and Internet use only in the context of union issues, and must be certain before terminating or disciplining employees that the communication is not about the terms and conditions of employment and therefore protected concerted activity.

VI. CONCLUSION

Maintaining a safe and efficient work environment requires companies to keep a watchful eye on employee activities which could pose harm to others or create liability for the employer. In today's computer-reliant world, that means monitoring electronic communications and Internet use to identify potential problems. Monitoring, however, is only the first step. Employees must be educated about the monitoring that is taking place in order to better understand the lack of privacy that exists. As the law slowly catches up with technology, many questions still remain and privacy advocates will likely continue to push for reforms that would offer greater protection to employees. If history is any judge, these efforts will likely fail. Until the law is changed, employers who adopt, and adhere to, comprehensive e-mail and Internet policies should be immunized under most circumstances.