J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 9(1) 27-37, 2000-2001

EMPLOYEE E-MAIL: A PROTECTED RIGHT TO PRIVACY?

BRANDY L. SCOTT
Harrisburg, Pennsylvania

ABSTRACT

This article examines the constitutional, statutory, and common law protection given to employee e-mail that is either transmitted or stored on the employer's communication system. The article looks at the protection given to employee e-mail by the U.S. Constitution, a number of federal and state statutes, and recent court decisions and it provides a policy exemplar for companies to consider. While the law is not fully settled, rarely have employee e-mail communications been accorded protection under concepts of privacy.

Currently no federal laws regulate electronic surveillance in the workplace, and most states do not have laws restricting electronic monitoring at work [1]. This article discusses the law as it pertains to employees' right to privacy regarding the use of workplace e-mail for personal reasons. The article outlines constitutional law, common law, and Electronic Communication Act of 1986, and the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA), as well as recognizing current case law dealing with an employee's right to the use of e-mail for personal use.

CONSTITUTIONAL LAW

The general right of privacy is implicitly rooted in the Fourth Amendment to the United States Constitution. That amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ." [2]. The United States Supreme

Court has explicitly recognized the right of privacy pursuant to the Fourth Amendment in cases such as *Griswold v. Connecticut* [3] and *Katz v. United States* [4]. However, the Fourth Amendment applies only to governmental participants, thereby protecting employees in the public sector workplace, but not in the private sector.

Supreme Court's landmark ruling in *O'Connor v. Ortega* defines the extent to which the Fourth Amendment protects employee privacy in the public employment [5]. In *Ortega,* a psychiatrist charged state hospital officials with violating his Fourth Amendment rights after they searched his office and seized various items from his desk and file cabinets. The Court held that the propriety of a workplace search, at its inception and in its scope, "should be judged by the standard or reasonableness under all circumstances" [5, at 725-726]. The Court concluded that under this standard, the Fourth Amendment is violated only if public employees have "an expectation of privacy that society is prepared to consider reasonable [5, at 715, citing 11]. This standard requires balancing the employer's need for control and supervision of the workplace against the privacy interests of employees [5, at 719-720].

COMMON LAW

An employee could bring a common law cause of action against a *private employer* when the employer obtains access to the employee's workplace e-mail. There are two common law causes of action in this situation: the privacy tort of intrusion upon seclusion and intentional infliction of emotional distress.

The intrusion upon seclusion tort is defined as follows: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person" [6, at 652B]. If an employee is to succeed in bringing this action s/he has to prove that an employer's access to the e-mail communications was a highly offensive intrusion to a reasonable person. One commentator has stated that "if an employer obtains information about the employee through the employer's . . . computer system . . . the employee will have much greater difficulty in winning an invasion of privacy lawsuit." As a result, employees usually do not succeed when bringing an intrusion upon seclusion claim against their employer for e-mail monitoring.

Second, employees may bring a claim against their employers for intentional infliction of emotional distress resulting from e-mail monitoring in the workplace. In defining the tort of intentional infliction of emotional distress, the Restatement (Second) of Torts states that "one who by extreme and outrageous conduct, intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to another results from it, for such bodily harm [6, at 46]. Although this tort could be available to an employee, it is unlikely that a court would characterize an employer's access to an

employee's e-mail to be extreme and outrageous conduct [7]. Therefore, except in the most "extreme and outrageous" circumstances, an employee's intentional infliction of emotional distress cause of action would most likely fail.

THE CALIFORNIA APPROACH

Possibly foreshadowing the future, in September 1999, the California Legislature sent Gov. Gray Davis a bill that would prohibit employers from secretly monitoring the electronic mail or other personal computer records of their employees, unless the employees have been notified of company policies allowing such monitoring [9]. The proposed bill did not pass, but it set forth new privacy rights for public and private sector employees by giving employees the right to know whether they may be monitored. Employers would be required to prepare and distribute copies of their policies and practices on workplace privacy and electronic monitoring to all employees. Affected employees would be required to sign or electronically verify the notices to acknowledge they have read the policies and understand them. If an employee declined to sign the policies, an employer still would comply with the law if the person who provided the policies to the employee signed a statement that the employer received the policies.

The bill would have given employees the right to have access to records their employer collects through electronic monitoring, and the right to dispute and correct that information. The bill would define "secret monitoring" as inspecting, reviewing, or retaining personal electronic mail or any other computer records generated by an employee when an employer has not notified the employee of the employer's workplace privacy and electronic monitoring policies and practices.

THE ELECTRONIC COMMUNICATION ACT OF 1986

The United States Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) [10] to amend the technologically out-of-date Title III of the Omnibus Crime Control and Safe Streets Act of 1968 [11]. By 1986, Congress realized that the existing laws protecting business and personal communications had not kept pace with the development of communications and computer technology or with the changes in the structure of the telecommunications industry [12]. In amending Title III of OCCSSA, Congress sought to "bring it in line with technological developments and changes in the structure of the telecommunications industry" [12, p. 3]. In its discussion of technological advancements, Congress specifically mentioned that e-mail required additional protection [12, pp. 3-4]. The Senate Report described electronic mail in the following manner:

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then

> transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer. If the addressee is not a subscriber to the service, the electronic mail company can put the message onto paper and then deposit it in the normal postal system. Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence [12, p. 8].

Access to Stored E-Mail: Title II of the ECPA

Cases involving employer access to stored e-mail messages are governed by 18 U.S.C. 2701 [13]. Under 2701, a person or entity violates the Stored Wire and Electronic Communications and Transactional Records Access (Stored Communications). If someone "intentionally accesses without authorization a facility through which an electronic communication service is provided, courts must sanction a violation of the Stored Communications Act for "commercial advantage, malicious destruction or damage, or private commercial gain" with more severity than other violations [13, at 2701(b).]

But the Stored Communications Act provides two exceptions for e-mail communications: the provider exception and the user exception. First, under the provider exception, the Stored Communications Act does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service" [13, at 2701(c)(1)]. According to many commentators who interpret the provider exception broadly, private employers who maintain a computer system have the ability to peruse and disclose employee e-mail communications without violating the Stored Communications Act [14, p. 925]. Second, under the user exception, the Stored Communications Act does not apply to conduct authorized "by a user of that service with respect to a communication of or intended for that user" [13, at 2701(c)(2)].

Interception of E-Mail: Title III of the OCCSSA as Amended by Title I of the ECPA

The interception of an e-mail communication is governed by Title III of OCCSSA [17, at 2510-2521; 39-40]. Through Title I of the ECPA, Title III of OCCSSA was amended to extend interception protection to "electronic communication." Under 18 U.S.C. 2511, an individual violates Title III of OCCSSA if s/he "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communications [11, at 2511(1)(2)]. Damages for a violation of Title III of OCCSSA are more severe than damages for a violation of the Stored Communications Act. Penalties may include punitive damages, attorneys fees, and litigation costs.

Title III of OCCSSA has exceptions that create allowable interceptions of wire, oral, or electronic communications. Section 2520(d) of 18 U.S.C. provides three good faith defenses to liability: 1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; or 2) a request of an investigative or law enforcement officer under section 2518(7) or this title; or 3) a good-faith determination that section 2511(3) of the title permitted the conduct.

The ordinary course of business exception is found in Title III's definition section. Under this exception, an employer may intercept an employee's e-mail communications in the ordinary course of its business if it uses "equipment or a facility, or any component thereof" furnished by the provider of the electronic communication service in the ordinary course of its business [11, 2511(1)(1) 1994]. One commentator has separated cases dealing with employer liability under the ordinary course of business exception of Title III of the OCCSSA into two distinct branches: "legitimate business purpose" cases and "subject of the call" cases [15, p. 239]. Cases involving the legitimate-business-purpose exception focus on whether the employer had a legitimate business purpose to justify the interception of the employee's communication. Courts have held that telephone monitoring to ensure better quality control and to reduce personal use was an allowable interception under Title III's ordinary-course-of-business exception [16].

RECENT CASE LAW INVOLVING E-MAIL IN THE WORKPLACE

As mentioned above, few cases exist involving an employee's right to privacy concerning e-mail communications. In 1996, two federal district courts and one state court addressed the issue of e-mail privacy in the employment context. The U.S. District Court for the District of Nevada decided the most recent employment e-mail privacy case in *Bohach v. City of Reno* [17]. In *Bohach,* the plaintiffs, two Reno, Nevada, police officers claimed the city of Reno had violated the federal wiretapping statutes and their constitutional right to privacy when it 1) stored messages sent over an "Alphapage" message system and 2) accessed the stored messages from police department computer files. Their suit attempted to halt the city's investigation into their alleged misuse of communication equipment.

The district court held, first, that the plaintiffs suffered no constitutional injury under the Fourth Amendment because they had no reasonable expectation of privacy when using the Alphapage message system [17, p. 1234]. The court noted that any subjective expectation of privacy was unreasonable because 1) the police department notified all Alphapage users that their messages would be stored on the network; 2) the department prohibited certain types of messages from being broadcast via Alphapage; and 3) the Alphapage system was easily accessible to anyone with access to the department's computer system [17, p. 1235].

Second, the district court held that the plaintiffs did not have a claim under federal wiretapping statutes because no interception of electronic communications occurred, and the city, as the provider of computer service under the ECPA, could lawfully access any stored electronic communication on its Alphapage system. The district court denied the plaintiff's motion to prevent access to the stored Alphapage messages [17, pp. 1236, 1237].

The U.S. District Court of the Eastern District of Pennsylvania addressed an employee's e-mail privacy rights in *Smith v. Pillsbury Co.* [18]. In *Pillsbury,* the district court sought to determine whether an employee had a claim for wrongful discharge after Pillsbury accessed the employee's work-related e-mail communications [18, p. 98]. The plaintiff had sent e-mail messages to his supervisor that the company concluded were "unprofessional." Smith was then terminated. The plaintiff relied on *Borse v. Piece Goods Shop, Inc.* [19] to support its proposition that a tortious invasion of privacy may be a sufficiently clear mandate of public policy to bar an at-will employment discharge. The district court noted, however, that the *Borse* decision supported such a proposition only if an employer's invasion of privacy was substantial and highly offensive to the 'ordinary reasonable person.' Applying this standard, the court first determined that the plaintiff did not have a reasonable expectation of privacy in workplace e-mail communications.

The court distinguished the present privacy intrusion from those in which a person has a reasonable expectation of privacy, namely, urinalysis and personal property searches. In addition, the court further differentiated this case because the Pillsbury executives did not require the plaintiff to disclose any personal information, as would have been the case in the urinalysis and personal property search cases. The court determined the e-mail communications did not enjoy a reasonable expectation of privacy even though Pillsbury had made assurances to its employees that employee e-mail would not be intercepted. Once the plaintiff had voluntarily transmitted the communication to another individual, his supervisor, the court concluded that any reasonable expectation of privacy was lost [20].

The court concluded that no reasonable person would find Pillsbury's actions to be a substantial and highly offensive invasion of an employee's privacy interest. Pillsbury's interest in "preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have" [18, at 100]. In addition, the court noted that Pillsbury did not force the plaintiff to disclose personal information; nor did it invade the plaintiff's person, as would be the case with a urinalysis or a personal property search. The court therefore granted Pillsbury's motion to dismiss.

In another case, a Massachusetts appellate court ruled on a trial court's grant of summary judgment in favor of the employer in *Restuccia v. Burk Technology, Inc.* [21]. In *Restuccia,* an employer discharged two employees after reading their e-mail messages stored in the employer's backup computer files. The

employees' stored e-mail messages included messages containing nicknames for the employer and messages detailing the employer's extramarital affair with another employee.

The trial court granted summary judgment for the employer on most counts, including violations of the state wiretap law, intentional infliction of emotional distress, tortuous interference with contractual relations, wrongful termination, invasion of privacy, negligent infliction of emotional distress, and loss of consortium. The superior court reversed the trial court's summary judgment in regard to all but one of the judgments. The court held the employer was entitled to summary judgment only on the claims under the state wiretap statute [21].

In a more recent case, *United States v. Simons,* the defendant, a CIA employee, was charged with violating 18 U.S.C. §2250(A) by using the Web to receive and possess child pornography [22]. This 1998 case began with the observations of an operations center manager. The manager noted that its Internet access log was very large. When he searched on the word "sex," he found a significant number of hits, later traced back to the defendant's work station. This led to a remote examination of the defendant's files, which management determined were pornographic. A search warrant was issued and executed.

When indicted, Simons moved to suppress the evidence as an illegal search and, therefore, a violation of the Fourth Amendment. Judge Cacheris denied the motion, ruling that Simons had no expectation of privacy, particularly since the office in which he worked had previously published an official policy on "Permitted and Prohibited Official Use of the Internet." In light of the policy, the court did not find that the defendant had any reasonable expectation of privacy with respect to any of his Internet activity. Accordingly, the searches of his computer and his e-mail did violate the Fourth Amendment.

E-MAIL POLICIES IN THE WORKPLACE

An employer may provide employees with advance knowledge of how e-mail will be treated in their employment context by creating an e-mail monitoring policy [23]. The policy should clearly explain to employees the employer's intentions regarding workplace privacy [23]. Currently, it is estimated that only one-third of U.S. businesses utilizing e-mail systems have e-mail policies. E-mail monitoring policies serve multiple purposes. The policies create clear standards to prevent employment disputes and insure consistent supervisory administration of employment relations. In addition, an e-mail monitoring policy will provide proof to the employee, or to a court in the event of litigation, that the employer seeks to protect company property and resources and does not seek to invade the employee's privacy rights.

Attorney Adam Conti has posted a sample employer e-mail and electronic usage policy on his Internet Law Office Web page. Some extracts from this policy are:

1. The following procedures apply to all electronic media and services which are:
   –accessed on or from company premises,
   –accessed using company computer equipment, or via company-paid access methods, and/or
   –used in a manner which identifies the individual with the company.
2. Electronic media may not be used for knowingly transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene of X-rated communications, or are of a defamatory or threatening nature, or for "claim letter," or for any other purpose which is illegal or against company policy or contrary to the company's interest.
3. Electronic media and services are primarily for company business use. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, nonbusiness, purposes is understandable and acceptable—as is the case with personal phone calls. However, employees need to demonstrate a sense of responsibility and may not abuse the privilege.
4. Electronic information created and/or communicated by an employee using e-mail, word processing, utility programs, spreadsheets, voice-mail, telephones, Internet/BBS access, etc. will not generally be monitored by the company, and we respect our employees' wish to work without "Big Brother" looking over their shoulder.
5. The company routinely monitors usage patterns for both voice and data communications (e.g., number called or site accessed; call length; times of day calls. Reasons include cost analysis/allocation and the management of our gateway to the Internet.
6. The company also reserve the right, in its discretion, to review any employee's electronic files and messages and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other company policies.
7. Each employee who uses any security measures on a company-supplied PC or MAC must provide his/her group administrative assistant with a sealed hard copy record (to be retained in a secure location) of all of his/her PC or MAC passwords and encryption keys (if any) for company use if required. (Example: there may be a need for the company to access an employee's system or files when s/he is away from the office.) There is no need to provide UNIX passwords since the UNIX system administrator can access all e-mail and files via "root" passwords if necessary.
8. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and attributable to our company. While some users include personal "disclaimers" in electronic messages, it should be noted that there would still be a connection with the company, and the statement might still be legally imputed to the company. All communications sent by employees via a network must comply with this

and other company policies, and may not disclose any confidential and proprietary company information.

9. Any employee found to be abusing the privilege of company-facilitated access to electronic media or services will be subject to corrective action and/or risk having the privilege removed for him/herself and possible other employees [24].

CONCLUSION

The current law regarding employees' right to privacy in their workplace e-mail usage is not entirely settled, but, for the most part, the employee claims of privacy in their e-mail have not been supported. The only sure-fire method an employer can use to avoid legal liability for monitoring employees is to obtain their consent in advance. In doing so, an employer should establish and explain clear written policies for employee monitoring and educate supervisors when monitoring is permissible. All employers should reserve the right to access e-mail and monitor computer usage for the purpose of retrieving documents, troubleshooting, security, and complying with legal and regulatory requirements. Each employer needs to decide what the appropriate level of monitoring should be for its workplace.

Employers should caution supervisors to refrain from discussing or disclosing any personal non-work-related information about an employee that is discovered from employee monitoring. Employees should be explicitly informed that their e-mail and Internet usage is being monitored by computer software. Employees should be required to sign an acknowledgment that they have read the policy on electronic monitoring and understand that their e-mail and Internet usage may be monitored and recorded. The acknowledgment should also explain that the employer may disclose any information obtained as a result of such monitoring to law enforcement officials and regulators.

Obtaining written consent or acknowledgment is essential because the courts have been reluctant to make a finding of implied consent. To reinforce the policy and strengthen their position in any potential liability lawsuit, employers should circulate periodic reminders of the policy to every employee and supervisor. Finally, any policy adopted should be reviewed from time to time. In addition, such a policy should be reviewed by legal counsel if an employer expands operations to a new state or internationally. If employers take these steps, they can legally use software to monitor employees' e-mail and computer usage.

ENDNOTES

1. Connecticut is the exception, where electronic monitoring is not permitted in areas designated for the personal health or comfort of employees.

2. United States Constitution, Amendment IV.
3. 381 U.S. 479 (1965). Addressing the issue of contraception.
4. 389 U.S. 487 (1967). Holding that warrantless electronic surveillance violated the Fourth Amendment.
5. 480 U.S. 709 (1987).
6. Restatement (Second) of Torts, 652B (1965).
7. J. A. Flanagan, Note, Restricting Electronic Monitoring the Private Workplace, *43 Duke L. J., 1256,* at 1267.
8. "The employer's conduct must be extreme in degree, outrageous in character, and 'atrocious' and utterly intolerable in a civilized community," *Kaminsky v. United Parcel Serv.,* 501 N.Y.S. 2d 871 (873) (App. Div., 1986).
9. *Individual Employment Rights: Labor Relations Reporter.* Washington: Bureau of National Affairs, Vol. 15, No. 9, p. 34.
10. Pub. L. No. 99-508 100 Stat. 1848 (codified into scattered sections of 18 U.S.C.).
11. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520 (1994). Title II of the OCCSSA was enacted by Congress in response to the Supreme Court's decision in *Berger v. New York,* 388 U.S. 41 (1967) which granted Fourth Amendment protection to oral conversations from electronic eavesdropping.
12. Senate Rep. No. 99-541 at 2.
13. 18 U.S.C. 2701-2711 (1994). See *Steve Jackson Games, Inc. v. United States Secret Serv.,* 36 F. 3d, 457, 462-463 (5th Cir. 1994) holding that seizure of stored electronic communications is governed by Title II of ECPA.
14. J. T. Baumhart, The Employer's Right to Read Employee E-Mail: Protecting Property of Personal Prying, 8 Lab. Law. J. 923, 925 (1992). Baumhart argues that when the employer owns the e-mail system, it has been given the right to read employee e-mail messages, no matter how personal, and disclose the contents.
15. T. R. Greenberg, Comment, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 Am. U. L. Rev. 219.
16. *James v. Newspaper Agency Corp.,* 591 F. 2s 579 (10th Cir. 1979); *Simmons v. Southwestern Bell Tel. Co.,* 452 F. Suppl. 392. Both cases supported the employer's right to monitor telephone communications and exercise discipline after giving notice to employee that they could be monitored.
17. 932 F. Supp. 1232 (Nev. 1996).
18. 914 F. Supp. 97 (E.D. Pa. 1996).
19. 963 F. 2d 611 (3d Cir. 1992).
20. A Pillsbury senior executive named DeOcejo challenged Smyth's claim that Pillsbury assured its employees of privacy on the Pillsbury computer system. He claimed the existence of a signed waiver that showed Smyth consented to e-mail monitoring.
21. No. 95-2125 (Mass. App. Ct. 1996), reprinted in *The Week's Opinions: Superior Court, Massachusetts Lawyers Weekly,* Dec. 16, 1996, at 16.
22. 29 F. Supp. 2d (E.D. Va. 1998).
23. For discussion, please see B. C. Glassberg, W. J. Kettinger, and J. E. Logan, Electronic Communication: An Ounce of Policy is Worth a Pound of Cure, *Business Horizons, Vol. 39, No. 4, pp. 74-80 (July 1996); or E. Brown, The Myth of E-Mail Privacy, Fortune,* Vol. 135, No. 2, pp. 69-71 (February 3, 1997).

24. A. Conti, *Employment Policies and Employee Handbooks,* Internet Law Office, www.contilaw.com.

Direct reprint requests to:

Brandy L. Scott
963 Chestnut St. #2
Kulpmont, PA 17834