UIC Law Review

Volume 28 | Issue 1 Article 4

Fall 1994

Watch Your E-mail - Employee E-Mail Monitoring and Privacy Law in the Age of the Electronic Sweatshop, 28 J. Marshall L. Rev. 139 (1994)

Laurie Thomas Lee

WATCH YOUR E-MAIL! EMPLOYEE E-MAIL MONITORING AND PRIVACY LAW IN THE AGE OF THE "ELECTRONIC SWEATSHOP"

LAURIE THOMAS LEE*

INTRODUCTION

Employee privacy is considered to be the most significant workplace issue facing companies today.[1] A recent survey of American businesses by *MacWorld* magazine suggests that twenty million Americans may be subject to some type of electronic monitoring through their computers on the job.[2] Employer access to what employees thought were private electronic mail (E-mail) files is especially raising eyebrows. The same study reveals that of those companies that engage in electronic monitoring practices, over forty percent have searched employee E-mail files.[3] This is particularly troubling when less than one-third of all admitted electronic surveillants say they ever warn employees,[4] and only eighteen percent of companies even have a written policy on electronic monitoring.[5]

E-mail is considered to be the fastest growing form of electronic communication in the workplace, but the laws addressing employee privacy rights with respect to E-mail are unclear. Little conclusive research has been done on the legality of E-mail moni-

---

* Ph.D. Mass Media (Telecommunications), Michigan State University, 1993; M.A., University of Iowa, 1983; B.S., Kearney State College, 1982. Dr. Lee is currently an Assistant Professor in the Department of Broadcasting, College of Journalism and Mass Communications at the University of Nebraska-Lincoln.

1. At the American Civil Liberties Union, violations of privacy at the workplace have become the largest category among its 50,000 complaints received each year. Peter Blackman & Barbara Franklin, *Blocking Big Brother; Proposed Law Limits Employers' Right to Snoop*, N.Y. L.J., Aug. 19, 1993, at 5.

2. Charles Piller, *Bosses With X-Ray Eyes*, MACWORLD, July 1993, at 188, 120. *MacWorld* conducted a survey of 301 businesses about employee monitoring. More than 21 percent of the respondents indicated that they have searched computer files, voice mail, E-mail, or other networking communications. For companies of more than 1,000 employees, that figure rises to 30 percent.

3. *Id.* at 123. An informal survey by the San Jose Mercury News of top Silicon Valley companies also found a majority retain the right to review E-mail, and no company said it would not read other people's E-mail. *E-mail Snoopers No Secret*, RECORD, Apr. 21, 1994, at DO2.

4. Piller, *supra* note 2, at 122.

5. *Id.* at 120.

toring. Do employers have the right to look at an employee's E-mail messages? Do employees have a right to privacy that bars corporate snooping?

This Article examines the privacy debate and the legality of E-mail monitoring in the workplace. Part I explains the far-reaching effects of E-mail monitoring and elucidates the divergent arguments in the debate for and against stricter controls. Part II begins the legal analysis by exploring the constitutionality of E-mail monitoring. Part III examines federal and state statutory law. Part IV of this Article examines E-mail monitoring under the common law, focusing on employee privacy rights. Part V explains that several bill are now pending in Congress that are intended to either limit employer access[6] or permit workplace monitoring.[7] Finally, Part VI proposes some guidelines for balancing employee privacy and corporate monitoring needs.

I. E-MAIL MONITORING

With an estimated forty million E-mail users expected to be sending sixty billion messages by the year 2000, it is no wonder that corporate America is closely watching to see how the courts and Congress will handle the E-mail monitoring issues.[8] Electronic mail has become an indispensable tool that has revolutionized the workplace. More workers are able to communicate everything from simple memos to complex business plans to colleagues and clients across the hall or around the world in a matter of seconds. Companies and employees alike recognize the benefits of a technology that has the power to speed communication and improve productivity and efficiency.[9] At a time of fierce international competition, few employers can afford to pass up any opportunities E-mail provides.

---

6. S. 984, 103d Cong., 1st Sess., 139 CONG. REC. S6122 (1993); and H.R. 1900, 103d Cong., 1st Sess., 139 CONG. REC. E1077 (1993).

7. S. 311, 103d Cong., 1st Sess., 139 CONG. REC. S1390 (1993).

8. Scott Dean, *E-Mail Forces Companies to Grapple With Privacy Issues*, CORP. LEGAL TIMES, Sept. 1993, at 11. Corporate E-mail has grown 83 percent among the Fortune 2000 firms between 1991 and 1993, and nine out of ten locations employing over 1,000 workers in the U.S. now uses E-mail. John Thackery, *Electronic-Mail Boxes a Dumping Ground for Meaningless Data*, OTTAWA CITIZEN, May 28, 1994, at B4 (citing projections by the Electronic Messaging Association).

9. For example, E-mail can be used to enhance a company's effectiveness by facilitating the flow of communications among employees at all levels, reducing "telephone tag," and resulting in a cost savings from reduced paper and postage usage. James J. Cappel, *Closing the E-mail Privacy Gap; Employer Monitoring of Employee E-mail*, J. SYS. MGMT., Dec. 1993, at 6. E-mail also allows users to send messages on any day (i.e., on weekends) and at any time of day (i.e., at 2 a.m.), does not require the simultaneous presence of the recipient, and allows messages tc be sent to more than one recipient at a time.

Yet the accessibility of corporate-owned E-mail systems also presents a compelling new opportunity for company executives to "sneak a peak" at intracompany and intercompany communications in order to monitor employees and maintain control over the workplace. E-mail messages can easily be intercepted and read by not only system managers and operators, but by anyone with a working knowledge of and access to the corporate network.[10] In some cases, corporate executives may simply "ask" network administrators to present them with an employee's E-mail files.[11] In general, administrators will often monitor the message traffic and store E-mail as a permanent electronic record, and in some cases make and store printed copies.[12] Of course, messages are also vulnerable if employees are not given passwords to log into their mail, simply stay logged-in when they are away from their computers, or inadvertently route their messages to unintended recipients.[13] While some encryption technology is available or being developed for E-mail systems,[14] few companies may use encryption because of cost and efficiency factors.[15] Some type of E-mail security is desperately needed.[16]

---

10. *See* Piller, *supra* note 2. *MacWorld* examined some E-mail products for their ability to be invaded. *Id.*

11. Doug vanKirk, *IS Managers Balance Privacy Rights and Risks; Proactive Companies are Establishing Clear Guidelines and Informing Employees*, INFOWORLD, Nov. 29, 1993, at 65.

12. This is what happened in 1990 when the Mayor of Colorado Springs, Colorado, admitted he had been reading the electronic mail that city council members had sent to one another. Don J. DeBenedictis, *E-Mail Snoops*, A.B.A. J., Sept. 1990, at 26. An E-mail policy had required that messages be printed periodically and be deleted to save space on the city computer. *Id.* The printouts were kept in case any messages were deemed covered by the state's public-records law. *Id.*

13. The ease of replying to E-mail messages and sending messages to many people on a "whim" (as compared to sending ordinary letters) can also exacerbate the monitoring problem in terms of what may be communicated and regrettably read. A notorious example is that of Officer Lawrence Powell who, after the beating of Rodney King, broadcast an E-mail message over the Los Angeles Police Department system saying, "Oops, I haven't beaten anyone so bad in a long time." John K. Keitt, Jr. & Cynthia L. Kahn, *Cyberspace Snooping*, LEGAL TIMES, May 2, 1994, at 24.

14. *See, e.g.*, Reuven M. Lerner, *Protecting E-mail*, TECH. REV., Sept. 1992, at 11, which discusses the use of public-key cryptosystems which grant the receiver of any E-mail sole access to its contents. *See also* Stephen T. Kent, *Internet Privacy Enhanced Mail: Development of Security Standards for Internet Computer Network*, COMM. ACM, Aug. 1993, at 48 (discussing Internet security concerns).

15. Dean, *supra* note 8.

16. E-mail security technology is lagging behind, yet software makers are reportedly hesitant to develop encryption programs because the Clinton administration may soon require them to use "backdoors"—i.e., with the "Clipper Chip"—that would allow authorized federal agencies like the F.B.I. to break the code and retrieve messages. *See, e.g.*, Winn Schwartau, *Crypto Policy and Business Privacy: The Clinton Administration's Proposed Clipper Chip Workplace Privacy*, PC WK.,

Some employees are already finding this out the hard way. In what is believed to be the first publicly known E-mail case from 1990, an E-mail administrator for Epson America, Inc., discovered a supervisor reading all employee E-mail originating from outside the company. Alana Shoars had been told to reassure some 700 Epson employees that their E-mail would be private. When she complained about the monitoring, she was fired.[17] In another case, two system administrators of the California-based Nissan subsidiary's E-mail network were fired after filing a grievance alleging that their privacy had been invaded when their boss read their E-mail and had subsequently fired them.[18] Perhaps the most notorious case of E-mail insecurity involved Oliver North and John Poindexter who were communicating through E-mail in the system at the National Security Council. Although they thought they had sufficiently deleted their messages, back-up tapes had been made and were allowed as evidence for use by prosecutors in the Iran-Contra investigation.[19] A more recent civil suit that is still pending may have serious implications for anyone who uses E-mail at work. In 1992, a former Borland International Vice President defected to a rival computer software maker, but not before allegedly forwarding trade secrets via Borland's MCI Mail. Borland executives obtained the departing Vice President's password and discovered the messages which it intended to use as evidence against the former employee.[20] However, because MCI Mail was used as opposed to an intracompany E-mail system, a different legal analysis may come into play.[21]

June 28, 1993, at 207.

17. *Electronic Mail Raises Issues About Privacy, Experts Say*, Daily Lab. Rep., (BNA) No. 222, at A-7 (Nov. 17, 1992) [hereinafter *Electronic Mail Raises Issues*]; Nicole Casarez, *Electronic Mail and Employee Relations: Why Privacy Must Be Considered*, PUB. REL. Q., Summer 1992, at 37; Piller, *supra* note 2; Lynn Schwebach, *Reconciling Electronic Privacy Rights in the Workplace*, PC TODAY, Jan. 1992, at 38. She sued and a class action suit followed, but both cases were thrown out. Appeals are pending. See *infra* note 162 for a discussion of the *Epson* case.

18. Dean, *supra* note 8. Their E-mail had included jokes, racy personal messages, and criticism of the boss. See *infra* note 162 for a discussion of the Nissan E-mail situation.

19. Alice Kahn, *Electronic Eavesdropping*, S.F. CHRON., Oct. 31, 1991, at D3. In January 1993, a U.S. District Court Judge for the District of Columbia ruled that the tapes are official records and cannot be destroyed. Dean, *supra* note 8, and Keitt, Jr. & Kahn, *supra* note 13. This case, however, involved government communications which are subject to a different legal analysis. See *infra* notes 35-52 and accompanying text for a discussion of the constitutionality of searches of government employees.

20. Dean, *supra* note 8. In a similar case, two computer programmers who worked for Mentor Graphics, a software company in San Jose, California, were fired for allegedly disclosing trade secrets to a rival computer company. The disclosure was discovered while monitoring E-mail messages sent over Internet. The case was settled in early 1992. *Electronic Mail Raises Issues*, *supra* note 17, at A-7.

21. Piller, *supra* note 2, at 122; Dean, *supra* note 8. See *infra* notes 70-71 and

A legal solution will not be without compromise because both proponents and opponents of E-mail monitoring are prepared to do battle. Proponents of E-mail monitoring are employers interested in protecting their corporate secrets as well as controlling their workplace. Opponents of monitoring are the employees, labor unions, and advocacy groups. The following section delineates both sides of the debate between employer monitoring and employee privacy.

A. The Debate

Legislation now before Congress addresses some of the issues of electronic monitoring in the workplace, including E-mail,[22] but not everyone is backing the measures. Proponents of stricter controls, including union leaders and advocacy groups, argue that without some reasonable restrictions, the nation runs the risk of turning workplaces into what are being coined as "electronic sweatshops," where constant monitoring freely occurs.[23] Yet virtually every business lobbying group in Washington is lining up against proposed legislation that would curtail their ability to monitor the workplace.

Historically, employers have always monitored their workers' performance by observing production lines, counting sales orders, and simply looking over an employee's shoulder. Encroachment on employee privacy has strong traditions, from the advent of the industrial age and production line monitoring to employee psychological testing and more recently, drug screening. But today, the product of more businesses is service and information, which requires a different type of monitoring approach. In addition, new technologies have ushered in more ways to overhear, watch, or read just about anything in the workplace,[24] including E-mail.

There are concerns that these new forms of monitoring are

---

accompanying text for a discussion of the relevant law which came into play because MCI mail was used.

22. S. 984, 103d Cong., 1st Sess., 139 CONG. REC. S6122 (1993); H.R. 1900, 103d Cong., 1st Sess., 139 CONG. REC. E1077 (1993); and S. 311, 103d Cong., 1st Sess., 139 CONG. REC. S1390 (1993).

23. Lini Kadaba, *Employer Eavesdropping Debated: Workers Say it Stresses Them Out; Companies Content They Have Right*, PHOENIX GAZETTE, Oct. 8, 1993, at C6; Bruce Phillips, *Uncontrolled Employee Monitoring Raises Threat of Electronic Sweatshops*, OTTAWA CITIZEN, Sept. 1, 1993, at A11.

24. For example, electronic cards and "Active Badges" can reveal a worker's presence and location, call accounting systems can show how many calls and facsimiles were made and to whom, and computer programs can record when and how long an employee was logged onto a computer. *See, e.g.*, Blackman & Franklin, *supra* note 1; Phillips, *supra* note 23; Larry Tye & Marla Van Schuyver, *Technology Tests Privacy in the Workplace: No Private Lives*, BOSTON GLOBE, Sept. 6, 1993, at 13.

diminishing the privacy rights of millions of workers, and opponents fear that the workplace monitoring problem will only be exacerbated by even newer technologies being developed. Proponents of legislation to limit electronic monitoring argue that the need for employee privacy protection is now. They point to the recent *MacWorld* survey[25] and other studies[26] that reveal an alarming amount of electronic surveillance of workers—much of it done surreptitiously. They argue that employees are entitled to human dignity and should not have to leave their right of privacy behind when they go through the office door. Moreover, people should be able to assume their mail is private, whether they are sending it via the Postal Service or an electronic method. There are fears of abuse by employers reading E-mail for non-legitimate reasons such as voyeurism and paranoia. In addition, studies[27] show that employee surveillance in general takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management, and lower productivity,[28] not to mention higher health-care costs.

On the other hand, the corporate world[29] argues that they

---

25. Piller, *supra* note 2, at 123.

26. For example, a 1991 study by the Society for Human Resource Management of its members found that eleven percent of the 1,493 respondents used video cameras to monitor workers; eight percent, computer terminal; and five percent, telephone taps. Kadaba, *supra* note 23. In 1990, a study of 186 New York metropolitan area companies found 73—roughly 40 percent—were engaging in some type of electronic surveillance of their employees. Gene Bylinsky, *How Companies Spy on Employees*, FORTUNE, Nov. 4, 1991, at 131, 132. On the other hand, a study by Robert Half International, Inc., revealed that only 44 percent of companies surveyed had a written code of ethics communicated to employees. Schwebach, *supra* note 17. Employees also seem to be naive about company monitoring practices. A Louis Harris Associates Survey of 1000 workers at 300 companies found more than 90 percent think that employers collect only information that is relevant and necessary. Lee Smith, *What the Boss Knows About You*, FORTUNE, Aug. 9, 1993, at 88.

27. These studies include one conducted by the University of Wisconsin that revealed that monitored telecommunications workers suffered more from depression, anxiety, and fatigue than non-monitored workers at the same plant. Blackman & Franklin, *supra* note 1, at 5. A Massachusetts survey showed that at companies monitoring for efficiency, 65 percent of employees could not perform their tasks effectively because they were required to work too fast. *Id.*

28. For a related discussion, *see* Ernest Kallman, *Electronic Monitoring of Employees: Issues & Guidelines*, J. SYS. MGMT., June 1993, at 17.

29. Trade associations and others are taking different stances on the debate. Richard A. Danca, *Privacy Act Would Force Firms to Inform Their Employees About E-Mail Monitoring: Privacy Issue Comes of Age in the Networked World*, PC WK., June 28, 1993, at 203. The ACLU's Task Force on Civil Liberties in the Workplace takes the position that companies should not open employee E-mail, although other organizations are also amenable to the corporate view. *Id.* The Computer Professionals for Social Responsibility (CPSR), which in fact lobbied Congress to specifically include E-mail in its proposed legislation, says that companies should give

need to reserve the right to electronically monitor job performance and work-related activities in order to investigate and prevent theft, fraud, insider trading, drug dealing, and other illegal conduct, as well as to assure productivity, efficiency, and quality control.[30] Employers use monitoring for such purposes as evaluating employees and ensuring that customer and client relations are handled properly.[31] Critics of legislation restricting employer access argue that what takes place on company premises over company phones and E-mail networks belongs to the company which has a right to access the work product for which it is paying. They contend that employers have a legitimate right to a fair day's work and to be able to ensure that work is accomplished by being able to keep track of personal use of company equipment and other abuse. Warning employees of when they will be monitored defeats the purpose. Moreover, they argue that limiting access would mean that employers might not be able to access an employee's E-mail in emergency situations.[32]

Unless adequate legislation is passed, workers subjected to E-

---

individuals more privacy, but that company policies could spell out monitoring practices. *Id.* The Electronic Frontier Foundation in Washington comes down on the side of privacy but agrees that if a monitoring policy is presented to employees, that employees are effectively giving the company permission to monitor their E-mail. *Id.* On the other hand, the Computer and Business Equipment Manufacturers Association considers computer monitoring to be a legitimate management tool, and the Electronic Mail Association (EMA), which represents E-mail suppliers and corporate users, agrees. *Id.* While company policies spelling out privacy are good, EMA Executive Director William Moroney thinks that "employers need the right to control, evaluate, and monitor all forms of employee communication." *Id.* The EMA essentially believes that employees should not expect any more of a right of privacy with E-mail than they would get from tossing a memo in their out-basket. *Id.*

30. According to the *MacWorld* survey, nearly half of the managers surveyed endorse the concept of electronic monitoring. Piller, *supra* note 2, at 121. Four percent endorse it "for routinely verifying employee honesty." *Id.* A much higher number, 23 percent, feel electronic monitoring is a good tool where reasonable evidence of wrongdoing, such as theft or negligence, comes to light. *Id.*

31. Terry Morehead Dworkin, *Protecting Private Employees From Enhanced Monitoring: Legislative Approaches*, 28 AM. BUS. L.J. 59 (Spring 1990). A study by Ernest Kallman found several specific arguments for employing electronic monitoring in general. Kallman, *supra* note 28, at 17. The primary argument put forth by management is to increase productivity. *Id.* The second argument is that electronic monitoring allows management to do a better job of personnel management since it provides a more objective appraisal. Finally, it improves the performance appraisal process. *Id.*

32. For example, there are concerns that if a newspaper working on a major story relied on some key information stuck in a reporter's E-mail, the newspaper would not be able to access the information if the reporter was not available to give permission. Likewise, if a purchase order were sent via E-mail to a specific recipient who was unavailable, no one else in that office would be able to access the file to process the order. Bob Brown, *E-Mail Users Voice Concern About Pending Legislation*, NETWORK WORLD, Aug. 23, 1993, at 6.

mail searches will have to turn to the existing laws for possible recourse. These laws are virtually untested as they pertain to employee E-mail and privacy rights. The following sections explore what federal and state constitutional and statutory provisions might apply to employee E-mail monitoring and examine the existing tort law remedies.

II. E-MAIL PRIVACY RIGHTS UNDER THE CONSTITUTION

An examination of the highest source of law reveals that Constitutional privacy rights,[33] as they might pertain to employees, are very limited in scope. The Fourth Amendment to the U.S. Constitution provides that the "right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated. . . ."[34] Most states also have a similar constitutional provision that provides similar protection. Yet the U.S. Constitution (and most state constitutions)[35] only prohibit searches and seizures by the government and not by the private sector.[36] Thus, in an employment context, only government employees may claim a Constitutional privacy right should their E-mail be accessed; nongovernment employees have no Constitutional guarantee of privacy in the workplace, unless infringed by a government search or seizure.[37]

While privacy protection afforded to public employees is beyond the scope of this Article, it is nonetheless instructive to briefly examine and compare the scope of these rights and the analysis used. For government employees (or employees subject to E-mail searches by the government) these rights are limited and may not be upheld. So far, no case law specifically addresses a constitutional right of privacy related to E-mail, so courts may rely on precedents associated with similar types of electronic surveillance such as the monitoring or recording of telephone communications. Here, the Supreme Court and lower courts have generally ruled in favor of the government infringers.

Section A initially discusses those federal and Supreme Court decisions relating to monitoring telephone communications. Sec-

---

33. A right of privacy is not explicitly stated in the U.S. Constitution, although it has an implicit textual basis found in several amendments such as the Fourth Amendment. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

34. U.S. CONST. amend. IV.

35. See *infra* notes 53-59 and accompanying text for a discussion of the relevant privacy provisions of several states' constitutions.

36. The Search and Seizure clause of the U.S. Constitution does not protect citizens from unreasonable searches by private parties. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113-14 (1984); Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974).

37. In this sense, one might observe that private employees actually enjoy less privacy protection than those working for the government.

tion B applies the tests formulated from those opinions that determine when monitoring violates the Constitutional right to privacy. Finally, section C analyzes state constitutions in relation to the Constitution, concentrating on the California State constitution which contains a specific privacy provision for private sector protection.

A. The United States Constitution

The Supreme Court tends to rule in favor of the alleged infringer in monitoring privacy cases. In the landmark privacy case *Katz v. U.S.*,[38] and the subsequent case *Smith v. Maryland*,[39] the Supreme Court defined the parameters within which government agencies may engage in telephone monitoring without warrants.[40] The Court relied on its two-part test which essentially determines whether the plaintiff exhibited a reasonable "expectation of privacy."[41] Whether an "expectation of privacy" exists (and thus whether a plaintiff's suit might be successful) depends on a number of factors such as the private nature of the information involved and whether the individual had "knowingly exposed" the information.[42] In *Smith*, the Court determined that the plaintiff had no expectation of privacy when a pen register employed by a telephone company at police request had recorded the telephone numbers he had dialed from his home. The Court stated that "[a]ll subscribers realize . . . that the phone company has facilities for

---

38. 389 U.S. 347 (1967).

39. 442 U.S. 735 (1979).

40. In *Katz*, F.B.I. agents acting without a warrant attached a listening device to the outside of a public phone booth to monitor the defendant's conversation. 389 U.S. at 348. In *Smith*, a telephone company used a pen register at police request to record the numbers dialed from the home of a man suspected of placing threatening calls to a robbery victim. 442 U.S. at 737.

41. This standard was first enunciated in *Katz* and later adopted in *Smith*. It first asks whether the individual, by his or her conduct, has "exhibited an actual (subjective) expectation of privacy," *id.* at 361 (Harlan, J., concurring), having shown that he or she "seeks to preserve (something) as private." *Id.* at 351. The second part of the analysis is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Id.* at 361. (Harlan, J., concurring). Most adjudication has relied on the second part of the inquiry, which remains the prevailing authority. *See, e.g.*, Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974) (discussing the reasonableness analysis of privacy cases).

42. Other criteria include whether there was a legitimate purpose or "compelling government interest" in the seizure/disclosure of the information; what alternatives were available; whether a property right could be maintained; and what precautions were taken. For an analysis of these criteria, see Laurie Thomas Lee, *Constitutional and Common Law Informational Privacy: Proposing a "Reasonable Needs" Approach for New Technologies*, Paper Presented to the AEJMC Annual Convention, Kansas City (Aug. 1993) (unpublished manuscript on file with *The John Marshall Law Review*).

making permanent records of the numbers they dial. . . ."[43] The Court also concluded that an expectation of privacy in this case would not be reasonable because Smith had "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[44]

Applying the *Smith* standard to E-mail suggests that an employee's privacy interest in E-mail messages would likewise fail the "expectation of privacy" test since most users probably realize that a system administrator could have access to their E-mail accounts. Although most users assume that the administrator will not examine their mail,[45] they have nonetheless "voluntarily conveyed" the information. Moreover, if government employers have a publicized policy on this type of electronic monitoring, then the employee has generally assumed the risk that his or her messages will be searched. In fact, courts have recently held that a publicized monitoring policy reduces an employee's expectation of privacy as to the contents of his desk[46] or locker.[47] For the same reasons, private sector employees would likewise fail the expectation of privacy test and be vulnerable to E-mail searches by the government. Moreover, if the government (i.e., the police, F.B.I., etc.) is voluntarily offered the contents of any public *or* private sector employee's E-mail file by a *third party* (e.g., a co-worker), then a Constitutional right is not invoked.[48]

---

43. Smith v. Maryland, 442 U.S. 735, 742 (1979).

44. *Id.* at 744. The Court has also relied on the "knowingly exposed" criterion in *United States v. Knotts*, 460 U.S. 276 (1983) (where a "beeper" had been attached to an individual's car for tracking purposes, and an automobile otherwise travels over publicly viewed roads), and in *California v. Ciraolo*, 476 U.S. 207 (1986) (where a homeowner complained of the government flying over, observing, and photographing his fenced-in backyard, otherwise observable from overhead).

45. Piller, *supra* note 2, at 118. This is because of the large volume of messages being transmitted over the system and a perception that an E-mail administrator or operator would otherwise be disinterested. This assumption is probably valid, although telephone companies, too, have little interest in any one phone call of thousands, although some interceptions do still occur for various reasons.

46. Schowengerdt v. United States, 944 F.2d 483, 488-89 (9th Cir. 1991), *cert. denied*, 112 S.Ct. 1514 (1992).

47. American Postal Workers Union v. United States Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989).

48. A recent E-mail snooping allegation may serve as an example here. At the University of Nebraska at Omaha, computer administrators allegedly read student E-mail messages without their permission, but supposedly to help law enforcement authorities. In one case, computer files of one student were turned over to police pursuing a felony investigation. *See E-mail Snooping Alleged; UNO Administrators May Have Eavesdropped*, LINCOLN J., Mar. 30, 1994. If the administrators *voluntarily* released the contents to the authorities on their own initiative (or a warrant had been properly issued), then a constitutional right would not likely be found. *See, e.g.*, "false friend" cases such as Couch v. U.S., 409 U.S. 322 (1973); United

Even if the courts find a reasonable expectation of privacy in E-mail, then the reasonableness of a particular search or seizure would then be analyzed. This analysis requires a balancing of the nature of the intrusion against the importance of the government interests justifying the intrusion. In one of the few cases where the Supreme Court has considered public employees' privacy interests, it found that a public employee has a reasonable expectation of privacy in his office desk and file cabinets.[49] In fact, the Court noted that "not everything that passes through the confines of the business address can be considered part of the workplace context."[50] But the Court also noted that the reasonableness of a "search" requires balancing the privacy interest against the government's need for supervision, control, and efficiency as an employer. A government search may be considered reasonable if there are reasonable grounds for suspecting that the search will reveal worker misconduct, and the search was limited to accomplishing the underlying objectives.[51] Thus, a decision rendered in a case involving E-mail may turn on an assessment of the reasonableness of the search and a balancing of the interests and needs. In general, courts have tended to find that an employer's needs outweigh the employee's privacy interest, and in subsequent employee search cases, the Supreme Court has found the government's interest to prevail.[52] Thus, in applying the same criteria and balancing test to E-mail, the courts may find no Constitutional privacy rights infringed.

B. State Constitutions

Like the Constitution, most state constitutions will only protect privacy rights belonging to government employees or others subject to government monitoring.[53] While most states contain

---

States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963); *see also* California v. Greenwood, 486 U.S. 35 (1988); United States v. Miller, 425 U.S. 435 (1976).

49. O'Connor v. Ortega, 480 U.S. 709 (1987).

50. *Id.*

51. *Id.* at 719.

52. In one case, the Court concluded that suspicionless drug testing of railroad employees was reasonable in the interest of railroad safety. Skinner v. Railway Labor Executive's Ass'n, 489 U.S. 602, 633 (1989). In another case, the Court upheld a drug screen program for U.S. Customs Service employees involved in such activities as drug interdiction. National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).

53. *See, e.g.*, Bianco v. American Broadcasting Co., 470 F. Supp. (N.D. Ill. 1979) (holding that an employer's electronic eavesdropping of employees did not violate an Illinois constitutional provision prohibiting interceptions by eavesdropping devices, since the constitutional provision limits only governmental activity and not private activities).

provisions similar to the Fourth Amendment, a few state constitutions do recognize an explicit right to privacy.[54] However, only one state, California, has generally provided a constitutional privacy right that can be invoked by employees subject to private sector searches. Still, New Jersey recently recognized a state constitutional right of privacy[55] which may be applied to the private sector workplace.[56] Moreover, the Alaska Supreme Court, while finding that Alaska's constitutional privacy provision does not apply to private actors, nonetheless recently noted that its constitutional provision might form the basis for a "public policy supporting privacy."[57] Thus, a trend toward more state constitutional privacy protections for private sector employees may be emerging.

In California, the courts have held that the right to privacy in the state constitution applies with equal force to those in both the private and public sector.[58] The California courts have generally held that the state constitution prohibits all incursions into individual privacy unless justified by a "compelling interest." As with the Supreme Court, there is no clear answer as to how a California court will decide an E-mail privacy claim without first knowing the employer's justification for the search. However, California law does not extend to California companies and employees if the search or seizure by the employer occurs out of state. It will be instructive, however, to analyze the state's reactions to the few E-mail privacy cases which are still pending—since all of these cases happen to reside in California.[59]

---

54. See *infra* Table 1 for the state constitutions which expressly protect privacy.

55. N.J.S.A. CONST. art. 1, par. 1. This states that "[A]ll persons are by nature free and independent and have certain natural and inalienable rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing, and protecting property, and of pursuing and obtaining safety and happiness." *Id.*

56. Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11 (N.J. 1992). In this case, the Supreme Court of New Jersey nonetheless upheld an employer's discharge of an employee following a positive drug test. *Id.* at 23.

57. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1132-33 (Alaska 1989), *second appeal*, 834 P.2d 1220. It also found that public policy entitled private employers to withhold private information from their employers. 768 P.2d at 1131-33.

58. *See, e.g.*, Porten v. University of San Francisco, 134 Cal. Rptr. 839 (1976) (finding a private university improperly disclosed a student's grades from another university to the State Scholarship and Loan Commission); *see also* Valley Bank of Nevada v. Superior Court, 542 P.2d 977 (Cal. 1975) (where similarly, a private entity was prevented from disclosing another entity's financial records).

59. See *supra* note 20, and accompanying text for a description of one California E-mail intrusion case. See *infra* notes 159 for a discussion of similar invasions of privacy.

III. FEDERAL AND STATE STATUTORY LAW: E-MAIL WIRETAPPING

Both private and public employees may turn to current federal and state statutory law to contest an employer's "right" to E-mail monitoring, but may again find little relief. The relevant federal law, although facially applicable to E-mail, may fail to protect individual privacy in this area because of possible ambiguity and the presence of several exceptions. These exceptions include the non-interstate systems exception, the prior consent exception, and the business use exception. The relevant state statutes also fail to adequately limit monitoring. Section A addresses the applicable federal statutory law. Section B discusses the pertinent state statutes.

A. Federal Statutes

The key federal law to date in this area is the Electronic Communications Privacy Act of 1986 (ECPA),[60] which bars the interception of electronic communications. The ECPA would seem to protect workers from many types of electronic monitoring including E-mail interceptions, but it is not explicit when it comes to the workplace, and it contains some exceptions that courts may determine exclude employee protection.

Congress adopted the ECPA in 1986 as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[61] commonly known as the federal wiretapping statute. The intention was to update the law's language to encompass new technologies and to expand its scope[62] to include the interception of electronic communications and stored electronic communications, such as between computers or between a computer and a human.[63] In fact, the ECPA was also intended to include coverage of private communication systems such as intracompany networks.[64]

---

60. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988)).

61. 18 U.S.C.A. §§ 2510-2520 (1970 & Supp. 1994).

62. Congress believed the ECPA was necessary because the 1968 Act initially protected only against aural interception of voice communications, and the privacy protection was limited to narrowly defined "wire" and "oral" communications. It did not cover data communications. *See* U.S. v. Gregg, 629 F. Supp. 958 (W.D. Mo. 1986) (prompting the ECPA amendments because the court found that Title III, which regulated the "interception of wire and oral communications," did not apply to the interception of telex communications; telex interceptions did not involve "aural acquisition" of defendant's communications), *aff'd*, 829 F.2d 1430 (8th Cir. 1987).

63. 18 U.S.C. §§ 2510(1), (4), (12), (17) (Supp. 1994).

64. S. REP. NO. 541, 99th Cong., 2d Sess. 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566.

The ECPA does not directly mention electronic mail, but it is included within the scope of the act's general protections. The ECPA forbids, for example, the interception of electronic communications, which, according to the legislative history, includes E-mail.[65] The ECPA further defines an "electronic communication service" as one that provides to users the "ability to send or receive wire or electronic communications,"[66] which is intended to include electronic mail companies.[67] The ECPA also comprises the Stored Wire and Electronic Communications and Transactional Records Access Act,[68] which establishes broad prohibitions on accessing and disclosing electronically-stored communications.[69]

The ECPA has three exceptions, however, that may limit its protection of employee E-mail: non-interstate systems, prior consent, and business use.

1. Interstate Systems

In the first place, the ECPA may only protect messages sent over public networks such as MCI Mail, Internet, Prodigy, or CompuServe. This is because the definition of "electronic communications" under the statute only pertains to such communication that "affects interstate or foreign commerce."[70] Intracompany E-mail systems may not be covered by the ECPA. Although Congress did intend for the ECPA to include intracompany networks, it confined this broader coverage to "wire communication," and Congress has specified that "wire communication" includes some element of the human voice.[71] Thus, a company voice mail (PBX)

---

65. *Id.* at 3568. The ECPA defines electronic communications as the "transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . ." 18 U.S.C. §2510(12) (Supp. 1994). The legislative history further clarifies that the term "also includes electronic mail, digitized transmissions, and video teleconferences." S. REP. NO. 541, 99th Cong., 2d Sess. 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

66. 18 U.S.C. § 2510(1) (Supp. 1994).

67. S. REP. NO. 541, 99th Cong., 2d Sess. 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

68. 18 U.S.C. §§ 2701-2711 (Supp. 1994).

69. *Id.* § 2701. This provision makes it unlawful for anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents unauthorized access to a wire or electronic communication while it is in electronic storage in such system. . . ." *Id.* The Act does not specifically state that electronic storage pertains to E-mail, but this provision would still protect E-mail provided as an "electronic communication service." *Id.* § 2702(a)(1).

70. 18 U.S.C. § 2510(12) (Supp. 1994).

71. *Id.* § 2510(18); S. REP. NO. 541, 99th Cong., 2d Sess. 14 (1986), *reprinted in*

may be covered, but not an intracompany E-mail system—unless that system crosses state lines or perhaps connects to an interstate network. The ECPA is not at all clear on this point, however, and thus court interpretation will be needed.

2. Prior Consent

The ECPA also allows the interception of electronic communications where "one of the parties to the communication has given prior consent."[72] Unless other parties with whom an employee is communicating allow the employer access to the messages, the employee would appear protected, assuming he or she did not give consent. But the analysis may then turn on whether or not some aspect of the employer-employee relationship might be construed to suggest that implied consent was given. Courts have found that consent may be inferred from "surrounding circumstances indicating that the [parties] agreed to the surveillance."[73]

The courts do not construe the meaning of implied consent broadly, however. In *Watkins v. L.M. Berry & Co.*,[74] an appeals court determined that a telemarketing employee's *knowledge* of her employer's *capability* of monitoring her private telephone conversations could not be considered implied consent to such monitoring.[75] Yet the court in this case did find that Watkins had consented to a company *policy* of monitoring business calls that *could* include the unintentional interception of a personal call

---

1986 U.S.C.C.A.N. 3555, 3568. This states that "the transmission of 'communications affecting interstate or foreign commerce,' are within the definition of a 'wire communication.' This language recognizes that private networks and intracompany communications systems are common today and brings them within the protection of the statute." S. REP. NO. 541, at 11-12. "[T]he term 'wire communication' means the transfer of a communication which includes the human voice at some point." Congress considers voice mail to be an example of "wire communication." *Id.* at 12. Congress does not explicitly include private networks and intracompany communications within its discussion of electronic communications. What is confusing about this distinction, however, is that the definition of "wire communication" in the Act "includes any electronic storage of such communication." 18 U.S.C. § 2510(1) (Supp. 1994).

72. 18 U.S.C. § 2511(2)(d) (Supp. 1994) The Stored Wire and Electronic Communications provisions also permit access to stored communications with the authorization "by the user of that service with respect to a communication of or intended for that user;. . . ." *Id.* § 2701(c)(2)

73. Griggs-Ryan v. Smith 904 F.2d 112, 117 (1st Cir. 1990) (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)). The court further stated that "consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." *Griggs-Ryan*, 940 F.2d at 116. This case was outside the employment context, although it concerned telephone monitoring.

74. 704 F.2d 577 (11th Cir. 1983).

75. *Id.* at 581.

for a limited time.[76] The court stated that the prior consent exception (of then Title III) does not give employers carte blanche monitoring rights, but can be used to justify monitoring business calls including the momentary interception of a personal call until the personal nature is established.[77] Thus, monitoring of business communications and the inadvertent monitoring of personal communications could be allowed if an employer has a written policy addressing E-mail monitoring. In this case, employees using the system would be considered to have given implied consent.

Yet it should be noted that implied consent would not be found if the monitoring exceeded the terms of the company's policy.[78] In other words, if the monitoring policy was designed to survey only the extent of E-mail use in the company, for example, then uncovering a breach of trade secrets may be beyond the scope of implied consent. Moreover, implied consent would not be found if an employer only suggests to the employees that monitoring *may* be done. This was the scenario in a recent telephone case where, from a telephone extension, owners of a liquor store recorded conversations of an employee suspected in an unsolved burglary of the store. In *Deal v. Spears*,[79] Newell Spears advised his employee—who had been making numerous personal telephone calls—that he might be forced to monitor her calls if abuse of the store's telephone for personal calls continued.[80] The court held that the employee's consent was not implied because she was not informed that she was being monitored, only that "they might do so in order to cut down on personal calls."[81] Other courts also hold there is an absence of implied consent where defendants argue that a plaintiff simply "should have known" that he or she was being monitored.[82] Thus, the legality of E-mail monitoring under the prior consent exception may depend on the specificity and clarity of the company's monitoring policy.

3. Business Use Exception

Perhaps most troubling for employees are provisions that—regardless of prior consent—might exclude from coverage

---

76. *Id.*

77. *Id.* at 581-82.

78. This was the case in *Watkins*, where a personal call was more than inadvertently monitored. *Watkins*, 704 F.2d at 582. The court remanded the case to determine the scope of the consent and to decide whether and to what extent the interception exceeded the consent. *Id.*

79. 980 F.2d 1153 (8th Cir. 1992).

80. *Id.* at 1156-57.

81. *Id.* at 1157.

82. Campiti v. Walonis, 611 F.2d 387, 396 (1979) (finding that there was no implied consent when a police officer used an extension phone to intercept inmates' telephone conversations).

certain types of interceptions made in the "ordinary course of business." There are two key provisions of the ECPA that address this type of exception. One provision has been relied on in telephone extension monitoring cases,[83] but may not pertain to E-mail monitoring unless telephone equipment or facilities are specifically involved. This provision essentially permits interceptions where telephone or telegraph equipment are used in the ordinary course of business.[84] Yet courts may not consider a network manager's modem, computer, or software program to be telephone or telegraph equipment, and the leasing of telephone lines may not necessarily qualify under this exemption. Even in telephone extension cases, the telephone equipment distinction has been narrowly construed.[85]

Still, employers may turn to another ECPA "business use" exception that does not specify the type of equipment, but rather allows certain interceptions by electronic communication service providers or their "agents." The section provides:

> [i]t shall not be unlawful under this chapter for an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire 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 . . . .[86]

---

83. *See, e.g.*, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (applying a provision of the ECPA in a telephone monitoring case); Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412 (11th Cir. 1986) (same); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (same).

84. The ECPA finds interceptions of electronic communications to be unlawful if accomplished through the use of an "electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (Supp. 1994). But such devices do not include:

> a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of a wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and is used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business . . . .

Id. § 2510(5)(a).

85. For example, in Epps v. St. Mary's Hosp., the court, in determining the exceptions under § 2510, distinguished a "ringdown line" from an entire extension telephone, and distinguished recording equipment used from the intercepting dispatch panel. 802 F.2d 412 (11th Cir. 1986). In Deal v. Spears, the court distinguished the use of a telephone recording device purchased from Radio Shack to fall outside the exception since the device was not provided by a telephone company. 908 F.2d 1153, 1158 (8th Cir. 1992).

86. 18 U.S.C. § 2511(23)(a)(i) (Supp. 1994).

The term "provider" would likely include public E-mail networks, such as Prodigy and CompuServe, and the term "agent" may or may not be defined to include employers who subscribe to or use their E-mail service. Companies with their own E-mail systems on their own wide area (interstate) networks could also fall under this exception as electronic communication service providers.[87]

It is the second element of both ECPA provisions—the "business use" exception—which may then be interpreted to give employers fairly broad authority to intercept and monitor E-mail messages. Of course, the law would require employers and public E-mail providers to demonstrate that a particular interception was done in the ordinary course of business—such as the rendering of service maintenance. In fact, under the section quoted above, service providers or employers would need to prove that the monitoring was necessary to render service or to protect their rights or property. Still, the courts may find that this includes such reasons as the need to prevent abuses of the system such as computer crime, system failure, or unpermitted personal use.[88]

In cases involving telephone extension monitoring, the courts have been fairly liberal in their interpretation of the business use exception. In *James v. Newspaper Agency Corp.*,[89] the court held that a newspaper's telephone monitoring program of its telemarketing employees was squarely within the business (telephone) extension exception because it was conducted for a "legitimate business purpose" designed to help employees deal with the public effectively.[90] In *Briggs v. American Air Filter Co.*,[91] where a supervisor monitored a business call where an employee divulged trade secrets to a competitor, the court held that the monitoring was within the ordinary course of business.[92]

Some courts have nonetheless limited the business use exception according to the scope of the intrusion and the nature of the

---

87. One confusing aspect is that the service provider must be using facilities for the transmission of a wire communication, which by definition, may limit this to only providers that also transport voice communications. See *supra* note 69 for the text of the section that makes it unlawful to access a facility through which an electronic communication service is provided unless authorization is given.

88. Section 2511(2)(a)(i) does not further limit the extent of monitoring by electronic communication service providers. Instead, it states only that "a provider of *wire* communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks." 18 U.S.C. § 2511(2)(a)(i) (emphasis added).

89. 591 F.2d 579 (10th Cir. 1979).

90. *Id.* at 581.

91. 455 F. Supp. 179 (N.D. Ga. 1978), *aff'd*, 630 F.2d 414 (5th Cir. 1980).

92. *Id.* at 181-82.

communication. For example, in *Watkins v. L.M. Berry & Co.*,[93] where the interception was of a *personal* call, the court followed *Briggs*, but said it would only allow the unintentional interception of a personal call, and for only a limited time until the personal nature of the call is established.[94] In *Deal v. Spears*,[95] the court found that the employer had exceeded the scope of the exception by having listened to all 22 hours of his employee's tape recorded personal calls. Even though the court agreed that the employer had a "legitimate business reason" for listening (i.e., employee's suspected burglary involvement and abuse of phone privileges), the court agreed with the *Watkins* court in concluding that the employer might have legitimately monitored the calls only to the extent necessary to determine that they were personal and in violation of store policy.[96]

Thus, if the courts analogize E-mail interceptions to telephone extension monitoring, employers may be able to prove a legitimate business reason for the monitoring, provided that the monitoring does not include reading personal E-mail in its entirety. Of course, personal E-mail would still be vulnerable to some degree of observation, and unless the contents of the messages are divulged or clearly acted upon, it may be difficult to prove that intercepted personal messages were completely read. Even Congress acknowledges that computer monitoring may be more difficult to limit than telephone conversations.[97]

In addition to the prohibitions on interception, it should also be noted that the ECPA further prohibits the intentional *disclosure* of the contents of an electronic communication obtained through an illegal interception.[98] This would include any information concerning the "substance, purport, or meaning" of the communication.[99] In *Deal v. Spears*, where one of the liquor store

---

93. 704 F.2d 577 (11th Cir. 1983).

94. *Id.* at 581-82.

95. 980 F.2d 1153 (8th Cir. 1992).

96. *Id.* at 1158. The court did, however, refuse to grant punitive damages, considering that the employee was warned, that the employer had a purpose to solve a crime, that the employer had asked a law enforcement officer in advance about the legality of recording, and that the tapes were only played to the employee. *Id.* at 1159.

97. "It is impossible to 'listen' to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation." S. REP. NO. 541, 99th Cong., 2d Sess. 31 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568. This would "require a somewhat different procedure than that used to minimize a telephone call." *Id.* at 3583.

98. 18 U.S.C. § 2511(1)(c). This attaches liability when a party "intentionally discloses . . . to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained" through an interception illegal under the Act. *Id.*

99. *Id.* § 2510(8).

owners had disclosed only the general nature of the taped contents to the plaintiffs' spouses, the disclosure fell within the statute's purview.[100] Thus, if an employee is successful in showing that an E-mail interception was in violation of the Act, he or she may also then recover damages[101] if the employer showed or even discussed the contents of a message with others.

Finally, for government employees and employees subject to government interceptions of their E-mail, the ECPA does provide greater relief by requiring that a warrant be issued first.[102] If a warrant is issued, however, providers would be required to disclose the contents of an electronic communication in electronic storage. Not all personal communications beyond the application of the search warrant may be "seized" and read, however. This proposition was recently tested in a March 1993 case where a judge ruled that Secret Service agents had indeed violated the ECPA when they read (and destroyed) additional stored electronic messages—including personal E-mail—on computers they had seized with a warrant.[103]

B. State Statutes

Most states also have statutes that limit the interception of electronic communications, and states are also free to enact laws that are more restrictive and thus provide even greater privacy protections than the federal law. Unless a conflict between the laws exists, the state law will prevail.[104]

Many states have laws that, in fact, incorporate the provisions of the ECPA, including the "prior consent" and "business use" exceptions.[105] Yet several states also require the prior con-

---

100. Deal v. Spears, 980 F.2d at 1156, 1158 (8th Cir. 1992).

101. Under any of these sections of the ECPA, a successful civil plaintiff may recover the greater of either A) actual damages plus any profits made by the violator, or B) the greater of $100 a day for each day of violation or $10,000. 18 U.S.C. § 2520(c)(2)(A), (B) (Supp. 1994). Punitive damages, attorney fees, and other litigation costs reasonably incurred are also allowed. *Id.* § 2520(b)(2), (3).

102. 18 U.S.C. § 2703(a) (Supp. 1994).

103. The computers belonged to an individual suspected of a computer crime conspiracy to disrupt 911 systems. Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993). The court held that the Secret Service had violated provisions of the Stored Wire and Electronic Communications and Transactional Records Access Act (of the ECPA), 18 U.S.C. §§ 2701-2711. *Steve Jackson Games, Inc.*, 816 F. Supp. at 443.

104. Federal law does not pre-empt state law under the Supremacy Clause of the U.S. Constitution. *See, e.g.*, Ann K. Bradley, *An Employer's Perspective on Monitoring Telemarketing Calls: Invasion of Privacy or Legitimate Business Practice?*, 42 LAB. L.J. 259 (May 1991).

105. *See infra* Table 2.

sent of "all parties"[106] which could severely limit employee E-mail monitoring if the consent of the party with whom an employee is communicating must also give his or her consent.[107] Many states also only exempt communications *common carriers* under their business use exceptions, rather than "electronic communication service" providers.[108] The term "common carrier" could arguably preclude from these exceptions any service providers such as Prodigy, CompuServe, and value-added carriers that are not identified and regulated as "common carriers."[109] In this sense, employees in a few states may find greater protection from monitoring under state law.[110]

Yet in other states there are no similar wiretap provisions that may protect employees,[111] and in one state, Nebraska, employers are specifically exempted under that state's wiretapping provision. Nebraska, which supports many telemarketing firms and has a fairly liberal telecommunications regulatory environment, permits "an employer on his, her, or its business premises . . . to intercept, disclose, or use" an electronic communication while "in the normal course of his, her, or its employment. . . ."[112] The law limits the monitoring, but does permit the monitoring for "performance control checks as long as reasonable notice of the policy of random monitoring is provided to their

---

106. *Id.*

107. Unless, of course, the other party is also an employee of the same company and "implied consent" is found.

108. *See infra* Table 2.

109. A communications common carrier provides transmission service facilities to the general public—such as a telephone or telegraph company—and is regulated by federal and state regulatory agencies. *See, e.g.*, W. JOHN BLYTH & MARY M. BLYTH, TELECOMMUNICATIONS: CONCEPTS, DEVELOPMENTS, AND MANAGEMENT 329 (2d ed. 1990).

110. It should be noted that while many states limit the business use exemption, employees may still lose protection where prior consent is found.

111. See *infra* Table 2 for those states not listed or that do not clearly identify a business use exemption (Prior Consent Exemption Only).

112. NEB. REV. STAT. § 86-702(2)(a) (1992). This specifically states:

> It shall not be unlawful . . . for an employer on his, her, or its business premises, for an operator of a switchboard, or for an officer, employee, or agent of any provider, the facilities of which are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his, her, or its employment while engaged in an activity which is a necessary incident to the rendition of his, her, or its service or to the protection of the rights or property of the carrier or provider of such communication services. Such employers and providers shall not utilize service observing or random monitoring except for mechanical, service quality, or performance control checks as long as reasonable notice of the policy of random monitoring is provided to their employees.

Id.

employees."[113]

A few states have considered stricter laws that would specifically constrain the monitoring practices of private sector employees,[114] although many of these measures have generally been defeated by corporate lobbyists.[115] A law was proposed in Texas, that did not pass, which would have protected privacy by prohibiting secret electronic surveillance and unreasonable searches, and by preventing employers from obtaining unnecessary private information about employees.[116] California recently attempted to pass a law to specifically prohibit telephone companies from monitoring or recording their employees' conversations, but the bill was vetoed by the Governor.[117] Other states have passed laws that restrict surveillance, but do not necessarily protect E-mail or computer files.[118]

One of the most comprehensive pieces of legislation currently proposed is in Massachusetts. Earlier bills[119] did not pass or were struck down as being overly broad,[120] but a new bill has been introduced in 1994.[121] It essentially provides that employers can only monitor their employees if they give written notice about the electronic monitoring. In addition, the Massachusetts bill requires employers to inform the monitored employees of the frequency of surveillance, the type of data to be collected, and how the employer will use the monitoring. Georgia has also introduced legislation this year to provide restrictions on electronic monitoring by employers,[122] and New York introduced a bill that would prohibit employers from operating electronic monitoring and/or surveillance equipment for observing "non-work

---

113. *Id.*

114. *See* Dworkin, *supra* note 31, at 80.

115. Casarez, *supra* note 17, at 38.

116. Dworkin, *supra* note 31, at 80.

117. 1993 CA A.B. 2271 (vetoed Oct. 11, 1993). The law would have prohibited "any officer, employee, or agent of a telephone corporation from monitoring, recording, wiretapping, eavesdropping, or otherwise documenting any conversation of its employees, except . . . a telephone corporation may monitor telephone conversations of its employees solely for the purposes of quality assurance and training."

118. For example, Nevada passed a law that prohibits surreptitious monitoring of other people, but it is limited to private conversations. NEV. REV. STAT. ANN. § 200.650 (Michie 1991). Connecticut passed a law that prevents electronic surveillance of areas provided for the "health or personal comfort of employees or for the safeguarding of their possessions." CONN. GEN. STAT. ANN. § 31-48b(b) (West 1987). Although the state law does not specify E-mail, it is considered to apply to the surveillance of related areas such as lounges, locker rooms, and rest areas, and it does not consider prior notification as an exception. Dworkin, *supra* note 31, at 80.

119. Such as 1991 MA H.B. 4457.

120. Opinion of the Justices, 358 Mass. 827, 260 N.E. 740 (1970).

121. 1994 MA H.B. 1800. As of June 1994, the bill had not passed the House.

122. 1994 GA S.B. 646 (introduced Feb. 15, 1994).

related activities."[123] No other bills addressing electronic monitoring are currently pending in any other state. Currently, private sector employees in most states may generally be left unprotected under state law.

IV. COMMON LAW AND E-MAIL INTRUSION

In the absence of clear statutory or constitutional rights to E-mail privacy, employees may be able to find relief in a common law cause of action known generally as "invasion of privacy."[124] This common law cause of action has been fairly recently recognized by courts and legislative bodies as a means of protecting against unwarranted intrusions into one's affairs; essentially, one who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other. Some states recognize a common law right of privacy which may protect private employees.[125] This section discusses the tort of intrusion into seclusion, the tort's elements, and some of the conditions courts have adopted as criteria in deciding a case involving an intrusion into seclusion.

Of four generally recognized privacy torts,[126] the specific tort known as "intrusion into seclusion or private affairs" would be the most applicable to the interests of E-mail users. This tort provides that "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his or her private affairs or concerns, is subject to liability to the other for invasion of his or her privacy, if the intrusion would be highly offensive to a reasonable person."[127] This right of privacy would arguably include the right to be free from unreasonable intrusions by employer searches.[128]

---

123. 1994 NY A.B. 10705 (introduced April 1, 1994). This may apply to personal E-mail messages if considered to be "non-work related activities."

124. Privacy law began as a common law tort that grew from a set of rights broadened to mean "the right to enjoy life—the right to be let alone." *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 192, 192 (1890).

125. 2 PRIVACY LAW AND PRACTICE ¶ 9.02[3] (George B. Trubow, ed., 1987).

126. In 1960, Dean William L. Prosser synthesized hundreds of cases recognizing a right of privacy actionable in tort. William L. Prosser, *Privacy*, 28 CALIF. L. REV. 383 (1960). His widely accepted analysis (reflected in RESTATEMENT (SECOND) OF TORTS § 652B (1977)) breaks down the privacy invasion lawsuit into four separate torts: 1) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness, 2) Publicity, which places a person in a false light in the public eye, 3) Public disclosure of embarrassing, private facts about the plaintiff, and 4) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

127. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

128. 2 PRIVACY LAW AND PRACTICE, *supra* note 125 (citing Love v. Southern Bell

Until 1979, however, few employees brought suits against their employers.[129] Since then, there has been a dramatic upsurge in privacy litigation.[130] In general, employee privacy suits under common law have concerned such matters as drug testing[131] and polygraph testing,[132] where the courts appear to be supportive of employers' attempts to create a safe working environment.[133] Other types of employee privacy suits have concerned the photographing of employees,[134] where courts have generally allowed employers to photograph their employees over the employees' objections when the employer has shown a legitimate purpose for taking the pictures.[135]

Although the courts do not specifically rule according to any list of criteria, several factors have evolved for use in determining a common law right against intrusion. Courts tend to consider: 1) whether there was an intentional intrusion;[136] 2) the location and private nature of the activity involved;[137] 3) whether the in-

---

Tel. and Tel. Co., 263 So. 2d 460 (La. Ct. App.), *cert. denied*, 266 So. 2d 429 (La. 1972)).

129. *See* David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the '90s*, 23 J. MARSHALL L. REV. 591 (1990) (discussing the history of suits brought by employees for invasion of privacy).

130. *Id.*

131. *See, e.g.*, Luedtke v. Nabors Alaska Drilling Inc., P.2d 1123 (Alaska 1989) (where employer testing for drug use was found not actionable as an invasion of privacy because the intrusion was not unwarranted), *second appeal*, 834 P.2d 1220.

132. *See, e.g.*, Ballaron v. Equitable Shipyards, Inc., 521 So. 2d 481 (La. Ct. App. 1988), *cert. denied*, 522 So. 2d 571 (La. 1988); Gibson v. Hummel, 688 S.W.2d 4 (Mo. Ct. App. 1985) (requiring a polygraph test did not constitute outrageous conduct where employee admitted to stealing during the test).

133. 62A AM. JUR. 2D *Privacy* § 61 (1990).

134. *See, e.g.*, Thomas v. General Elec. Co., 207 F. Supp. 792 (W.D. Ky. 1962) (holding that the employer could take motion pictures of employees without their consent for purposes of studies to increase efficiency and promote the safety of employees).

135. 62A AM. JUR. 2D, *supra* note 133.

136. This would include surreptitious surveillance such as wiretapping or eavesdropping. *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971); *see also* Marks v. Bell Tel. Co., 460 Pa. 73, 331 A.2d 424 (Pa. 1975) (where, in the absence of an intentional overhearing of a private conversation by an unauthorized party, the tort of invasion of privacy was not committed).

137. For example, courts have applied a different standard to privacy in the home and in similar quarters. *See, e.g.*, Byfield v. Candler, 125 S.E. 905, 906 (Ga. Ct. App. 1924) (intrusions into overnight quarters on a train or ship by management); Newcomb Hotel v. Corbett, 108 S.E. 309, 309-10 (Ga. Ct. App. 1921) (intrusions into guest rooms by hotel management). Yet if individuals are in a public place, there may be no cause of action. *See* Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482 (D.C. Me. 1988) (photographing passenger in a public place). Even if the plaintiff is considered to be in a public place, however, some consideration is given to the private nature of the activity. For example, in Lewis v. Dayton Hudson Corp., 339 N.W.2d 857 (Mich. Ct. App. 1983), the court considered the private

trusion was "highly offensive to the reasonable person;"[138] and 4) whether the infringer had a legitimate purpose warranting the intrusion.[139]

The first condition may not be difficult to meet, although it should be noted that any *un*intentional access to an E-mail message by a system administrator during system maintenance, for example, would certainly defeat an employee's privacy claim. In terms of the location and private nature involved, company lawyers may successfully argue that E-mail at the work location is within the work context and should not be deemed private as such. Moreover, an employee may have difficulty proving that any private communication was actually read.[140]

The last two factors that have been considered by courts present greater difficulty for employees. For example, an employee would have to convince the court that the employer's intrusion was "highly offensive" to a reasonable person. Courts may not consider the accessing and reading of employee E-mail to be "highly offensive," particularly if a court finds that the employee had no expectation of privacy in his or her E-mail.[141] Yet the courts may compare the use of a personal computer E-mail password to

---

nature of one's activity in a case involving the observations of a store patron trying on clothes in a dressing room—despite the fact that the activity occurred on store property. In general, that which is intruded upon must be entitled to be private. WILLIAM L. PROSSER & W. PAGE KEETON, THE LAW OF TORTS 855 (5th ed. 1984).

138. *See* RESTATEMENT, *supra* note 127, § 652B cmt d (stating that an intrusion must be "highly offensive to the ordinary reasonable man" which explicitly requires this criterion. Courts may also take into account the nature of the intrusion, such as whether it "was done in a vicious and malicious manner not reasonably limited and designed to obtain the information needed . . . " and was "calculated to frighten and torment . . . ." Pinkerton Nat'l Detective Agency, Inc. v. Stevens, 122 S.E.2d 119, 123 (Ga. Ct. App. 1963). Some courts have applied or recognized an even more stringent requirement of "outrageous conduct," where the conduct must be so outrageous in character and so extreme in degree as to go beyond all possible bounds of decency and be regarded as atrocious and utterly intolerable in a civilized community. RESTATEMENT, *supra* note 127.

139. *See, e.g.*, Horstman v. Newman, 291 S.W.2d 567 (Ky. Ct. App. 1956) (per curiam) (landlord may enter tenant's land to demand rent due); Engman v. Southwestern Bell Tel. Co., 631 S.W.2d 98 (Mo. Ct. App. 1982) (telephone company may enter home of individual who had not paid the phone bill, in order to remove the company's phones); Schmukler v. Ohio Bell Tel. Co., 116 N.E.2d 819 (Ohio C.P. 1953) (holding that there was no invasion of privacy where telephone company monitored residential phone after discovering the number of calls to be excessively high, where the monitoring was for a short period of time and was done for business purposes).

140. *See* Marks v. Bell Tel. Co., 331 A.2d 424, 431 (Pa. 1975) (finding even though the police department recorded all of the plaintiff's incoming telephone calls, the plaintiff could not recover without proving that some private conversation was either heard or replayed).

141. For an analysis of how courts might consider an expectation of privacy relative to company E-mail, see *supra* 45-53 and accompanying text.

the use of a padlock on a locker, as in *K-Mart Corp. v. Trotti*,[142] where a Texas court found that an employer unreasonably intruded on an employee's privacy when the employee's co-workers searched her locker which was secured with her own lock.[143] The courts may also find an employee E-mail search to be unreasonable if no advance notification was given, or a union official was not present.[144] Still, the courts may consider the offensiveness of the intrusion in light of the legitimate purpose criterion.[145] For example, in *Oliver v. Pacific Northwest Bell Telephone Co.*,[146] the court found that the "highly offensive" standard was not met where the employer monitored telephone conversations for the purposes of evaluating performance and whether or not an employee was disclosing documents to a competitor.[147] For this reason, a common law decision may ultimately hinge on a finding of a legitimate business purpose. As with the ECPA exceptions, an employer may easily satisfy this criterion by producing reasons for the interceptions that a court may find persuasive—such as the need to assess performance, protect against theft,[148] search for violations in disclosing trade secrets,[149] obtain information in a

142. 677 S.W.2d 632 (Tex. Ct. App. 1984), *writ of error denied*, 686 S.W.2d 593 (Tex. 1985).

143. 677 S.W.2d at 637. The court held that "the element of a highly offensive intrusion is a fundamental part of the definition of an invasion of privacy." *Id.*

144. *See, e.g.*, International Nickel Co., 50 Lab. Arb. 65 (Shister 1967) (finding that when a company opened and searched the locker of an employee, there was no invasion of privacy because the company had a justified reason for opening the locker and there was a union representative present when the company opened the locker); B.F. Goodrich v. United Ass'n of Journeyman and Apprentices, Local 195, 70 Lab. Arb. (BNA) 326 (1978) (Oppenheim, Arb.); *see also* 2 PRIVACY LAW AND PRACTICE, *supra* note 125, ¶ 9.02[3] (citing the above cases).

145. Although it is argued that the purpose factor is too often merged with the question of outrageousness or offensiveness. *See* 1 PRIVACY LAW AND PRACTICE ¶ 1.06 (George B. Trubow, ed., 1986).

146. 632 P.2d 1295 (Or. Ct. App. 1981).

147. *See also* Froelich v. Werbin, 509 P.2d 1118 (Kan. 1968); *second appeal*, Froelich v. Adair, 516 P.2d 993 (Kan. 1973); *third appeal*, Froelich v. Werbin, 548 P.2d 482 (Kan. 1976), where the Kansas Supreme Court considered an intrusion to be offensive when a hospital orderly collected a hair sample from a patient's hairbrush for the purpose of establishing the patient's homosexuality. The dissenting opinion stated that the purpose of the intrusion was irrelevant. 516 P.2d at 998.

148. A search for stolen property by an employer has also been held not to be an unreasonable invasion of privacy. *See* 2 PRIVACY LAW AND PRACTICE, *supra* note 125, ¶ 9.02[3] (citing Cherkin v. Bellevue Hosp. Ctr., 479 F. Supp. 207 (S.D.N.Y. 1979)). *Cf.* K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984), *writ of error denied*, 686 S.W.2d (Tex. 1985) (holding that mere suspicion that an employee stole merchandise was insufficient to justify a search of the employee's locker without consent).

149. For a case where there was wiretapping by a company in order to determine whether an employee was disclosing confidential company information, see Oliver v. Pacific N.W. Bell Tel. Co., 632 P.2d 1295 (Or. Ct. App. 1981).

business emergency, or simply promote efficiency.[150]

There are other factors that may also affect recovery, such as whether or not the employee must show anguish and suffering as a result of the privacy invasion.[151] The courts may also consider whether or not the employee consented (explicitly or implicitly) to the monitoring,[152] and whether or not the search was in accordance with an announced inspection policy.[153] In addition, a decision may turn on an analysis of common law privilege. Here, a court may find that within the employer-employee relationship, certain communications constitute a conditional privilege, possibly giving an employer justification in examining E-mail messages as information that affects a sufficiently important interest of the company.[154] Courts have not expressly adopted common law privileges in "intrusion upon seclusion" actions, but such an analysis may occur.[155]

Finally, in applying various criteria, the courts may specifically analogize employee E-mail intrusions under common law to common law actions associated with the opening of personal mail, eavesdropping, and recording of conversations.[156] Few cases appear to exist that address a common law cause of action associat-

---

150. *See, e.g.*, Thomas v. General Elec. Co., 207 F. Supp. 792 (W.D. Ky. 1962) (finding a legitimate business interest in photographing employees without their consent for purposes of a study to increase efficiency). Note also that an employer may defend its monitoring actions by citing the RESTATEMENT (SECOND) OF AGENCY §§ 380-398 (1957), which indicates that an employee owes a duty of loyalty and a duty to act with reasonable skill and care to the employer.

151. *See, e.g.*, Hoth v. American States Ins. Co., 735 F. Supp. 290, 292 (N.D. Ill. 1990) (finding that the plaintiff failed to state a cause of action in Illinois for invasion of privacy where an employer searched his desk and file cabinets because the employee suffered no anguish and did not allege that the employer lacked authority to conduct the search).

152. PROSSER & KEETON, *supra* note 137, at 867.

153. 2 PRIVACY LAW AND PRACTICE, *supra* note 125 (citing Cherkin v. Bellevue Hosp. Ctr., 479 F. Supp. 207 (S.D.N.Y. 1979), where a court held that an employer may search an employee's purse in accordance with an announced inspection policy).

154. *See* Senogles v. Security Ben. Life Ins. Co., 536 P.2d 1358 (Kan. 1975) (holding that an insurance claimant consented to a reasonable investigation upon filing an injury claim, and therefore, there existed a privileged relationship between the claimant and the investigators).

155. 1 PRIVACY LAW AND PRACTICE, *supra* note 145, ¶ 1.06[5].

156. Courts may also compare E-mail to a locker or desk drawer. For a case which involved an employer having searched an employee's locker, see K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984), *writ of error denied*, 686 S.W.2d 593 (Tex. 1985). It is also possible that an E-mail message may be likened to a bulletin-board notice, in which case protection would not likely be found. Note that because telephone eavesdropping and wiretapping cases are generally subject to constitutional and statutory law, courts do not often apply common law to these cases.

ed with privacy and the mail. Yet, in *Vernars v. Young*,[157] a tort law claim of invasion of privacy was considered valid where a corporate officer opened and read a fellow corporate employee's mail which was delivered to the corporation's office and marked personal. This case suggested that a reasonable expectation of privacy under common law may exist in one's mail.[158] Other related cases involving eavesdropping and recordings, however, reveal only little relief for employees, since a legitimate business purpose often prevails.[159] The courts may nonetheless take into account whether or not the intercepted communications were subsequently disclosed and whether the employer instigated the action. In *Beard v. Akzona, Inc.*,[160] for example, a secretary was fired after her husband, also an employee, turned over to their employer telephone tape recordings of her conversations with a fellow employee with whom she was having an affair. No invasion of privacy was established because the tapes were not heard by anyone other than the employer's managerial staff, and the employer did not instigate the deception. In this sense, a court may find no invasion of privacy with E-mail if a network manager, on his or her own initiative, turns E-mail files over to corporate management, and the contents of the messages are not publicly disclosed.

To date, no court has considered whether E-mail interception constitutes an unreasonable, offensive intrusion into the private affairs of workers.[161] The few cases that exist concerning E-mail searches have been brought under suits of wrongful termination (resulting from the employer having read the mail),[162] ECPA

---

157. 539 F.2d 966 (3d Cir. 1976).

158. The *Young* court cited a telephone wiretapping case, Marks v. Bell Tel. Co., 331 A.2d 424 (Pa. 1975), commenting that "[j]ust as private individuals have a right to expect that their telephonic communications will not be monitored, they also have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons." Vernars v. Young, 539 F.2d at 969. In *Marks*, however, privacy rights were not considered infringed because no private conversation was intentionally overheard. 331 A.2d at 424.

159. *See, e.g.*, Schmukler v. Ohio Bell Tel. Co., 116 N.E.2d 819 (C.P. 1953) (holding that there was no actionable invasion of privacy where a telephone company monitored a residential phone after discovering that there was an excessively high number of calls being made, where the monitoring was done for a short time and was for business purposes only).

160. 517 F. Supp. 128 (E.D. Tenn. 1981).

161. Casarez, *supra* note 17, at 37.

162. See Dean, *supra* note 8, at 11 which mentions a case whereby Nissan Motor Company was sued because it allegedly fired a pair of employees after reading their personal E-mail messages on the company's system. A California court rejected the privacy claim in Bourke v. Nissan Motor Corp., No YC 003979, slip op. (D.C. Cal. 1993). *See also* Michael Furey et al., *Overview: More Whistleblowers?*, NEW JERSEY L.J., Apr. 11, 1994, at 4.

violation,[163] or passing trade secrets.[164] These cases have largely been thrown out, settled out of court, or are still pending. Thus, while the courts have generally tolerated the surveillance of employees, at least where a legitimate business interest is found, the courts are uncertain as to how they will treat and balance employer and employee interests relative to E-mail searches.

V. PENDING LEGISLATION

This section briefly discusses two bills that have been introduced in Congress to address E-mail and other forms of electronic monitoring of employees. Legislation was first proposed several years ago when the complaints of workers from airline reservation agents, secretaries, telephone operators, and a broad range of blue-collar America first registered in Washington, D.C. But only recently have the bills caught the interest of lawmakers and the White House.[165]

The Privacy for Consumers and Workers Act, sponsored by Senator Paul Simon (D-Ill.),[166] and its companion bill in the House,[167] were originally drafted to prevent telephone companies and telemarketing firms from monitoring the telephone calls of operators and telemarketers. They were later revised to curb snooping on employees via video cameras. But recent revisions expand the scope of the legislation to cover all kinds of computer communications, including E-mail and voice mail.[168]

The proposed law would limit monitoring in several ways, including the following: 1) employers would have to tell new em-

---

A wrongful-termination charge also applied to cases involving Alana Shoars, formerly an E-mail administrator at Epson America, who was allegedly fired for complaining about her boss reading the supposedly private E-mail of Epson employees. Shoars v. Epson Am., Inc., No. SWC 112749, slip op. (D.C. Cal. 1990). The employee who Epson fired filed a class action suit, Flanagan v. Epson Am., Inc., No. BC 007036, slip op. (D.C. Cal. 1990), for invasion of privacy on behalf of a large group of Epson employees who had their electronic mail read by management. Both Epson cases were dismissed by lower courts, but are currently on appeal. Piller, *supra* note 2, at 122.

163. See *supra* note 102 and accompanying text for a discussion of a case which involved electronic mail and an ECPA violation.

164. *See, e.g.*, Dean, *supra* note 8, at 11 (discussing a case where Borland International sued its former employee Eugene Wang for sending trade secrets on electronic mail to a competitor); *Electronic Mail Raises Issues*, *supra* note 17, at A-7 (mentioning a case where a computer software company called Mentor Graphics sued two former employees for sending trade secrets to a competitor).

165. Blackman & Franklin, *supra* note 1, at 5.

166. S. 984, 103d Cong., 1st Sess., 139 CONG. REC. E1077 (1993) (introduced by Rep. Pat Williams (D-MT)).

167. H.R. 1900, 103d Cong., 1st Sess., 139 CONG. REC. E1077 (1993) (introduced by Rep. Pat Williams (D-MT)).

168. Brown, *supra* note 32, at 6.

ployees how they might be monitored and how the collected data would be used;[169] 2) employers would be required to give advance notice (day and hour) that monitoring will take place[170] (House version:[171] notice not required to specify day/hour); 3) The total time that an employee could be monitored would be capped at two hours per week[172] (House version: unlimited during the first 60 days of employment, 40 times/month for first two years, and 15 times/month thereafter),[173] and; 4) Periodic or random monitoring of long-term employees (over 5 years) would be prohibited[174] (House version: continues at 15 times/month).[175]

The legislation also requires that notice be given to others (non-employees) who may also be monitored[176] (which may pose interesting difficulties in the case of E-mail addressees and senders). Employers may only collect and review data limited to an employee's work,[177] and cannot intentionally engage in electronic monitoring of an employee engaged in First Amendment rights.[178] In addition, no action may be taken by the employer based on any personal data that was illegally obtained.[179] The legislation also does not require advance notice if an employer suspects the employee is engaged in unlawful activity, willful gross misconduct, or conduct that would have a "significant adverse effect" on the employer or other employees.[180] It allows employers to access information in case of "immediate business needs."[181] Finally, it provides exceptions for financial institutions, securities firms, the intelligence community, and gambling facilities.[182]

The proposed legislation has so far attracted many co-sponsors, but has also spurred considerable debate. The Department of Labor, for instance, has not been in favor of the legislation, partly because it considers the bills to contain too many unclear terms

---

169. S. 984, *supra* note 166, § 4(B).

170. *Id.* § 4(B)(3).

171. The House version underwent several modifications in early 1994 that are reflected here. *See, e.g., Section by Section Analysis of the Substitute Privacy for Consumers and Workers Act (HR 1900)*, DAILY LAB. REP., Feb. 24, 1994, at d32.

172. S. 984, *supra* note 166, § 5(B)(2). New employees may be monitored for no more than 60 days. *Id.* § 5(B)(1).

173. H.R. 1900, *supra* note 167, § 5.

174. S. 984, *supra* note 166, § 5(B)(3).

175. H.R. 1900, *supra* note 167, § 5.

176. S. 984, *supra* note 166, § 4(E).

177. *Id.* §§ 6(B), 10(A).

178. *Id.* § 10(C).

179. *Id.* § 8(a).

180. *Id.* § 5(C)(1).

181. *Id.* § 9(A).

182. *Id.* § 13(C).

and overly broad definitions that pertain to management practices in which personal employee data do not have relevance.[183] Others consider the bills to be unnecessarily burdensome for small businesses and difficult to interpret and administer.[184] The telephone companies, including AT&T, are especially speaking out against the measure.[185] They are concerned about the impact of the bills on E-mail management and usage. They argue that the legislation could cripple the electronic messaging business. Thus, with such opposition, the legislation may not just yet succeed in providing relief for E-mail users.

Another bill introduced in Congress that has not gained as much attention but is still under consideration is the Telephone Privacy Act of 1993, introduced by Senator Dale Bumpers (D-AR).[186] This bill would do essentially the opposite, making it lawful to intercept an electronic communication where "such person is an employer or its agent engaged in lawful electronic monitoring of its employees' communications made in the course of the employees' duties."[187] The bill has not advanced, but its introduction indicates that the matter is still open to debate and may not be easily settled.

VI. CONCLUSIONS

Current law thus appears to generally favor employers when it comes to E-mail monitoring in the workplace. Constitutional privacy rights only pertain to government interceptions, and federal statutory law does not appear to provide protection for interceptions within an intracompany system. Prior consent and business use exemptions of federal and state statutory laws may be construed to permit monitoring. State laws specifically addressing the E-mail issue are lacking, and a common law right of privacy may not be found to protect employee E-mail interests. Unless the courts provide a precise interpretation of the existing law in favor of employee privacy interests, or adequate legislation is passed, employees may be at the mercy of employers who take an active role in browsing through their E-mail. In fact, more employers may take advantage of this "new" opportunity once they under-

---

183. *See* Jennifer J. Laabs, *Surveillance: Tool or Trap?*, 71 PERSONNEL J. 96 (June 1992) (discussing the position that the Department of Labor has taken).

184. *See, e.g., Pros, Cons of Privacy Bill Explored During Senate Hearing*, Daily Lab. Rep., (BNA) June 23, 1993 (quoting a top executive who testified at the Senate hearing that the bill would be hard on small companies, and the bill would be difficult to interpret).

185. *CWA Calls Monitoring 'Menace;' Bill Would Force Companies to Disclose Monitoring Practices*, COMM. DAILY, June 24, 1993, at 3.

186. S. 311, 103d Cong., 1st Sess., 139 CONG. REC. S1390 (1993).

187. *Id.* § 2 (proposing to amend 18 U.S.C. § 2511(2)(d)).

stand that it may not be unlawful.

Despite the fact that Congress is considering passing laws which may help define what is acceptable monitoring in the workplace, these laws are inadequate in prescribing what is permissible E-mail workplace monitoring. This section first analyzes the bills which Congress is contemplating and asserts that these bills are inadequate. This section then proposes federal legislation with specific guidelines for employers as a solution which offers a balanced approach to the problem of workplace monitoring.

A. Legislative Solutions

E-mail presents a difficult case for lawmakers because it falls somewhere between a telephone call and a written correspondence. Some business people may feel comfortable with an employer's right to examine written material, but would not sanction listening in on telephone conversations. Yet case law generally permits telephone extension monitoring,[188] while mail is afforded greater privacy protection.[189] While both employers and employees have valid concerns about E-mail privacy, striking a balance may not be easy.

The answer may exist in adopting a legislative solution, but only if the law is carefully crafted and clearly applicable to E-mail and similar electronic storage systems. States may act now by proposing laws aimed at placing restrictions on monitoring. But because corporate communications cross state lines, a federal policy should also be adopted to provide uniform protections.

The Privacy for Consumers and Workers Act,[190] currently pending in Congress, addresses many of the concerns and uncertainties raised by the existing laws. As with the rulings under common law, employers would have to steer clear of communications that are not work-related,[191] and could not act on any personal information that may be unintentionally encountered.[192] The legislation requires advance notice, yet does not go so far as to prevent surreptitious monitoring to uncover suspected miscon-

---

188. See *supra* notes 74-77, 97, 151-55 and accompanying text for discussions of telephone extension monitoring.

189. *See, e.g.*, Vernars v. Young, 539 F.2d 966 (3d Cir. 1976) (finding a cause of action for invasion of privacy may be maintained if an unauthorized person opens the mail of another). For a discussion of the *Young* case, see *supra* notes 156-57. *See also* Annotation, *Opening, Search, and Seizure of Mail*, 61 A.L.R. 2d 1282 (1958 & Later Case Service 1984 & 1993) (analyzing the search and seizure of mail under the U.S Constitution).

190. S. 984, *supra* note 166; H.R. 1900, *supra* note 167.

191. *Id.* §§ 6(B), 10(A).

192. *Id.* § 8(a).

duct.[193] Finally, it provides protections that would apply to all operations, whether intrastate or interstate, and generally does not allow for any waivers (i.e., consent) by employees of their rights under the law.[194]

Unfortunately, the Privacy for Consumers and Workers Act may also be too narrow in scope and may not adequately balance the needs of both employers and employees. The specific restrictions that limit monitoring to only new employees and to specified amounts of time or observations (i.e., forty times a month[195]) are too inflexible and do not take into account the type of business operation. For example, allowing unrestricted monitoring of new employees, within the first sixty days, and no monitoring of those beyond five years of employment[196] may be too specific, not accounting for special needs or the privacy rights of new employees. Moreover, monitoring of *all* employees for *more* than two hours per week[197] may be justifiable and even necessary for polling and survey research organizations and telemarketing firms, which are not exempted under the legislation. Yet allowing college administrators the ability to monitor untenured faculty E-mail for up to two hours per week would hardly seem acceptable.[198]

There is also no agreement so far between the House and Senate bills as to whether or not employees must be given advance notice of a company's monitoring in general, or whether the employees must be given the exact days and hours when the monitoring will take place. Some adequate compromise will need to be achieved on this point. Precise notice may go too far in stripping employers of the ability to access company computer files outside of specified monitoring periods. The ability to manage and control safety, quality, and efficiency could be negatively affected. Yet having only a general company policy with vague monitoring procedures may go too far in allowing employers the ability to

193. *Id.* § 5(C)(1).

194. *Id.* § 12(d).

195. H.R. 1900, *supra* note 167, § 5.

196. S. 984, *supra* note 166, § 5(B)(1), (3).

197. *Id.* § 5(B)(2).

198. The accessibility of college faculty E-mail is already being scrutinized. Karl Bates, *U-M Takes Stand: E-mail is Private*, ANN ARBOR NEWS, Jan. 12, 1994, at B1, B3. Some government offices are declaring that government employee E-mail is subject to the Freedom of Information Act and must be available to the public and the press to the same extent as other government records. *Id.* Whether the E-mail of employees of state-supported institutions must be available to the public is unclear. *Id.* The University of Michigan recently addressed this issue and maintained that its E-mail is off-limits, arguing that the E-mail is not "owned" by a public body. *Id.* Nevertheless, in response to requests by two newspapers, the university released copies of messages exchanged during a computer conference of the school's regents. *Online*, CHRONICLE HIGHER EDUC., Apr. 27, 1994, at A26.

monitor employee E-mail *anytime*. In either case, the employer's ability to monitor is sanctioned by eliminating the surreptitious nature of the monitoring (and hence, the expectation of privacy) with less regard given to the reasonableness of the intrusion and the particular needs or circumstances involved.

Finally, the proposed legislation addressing "electronic monitoring" does not cover interceptions of electronic communications as protected under the ECPA.[199] Thus, if the ECPA is held to be applicable to employee E-mail actions, then the accessing and reading of E-mail files may fall outside of the proposed legislation. Under the ECPA, the prior consent or business use exemptions may pertain, and monitoring may be found permissible, at least on an interstate basis.

Senator Bumpers' bill, the Telephone Privacy Act of 1993,[200] also goes too far in granting employers unlimited access, including access to E-mail of a personal nature. While it can be argued that private, personal discussions have no place in the office, this argument is unrealistic. The legislation is overly broad, ignoring any privacy rights or interests of employees.

B. Proposed Guidelines

A federal monitoring law with very specific provisions may never fully meet the needs of employee privacy while preserving employer management needs. The type of federal policy that should be adopted must be flexible and aimed at preventing unreasonable intrusions relative to varying types of business operations, organizational needs, and employee privacy needs. Guidelines must also be broad so that it may clearly apply to all forms of similar surveillance and be able to accommodate future communications technologies.

Such a broad federal policy could require that monitoring be "reasonable," requiring employers to: 1) have a "legitimate business purpose" for engaging in monitoring; 2) use the least intrusive means possible to achieve the business objective; 3) limit the access, use, and disclosure to information reasonably meeting that objective; and 4) provide reasonable notification of the monitoring and its use. Instead of specifying forty service observations per month, for example, the courts could be the ultimate arbiters in defining the scope of "reasonableness" relative to different types and degrees of intrusion for different industries and as technologies and conditions change over time.

The federal law could then promote the education of employers and employees on the issue and mandate the development of

199. S. 984, *supra* note 166, § 2(2)(C)(i).

200. S. 311, *supra* note 186.

company monitoring policies which could then provide the particular specificity that may be needed, within the federal guidelines on reasonableness. It is imperative that employers create a company policy that clearly spells out monitoring practices and employee privacy specific to that company's operation. Federal law could require a company's electronic monitoring policy to accomplish several objectives, such as: 1) identify the acceptable reasons for surveillance and the specific business purpose to be achieved; 2) explain the monitoring procedures which may and may not be used; 3) contain limitations on what is collected and the use of the information obtained, restricting it to its stated purpose, and ensuring confidentiality; 4) provide for reasonable security measures to prevent unauthorized access; 5) allow only limited, authorized access, defining authorization and who may grant and be granted authorization; 6) make clear to employees that the security of their E-mail, for example, is not guaranteed and that E-mail may not be protected by privacy law; 7) establish employee usage guidelines, such as whether or not the system may be used for nonbusiness (personal) exchanges, when and to what extent; 8) provide for penalties for policy violations by employers and employees; 9) make the policy available to all employees at the time of being hired and periodically thereafter; 10) review the policy periodically.

The restrictiveness of a company's E-mail policy will depend on the specific work environment and the needs of both the company and the employees. The "reasonableness" of the policy will be kept in check by federal law as well as market forces, whereby restrictive policies may result in worker dissatisfaction, lower productivity, and unfilled positions. E-mail administrators and network managers should review the existing law and the proposed legislation with their corporate legal departments. Of course, the best policy that a company could adopt may be to avoid monitoring E-mail systems altogether, whether for the purpose of uncovering wrongdoing or for even accessing files for what might otherwise seem to be legitimate purposes.[201]

In the meantime, employees should take an active role in becoming more aware of the potential for monitoring and find out whether or not a company E-mail monitoring policy exists. If one is not available, employees should demand that a policy be created, they should be involved in its creation, and they should become familiar with it's provisions. Notwithstanding, employees should always be discreet and assume that there is no privacy with their E-mail. In general, employees should protect them-

201. Companies may also want to get a help kit designed to help companies develop an E-mail policy. The kit is available from the Electronic Mail Association, 1555 Wilson Blvd., Suite 300, Arlington, VA 22209 (703) 875-8620.

selves by limiting their use of the system to matters of company operations, and as a rule, never send anything that one would not send to a fax machine or on a postcard.

If both employers and employees take steps to protect themselves, even from unintentional intrusions, and federal and corporate policies are developed, some reasonable balance between privacy needs and management needs may be reached. Currently, there is a significant gap between employees' perceptions of E-mail privacy and the rights of employers to monitor messages. Employees are either unaware of the possibility of monitoring or believe it is illegal. Companies are also lax in responding to the issue and in examining their management monitoring practices. Given the rapid growth of electronic mail, it is likely that more lawsuits will be filed over the issue of E-mail privacy. Company monitoring policies, general public awareness, and a broad federal law prohibiting unreasonable intrusions should be created to address this new workplace issue.

TABLE 1

STATE CONSTITUTIONS
EXPLICITLY RECOGNIZING A PRIVACY RIGHT

ALASKA:[202] "The right of the people to *privacy* is recognized and shall not be infringed upon."

ARIZONA:[203] "No person shall be disturbed in his *private affairs*, or his home invaded, without authority of law."

CALIFORNIA:[204] "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring safety, happiness, and *privacy*."

FLORIDA:[205] "Every natural person has the right to be free from governmental intrusion into his *private life* except as otherwise provided herein."

HAWAII:[206] "The right of the people to *privacy* is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."

ILLINOIS:[207] "The people shall have the right to be secure in their persons, houses, papers and other possessions against

202. ALASKA CONST. art. 1, § 22 (emphasis added).
203. ARIZ. CONST. art. 2, § 8 (emphasis added).
204. CAL. CONST. art. 1, § 1 (emphasis added).
205. FLA. CONST. art. 1, § 23 (emphasis added).
206. HAW. CONST. art. 1, § 6 (emphasis added).
207. ILL. CONST. art. 1, § 6 (emphasis added).

unreasonable searches, seizures, *invasions of privacy* or interceptions of communications by eavesdropping devices or other means."

LOUISIANA:[208] "[E]very person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or *invasions of privacy*."

MONTANA:[209] "The right of *individual privacy* is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."

SOUTH CAROLINA:[210] "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and *unreasonable invasions of privacy* shall not be violated. . . ."

WASHINGTON:[211] "No person shall be disturbed in his *private affairs*, or his home invaded, without authority of law."

TABLE 2

STATE STATUTES WITH PRIOR CONSENT AND BUSINESS USE WIRETAP EXEMPTIONS

Arizona	ARIZ. REV. STAT. ANN. § 13-3012 (1993)
Colorado	COLO. REV. STAT. § 18-9-305 (West 1993)
Delaware	DEL. CODE ANN. tit. 11, § 1336 (1993)[212]
Dist. of Columbia	D.C. CODE ANN. § 23-542 (1993)[213]
Florida	FLA. STAT. ch. 934.03 (1993)[214]
Georgia	GA. CODE ANN. § 16-11-66 (Michie 1993)[215]
Hawaii	HAW. REV. STAT. § 803-42 (1993)
Idaho	IDAHO CODE §§ 18-6702; 18-6720 (West 1993)[216]
Iowa	IOWA CODE ANN. § 8082.B (1993)[217]

208. LA. CONST. art. 1, § 5 (emphasis added).

209. MONT. CONST. art. 2, § 10 (emphasis added).

210. S.C. CONST. art. 1, § 10 (emphasis added).

211. WASH. CONST. art. 1, § 7 (emphasis added).

212. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

213. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

214. Prior consent must be given by *all* parties.

215. Prior consent exemption only.

216. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

217. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

Kansas	KAN. STAT. ANN. § 21-4001; 22-2514 (West 1992)
Louisiana	LA. REV. STAT. ANN. § 15:1303 (1992)[218]
Maryland	MD. CODE ANN. CTS. & JUD. PROC. § 10-402 (1993)[219]
Minnesota	MINN. STAT. § 626A.02 (1993)
Mississippi	MISS. CODE ANN. § 41-29-531 (1993)[220]
Missouri	MO. ANN. STAT. § 542.402 (Vernon 1992)[221]
Nebraska	NEB. REV. STAT. § 86-702 (1993)
Nevada	NEV. REV. STAT. § 200.620 (1993)
New Hampshire	N.H. REV. STAT. ANN. §§ 570-B:3; 570-A:2 (1993)[222]
New Jersey	N.J. REV. STAT. § 2A:156A-4 (1994)[223]
New Mexico	N.M. STAT. ANN. § 30-12-1 (Michie 1994)[224]
North Dakota	N.D. CENT. CODE § 12.1-15-02 (1993)[225]
Ohio	OHIO REV. CODE ANN. § 2933.52 (Anderson 1994)[226]
Oklahoma	OKLA. STAT. tit. 13, § 176.4 (1993)[227]
Oregon	OR. REV. STAT. § 165.543 (1993)
Pennsylvania	PA. CONS. STAT. ANN. § 5704 (1993)[228]
Rhode Island	R.I. GEN. LAWS. § 11-35-21 (1993)[229]
Texas	TEX. PENAL CODE § 16.02 (West 1994)[230]
Utah	UTAH CODE ANN. § 77-23a-4 (1994)

218. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

219. Prior consent must be given by *all* parties.

220. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

221. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

222. Prior consent exemption only.

223. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

224. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

225. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

226. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

227. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

228. Prior consent must be given by *all* parties.

229. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

230. Exempts interceptions by communications common carriers, rather than electronic communication service providers.

Virginia	VA. CODE ANN. § 19.2-62 (Michie 1994)
West Virginia	W. VA. CODE § 62-1D-3 (1994)
Wisconsin	WIS. STAT. § 968.31 (1993)
Wyoming	WYO. STAT. § 7-3-602 (1994)