

Employee E-mail and Internet Use Policies

**by Brad Young
BICKERSTAFF, HEATH, POLLAN & CAROOM, L.L.P.**

**Texas Leadership Institute
April 18, 2007**

I. Overview

In today's brave new workplace, employers may have a legitimate interest in monitoring their employees' e-mail and Internet use. Reasons for monitoring can include boosting productivity, preventing dissemination of confidential information, or avoiding sexual harassment lawsuits. In addition, employers can be liable for copyright infringement where employees have improperly downloaded and distributed protected material from the web.¹ Public employers in Texas must bear in mind that work-related e-mail may be subject to public disclosure under the Texas Open Records Act.² And finally, in the litigation context, employers do not want employees to inadvertently create e-mail that waives the attorney-client privilege.³

In fashioning an e-mail and Internet use policy, however, the employer must take care not to violate an employee's statutorily or constitutionally protected free speech and privacy rights. Although there is still relatively little case law in this area, suits against employers are on the rise and generally tend to fall into one of four categories: claims under the Electronic Communications Privacy Act of 1986 ("ECPA"), state common law tort claims, Fourth Amendment search and seizure claims, and First Amendment free speech claims. The following section briefly outlines these various claims.

II. Causes of Action

A. The Electronic Communications Privacy Act of 1986

¹ For a discussion of copyright infringement issues, see section 3, below.

² TEX. GOV'T CODE § 552.002; *see* Tex. Att'y Gen. ORD-654 (1997).

³ Generally, the rules for claiming the attorney-client privilege over information sent via e-mail are the same as those for information sent through any other medium. *See, generally*, TEX. R. EVID. 503. That is, where a communication would be otherwise privileged, that privilege is not waived merely because it is transmitted over e-mail. *See in re Monsanto Co.*, 998 S.W.2d 917, 930 *et.seq.* (Tex. App. – Waco 1999, no pet.). The attorney-client privilege protects both the e-mail message itself and documents attached to a privileged e-mail. *See id.* at 931 n. 19.

The ECPA, which applies to both public and private employers, protects most electronic communications, including e-mail, from interception, attempted interception, disclosure, use and unauthorized access.⁴ Employers who violate the Act can incur both criminal and civil penalties, including preliminary or other equitable or declaratory relief, monetary damages, punitive damages, attorney's fees, and other reasonable costs of litigation.⁵

There are some important exceptions to the Act, however. First, section 2511 focuses on the unlawful "interception" of electronic communications.⁶ The Fifth Circuit has recognized that the word "interception" only applies to e-mail messages retrieved while they are in transit, and not after they have been saved in electronic storage.⁷ The Act itself creates specific exceptions from its own unauthorized access and disclosure prohibitions for the "person or entity providing a wire or electronic communications service"⁸ or "a person employed or authorized or whose facilities are used to forward the communication to its destination."⁹ Therefore, if the employer owns the network and does not read the e-mail before it reaches its destination, that employer probably has the right to store those e-mail messages on the server and to open and read them later.¹⁰

Finally, the most important exception to the ECPA involves consent. It is not an offense to intercept information sent over e-mail where "one of the parties to the information has given prior consent to such interception."¹¹ Prior consent also protects the disclosure of the contents of an e-mail.¹² Therefore, the extent to which an employer may be able to legally monitor employee e-mail

⁴ 18 U.S.C. §§ 2510-11, 2701-2; *see also* TEX. PENAL CODE § 16.02 (making it a criminal offense under Texas law to intentionally intercept, endeavor to intercept, or procure another person to intercept or endeavor to intercept a wire, oral, or electronic communication).

⁵ 18 U.S.C. § 2520(b). Criminal penalties can include imprisonment up to five years, fines, or both. 18 U.S.C. § 2511(4).

⁶ 18 U.S.C. § 251.

⁷ *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 461-2 (5th Cir. 1994); *see also Bohach v. City of Reno*, 932 F.Supp. 1232, 1236 (D. Nev. 1996) (rejecting police officers' ECPA claim that police department unlawfully "intercepted" stored messages sent over the department's computerized paging system).

⁸ 18 U.S.C. § 2701(c)(1) (creating exception to unauthorized access provision of ECPA).

⁹ 18 U.S.C. § 2702(b)(4) (creating exception to unauthorized disclosure provisions of ECPA).

¹⁰ *See* Andrew M. Low, *E-Mail, Voicemail, and Employees' Right to Privacy: Monitoring Employees' Electronic Communications*, COLO. LAWYER, Oct. 2000, at 13.

¹¹ 18 U.S.C. § 2511(2)(d).

¹² 18 U.S.C. § 2702(b)(3).

may depend on the extent to which the employer's e-mail and Internet use policy effectively limit e-mails, or disclaims an employee's privacy rights.¹³

B. State Common Law Tort Claims

A second area of litigation involving employer monitoring of employee e-mail and Internet use involves the state common law tort claim of invasion of privacy. In order to prevail in this area, the employee must establish that he or she had a "reasonable expectation of privacy" in his or her e-mail communications.¹⁴ In the leading case on this issue, *Smyth v. Pillsbury Co.*,¹⁵ an employee sued for wrongful discharge and invasion of privacy following his termination because of inappropriate e-mail messages he sent to his supervisor over the company e-mail system.¹⁶ The plaintiff argued that he had relied on repeated assurances by the employer that all e-mail communications would remain confidential and privileged, and that employee e-mail could not be intercepted and used by the employer as grounds for termination or reprimand.¹⁷ Despite these facts, the court found that there was no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."¹⁸ To reach this finding, the court applied a balancing test and determined that "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system [outweighed] any privacy interest the employee may have in those comments."¹⁹

In one of the few Texas cases to address employee e-mail monitoring, a plaintiff accused of

¹³ See *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582 (11th Cir. 1983) (holding employee, who only agreed to limited employer monitoring of telephone use, reasonably relied on limits set out by agreement); see also *McVeigh v. Cohen*, 983 F.Supp. 215, 219 (D.C. 1998) (finding Navy violated its own "don't ask, don't tell" policy by calling Internet service provider to investigate whether the alias "boysrch" on e-mail was traceable to a particular officer).

¹⁴ See *Smyth v. Pillsbury Co.*, 914 S.W.2d 97, 100-1 (E.D. Penn. 1996).

¹⁵ *Id.*

¹⁶ See *id.* at 98. The company alleged in its motion to dismiss that the e-mails "concerned sales management and contained threats to 'kill the backstabbing bastards' and referred to the planned holiday party as the 'Jim Jones Koolaid affair.'" *Id.* at 98 n. 1.

¹⁷ See *id.* at 98.

¹⁸ *Id.* at 101.

¹⁹ *Id.*

sexual harassment and “inventory questions” sued his former employer for invasion of privacy.²⁰ The Dallas Court of Appeals, recognizing that plaintiff’s workstation and computer were both company-owned and that all messages were saved in electronic storage, held that even by creating a personal password, plaintiff had no reasonable expectation of privacy in the contents of his e-mail messages such that the employer was precluded from viewing the messages.²¹

C. Fourth Amendment Claims

The Fourth Amendment to the United States Constitution, which prohibits unreasonable searches and seizures, offers an additional privacy protection for public employees.²² In order for a search or seizure to be *unreasonable*, however, the employee must have a *reasonable* expectation that his or her computer activity is private.²³ The Supreme Court has recognized that public employees’ expectations of privacy in their offices, desks and files “may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.”²⁴

It is not always easy for an employee to prove that he or she had a reasonable expectation of privacy. Factors a court may look at include: (1) the employee’s interest in and control of the area searched; (2) the employee’s subjective expectation of privacy in the area as evidenced by his or her efforts to ensure that privacy; and (3) society’s willingness to recognize that expectation as reasonable.²⁵ Under this analysis, the Fourth Circuit found that an employee had no reasonable expectation of privacy in stored electronic information over which he had no control.²⁶

Courts are also willing to consider a public employer’s e-mail and Internet use policies when evaluating Fourth Amendment claims. Therefore, where a governmental employer’s official policy informed employees that the employer would conduct “electronic audits” to identify, terminate, and prosecute unauthorized activity, employees had no reasonable expectation of privacy with regard to

²⁰ See *McLaren v. Microsoft Corp.*, No. 05-97-00824-CV, 1999 WL 339015, at *1 (Tex. App.— Dallas May 28, 1999) (unpublished opinion).

²¹ See *id.* at *4.

²² See *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987) (“Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment.”).

²³ See *id.*

²⁴ *Id.* at 717.

²⁵ See *United States v. Horowitz*, 806 F.2d 1222, 1225 (4th Cir. 1986).

²⁶ See *id.* at 1226.

Internet use.²⁷ Similarly, a court has held that police officers had a diminished expectation of privacy in a police department's pager system, where the Chief had issued an order stating that messages sent over the system would be "logged on the network," and that messages that violated the Department's discrimination policy were banned from the system.²⁸ Even where there is no unwritten policy, however, a search of an employees' computer may still be reasonable, and thus not in violation of the Fourth Amendment, where the search is directly related to suspected employee misconduct.²⁹

However, a recent case illustrates how a computer use policy that no one follows may be worse than no policy at all. In the case of *Quon v. Arch Wireless Operating Co.*,³⁰ the city had a "Computer Usage, Internet and E-Mail Policy":

Access to the Internet and the e-mail system is not confidential; and Information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.

After the distribution of city-owned pagers to the city's SWAT team, the police department informed its officers orally in a staff meeting and in a memo that the pagers were considered "e-mail" under the policy and were subject to audit. In a separate conversation, however, the lieutenant in charge of the use and provision of the department's electronic equipment informed his officers that he would only audit their pagers if there was an overage of the officer's allotted minutes. Based on this representation, the court held that the officers had an objectively reasonable expectation of privacy in the contents of messages sent over their pagers. Therefore, the city could be liable for Fourth Amendment violations arising from its supervisors' reading employee pager messages. In other words, the lieutenant's unwritten policy eviscerated the department's written computer usage policy.

Finally, a word about the Texas Public Information Act (a.k.a. the "Open Records Act") as it applies to employee communications. The Fifth Circuit Court of Appeals has held that an employee may have a objectively reasonable belief that the employee's communications conducted

²⁷ See *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000). In *Simons*, the defendant, an electronic engineer with the Foreign Bureau of Information Services component of the CIA, faced prosecution for accessing and downloading child pornography over the CIA's computer system. See *id.* at 325.

²⁸ See *Bohach*, 932 F.Supp. at 1234-5.

²⁹ *United States v. Slanina*, 283 F.3d 670 (5th Cir. 2002).

³⁰ 445 F.Supp.2d 1116 (C.D. Cal. 2006)

over the employer's equipment are private from the employer, even though such communications may be subject to disclosure under state open records laws.³¹

D. First Amendment Claims

Public employees are also subject to First Amendment free speech protections. Although this protection would ostensibly apply to the contents of employee e-mail or Internet use, there has been little litigation in this area so far. In one of the few published opinions, the Fourth Circuit held that a Virginia law prohibiting state employees from accessing sexually explicit material on computers owned or leased by the state, except in conjunction with an agency-approved research project, did not infringe upon the First Amendment rights of state employees.³² At least one commentator has suggested that an employer may have a *duty* to report child pornography that the employer discovers on its computers under a federal public health statute on child abuse reporting.³³

III. Copyright Infringement

The Federal Copyright Act protects an author's exclusive rights in copyrighted work,³⁴ and its protections extend to copyrighted material downloaded from the Internet.³⁵ The Act applies to governmental entities "in the same manner and to the same extent as any nongovernmental entity."³⁶ Under the theory of *respondeat superior*, courts have held that an employer can be vicariously liable for the copyright infringements of its employees.³⁷ Even more troubling, it is no excuse from

³¹ See *Zaffuto v. City of Hammond*, 308 F.3d 485 (5th Cir. 2002).

³² See *Urofsky v. Gilmore*, 216 F.3d 401, 416 (4th Cir. 2000).

³³ Robert J. Nobile, *An Employer's duty to Report Child Pornography Found in the Workplace*, GUIDE TO EMPLOYEE HANDBOOKS 9:69, Oct. 2006 (citing 42 U.S.C. § 12032(b)(1), which requires providers of "electronic communication services" to the public to report apparent child pornography to the National Center for Missing and Exploited Children).

³⁴ 17 U.S.C. § 106.

³⁵ See, e.g., *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013-4 (9th Cir. 2001) (finding users who downloaded copyrighted music violated reproduction rights); *Playboy Enters., Inc. v. Webworld, Inc.*, 991 F.Supp. 543, 551 (N.D. Tex. 1997) (finding copyright violation where company downloaded unauthorized copies of protected images).

³⁶ 17 U.S.C. § 501(a).

³⁷ See *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (2nd Cir. 1963); *Fermata Int'l Melodies, Inc. v. Champions Golf Club, Inc.*, 712 F.Supp. 1257, 1262 (S.D. Tex. 1989).

liability that the employer was not aware its employees were violating copyright law.³⁸

The Act does include an exception for material that is reproduced for a “fair use,” which the Act defines as “purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.”³⁹ Therefore, material downloaded for one of these purposes will ordinarily not constitute copyright infringement. However, because of the employer’s potential exposure for the unauthorized reproduction of material that does not fall within the fair use exception, the employer needs a clear policy that outlines the legitimate ways that employees may use the Internet at work. Further, each employee should understand and agree to that policy.

IV. Defenses

In general, courts have tended to treat employers favorably in disputes regarding employer monitoring of employee e-mail and Internet use. As litigation in this area increases, however, the prudent employer should protect his or her organization by implementing a clear e-mail and Internet use policy and making sure each employee understands and agrees to it.⁴⁰ The key to nearly all of these cases is consent: once employees understand their rights and responsibilities regarding the employer’s computer hardware, software, and network equipment employees become free to use these valuable resources in their daily work without exposing the employer to future liability stemming from its misuse.

The contents of this paper are provided for informational and educational purposes only and are not intended to provide legal advice.

³⁸ See *Swallow Turn Music v. Wilson*, 831 F.Supp. 575, 580 (E.D. Tex. 1993).

³⁹ 17 U.S.C. 107.

⁴⁰ See, e.g., Sindy J. Policy, *The Employer as Monitor: Keeping an Eye On Net Use and E-Mails Can Prevent Litigation*, BUSINESS LAW TODAY, Nov./Dec. 2000, at 9.