2004

The Right of Privacy of Employees with Respect to Employer-Owned Computers and E-mails

Charles Adams

Recommended Citation
75 Okla. B. J. 2567 (2004).

LABOR
& Employment

The Right of Privacy of Employees With Respect to Employer-Owned Computers and E-mails

By Charles W. Adams

An employee's right of privacy with respect to an employer-owned computer or e-mail system can be summed up by referring to the famous quotation from Scott McNealy: "You have zero privacy anyway .... Get over it." Employers have a number of justifications for obtaining access to computers as well as for monitoring the use that employees make of the e-mail systems and Internet access they are provided.

For one thing, the employers own the hardware — both the computers and the servers the computers are connected to. For another, the employers are paying for the employee's time, and therefore, they have a right to monitor their employees to see whether they are actually working or not. Besides loafing on the job, employees might be doing damage to the company: by bothering other employees, committing crimes, disclosing secrets to competitors or exposing the company to liability for their own offensive actions.

For a number of reasons, there have been no reported cases where employers have been found liable to employees for searching their employees' computers or e-mail records. Nevertheless, a potential for liability may exist if the employer does not follow appropriate procedures to avoid violating an employee's reasonable expectation of privacy or federal law. The rights of employees to privacy with respect to their computers and e-mails, and the potential for employer liability for searching employee computers and e-mail records are discussed below.

LIABILITY BASED ON INVASION OF PRIVACY

The potential for employer liability for invasion of privacy is suggested by a case called *K-Mart Corporation v. Trotti*.[1] The *Trotti* case arose out of K-Mart's search of lockers that it had supplied to employees at one of its stores to store their personal items during working hours. K-Mart also provided padlocks, but the employees had the option of using their own padlocks. Ms. Trotti stored her purse in a locker when she arrived for work and used her own combination lock. During her afternoon break, she noticed her lock was hanging open, and, although nothing was missing from either the locker or her purse, the personal items in her purse were in considerable disorder. The store manager admitted that he had searched the lockers that day, including Ms. Trotti's, because one of the security personnel suspected that an unidentified employee had stolen a watch. There was conflicting testimony on whether the employees had been informed previously that their lockers were subject to being searched.

Ms. Trotti sued K-Mart for invasion of privacy, and the jury returned a verdict of $8,000 for mental anguish and $100,000 in punitive damages. The appellate court reversed and ordered a new trial. It decided that in order to recover for invasion of privacy, a person must show an intrusion that was highly offensive to a reasonable person. Nevertheless, the appellate court ruled that Ms. Trotti was entitled to recover for invasion of privacy, because there was evidence that she satisfied this requirement. Even though K-Mart owned the locker it provided to Ms. Trotti, she had "demonstrated a legitimate expectation to a right of privacy in both the locker itself and those personal effects within it" by placing her own lock on it with K-Mart's consent.[2]

"...even though the employer had assured its employees that e-mails were confidential..."

By analogy to the *Trotti* case, an employer could potentially be liable for invasion of privacy, if it searched an employee's hard drive or read e-mail messages that the employee had sent or received, even though it owned the employee's computer and the e-mail system. A jury could find that the employee had "a legitimate expectation to a right to privacy" in the hard drive and the e-mails, and that the employer's intrusion was highly offensive to a reasonable person, particularly if the employee used a password on the computer and the e-mails were encrypted. Nevertheless, no employer has yet been found liable to an employee for invasion of privacy on account of reading e-mails or searching computer hard drives.

In *McLaren v. Microsoft Corp.*,[3] an ex-employee sued Microsoft for invasion of privacy. Mr. McLaren alleged that Microsoft had broken into some of the personal folders that were maintained on his office computer and were part of an application that Microsoft had created to store e-mail messages. The e-mail system was accessed through a network password, and in addition, access to the personal folders could be restricted by another password, which Mr. McLaren had created for them.

The trial court dismissed the case, and the appellate court affirmed. It ruled that the case differed from the *Trotti* case, because the locker in the *Trotti* case was provided so the employee could store personal items, while Microsoft provided Mr. McLaren with a computer for business purposes. In addition, it decided that Mr. McLaren did not have a reasonable expectation of privacy in the e-mail messages because they were stored on the office server, rather than on Mr. McLaren's computer. Moreover, the court concluded that even if Mr. McLaren did have a reasonable expectation of privacy in the e-mail messages, Microsoft's intrusion would not be highly offensive to a reasonable person, because Mr. McLaren was at the time on suspension pending an investigation of charges of sexual harassment and "inventory questions," and he had notified Microsoft that some of the e-mails were relevant to the investigations. Thus, the court determined that Microsoft's interests outweighed any privacy interest Mr. McLaren had with respect to the e-mails.

Smyth v. Pillsbury Co.[4] arose out of an employee's termination for making inappropriate and unprofessional comments over his employer's e-mail system. The court decided that the employee did not have a reasonable expectation of privacy in e-mails he sent to his supervisor, even though the employer had assured its employees that e-mails were confidential and that it would not use them against employees as grounds for termination or reprimand. The court said that the employer's reading of the employee's e-mails contrasted with a urinalysis or personal property search, because the employee was not compelled to disclose any personal information about himself, but instead sent the e-mails voluntarily over the company's e-mail system. In addition, the court determined that even if the employee did have a reasonable expectation of privacy in his e-mail messages, his privacy interest was out-

weighed by the employer's interest in preventing inappropriate and unprofessional comments and illegal activity over its e-mail system.

Invasion of privacy claims were also rejected by the courts in *Muick v. Glenayre Electronics*,[5] *TBG Insurance Services Corp. v. Superior Court*,[6] *Kelleher v. City of Reading*,[7] and *Garrity v. John Hancock Mutual Life Insurance Co.*[8] The employer in the *Muick* case seized an employee's laptop computer from the employee's work area at the request of federal law enforcement authorities after they had arrested him for charges of receiving and possessing child pornography. The court decided that the employee had no reasonable expectation of privacy in the laptop, because the employer had an announced policy that it could inspect the laptops it furnished to its employees.

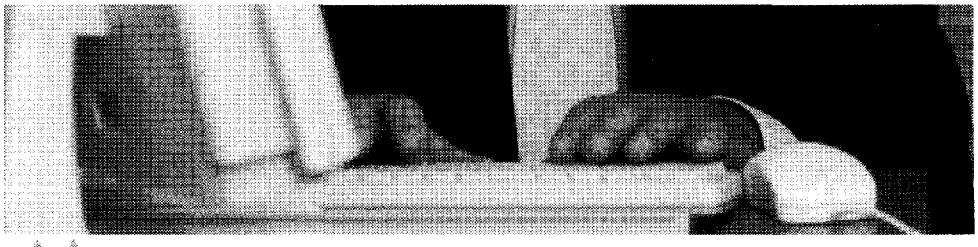
Similarly, the court in the *TBG Insurance Services Corp. v. Superior Court* case ruled that an employee had no reasonable expectation of privacy in a computer provided by his employer, since the employee had signed a policy statement that authorized his employer to monitor files and messages on it. An employer's e-mail policy also negated any expectation of privacy in the *Kelleher v. City of Reading case*. Finally, in the *Garrity v. John Hancock Mutual Life Insurance Co.* case, the court found that the employees had no reasonable expectation of privacy in their e-mails at work on account of the company's e-mail policy. Moreover, even if the employees did have an expectation of privacy, their privacy interests were outweighed by the employer's legitimate business interests in protecting its other employees from harassment from the sexually explicit e-mails that they were sending the other employees.

Despite all these cases, it is still conceivable that an employee could succeed on an invasion of privacy claim against an employer, particularly if an employer had no legitimate business interest in searching an employee's computer or reading the employee's e-mail, and the employer had given assurances to its employees that the contents of their computers and their e-mails were private and confidential. An announced policy that computers and e-mails are not private and confidential, but instead are subject to monitoring by the employer is recommended to negate any expectation of privacy that employees would claim. In addition, monitoring should only be conducted for specific business purposes.

MONITORING BY GOVERNMENTAL EMPLOYERS

Special considerations apply to the monitoring of employees by governmental employers. Unlike private employers, governmental employers are subject to the prohibition in the Fourth Amendment to the United States Constitution against "unreasonable searches and seizures." As a practical matter, however, the limitations on monitoring computers and e-mail systems by governmental employers are the same as for private employers.

The United States Supreme Court addressed the extent of privacy of government employees under the Fourth Amendment in *O'Connor v. Ortega*.[9] Dr. Ortega, a psychiatrist at a state hospital claimed that the hospital administration violated his rights under the Fourth Amendment when it searched his office, including his desk and file cabinets, while he was on administrative leave on account of an investigation of various work-related charges against him. The Supreme Court decided that the Fourth Amendment protects the privacy of governmental employees to the extent that they have a reasonable expectation of privacy, and it accepted the conclusion of the lower courts that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets. The court then went on to hold, though, that in contrast to a search conducted by law enforcement



"Special considerations apply to monitoring of employees by governmental employers."

authorities, neither a warrant nor probable cause was required before a governmental employer could conduct a work-related search of an employee's office. Instead, a search of a government employee's office would be permissible under the Fourth Amendment if it was conducted either for a noninvestigatory work-related purpose (such as to find a missing file), or if there were reasonable grounds for suspecting the employee of work-related misconduct.

> "...CIA had a reasonable basis for suspecting that the hard drive would provide evidence of work-related misconduct..."

The *O'Connor* case was followed in *United States v. Angevine*,[10] *Leventhal v. Knapek*,[11] and *United States v. Simons*.[12] In the *Angevine* case, the court ruled that a professor at Oklahoma State University did not have a reasonable expectation of privacy in his computer on account of a University computer use and Internet policy. It also ruled that the professor did not have a reasonable expectation of privacy with respect to child pornographic files that the police had recovered through the use of special technology after he had attempted to delete them from his computer, because he no longer had access to them. In the *Leventhal* case, the court decided that an employee of a state agency did have a reasonable expectation of privacy in his office computer, but the state agency did not violate his Fourth Amendment rights because the agency had reasonable grounds for suspecting the employee of work-related misconduct.

The *Simons* case involved both a remote search of a Central Intelligence Agency employee's computer for child pornography and a seizure of the employee's hard drive from his office. The court ruled that the employee had no reasonable expectation of privacy with respect to his Internet use because of the CIA's Internet policy, but he did have a reasonable expectation of privacy with respect to the hard drive in his office computer. Nevertheless, the court ruled that the seizure of the hard drive was reasonable, because the CIA had a reasonable basis for suspecting that the hard drive would provide evidence of work-related misconduct on account of the remote search of the employee's computer that it had already conducted.[13]

Although the Fourth Amendment protects the privacy of government employees, but not the privacy of private employees with respect to searches by their employer, there does not appear to any significant difference between what governmental or private employers can do in terms of searching the computers or e-mail records of their employees. In both cases, privacy is protected only if there is a reasonable expectation of privacy, and the expectation of privacy may be negated by a policy that computers and e-mail are not private and confidential. In addition, even if there is a reasonable expectation of privacy, the employee's interest in privacy may be outweighed by a government employer's legitimate work-related interests, such as investigating work-related misconduct of the employee.

FEDERAL LAW RELATING TO MONITORING OF EMPLOYEE E-MAILS

Another potential source of employer liability for monitoring employee e-mails is a federal law called the Electronic Communications Privacy Act (the "ECPA"). The federal wiretapping statute[14] originally prohibited the unauthorized interception of wire and oral communications in such a way that their contents could be audibly overheard. "Intercept" was originally defined in the federal wiretapping statute as "the aural acquisition of the contents of any wire or oral communications through the use of any electronic, mechanical, or other device."[15] In 1986, the ECPA extended the federal wiretapping statute to cover any unauthorized interception of wire, oral or electronic

communications. "Intercept" is now defined as "the aural **or other** acquisition of the contents of any wire, **electronic**, or oral communications through the use of any electronic, mechanical, or other device" (amendments bolded).[16]

In addition, the ECPA added a new chapter that prohibited unlawful access to a wire or electronic communication while it was in electronic storage.[17] Violations of the EPCA are punishable by fine and imprisonment for up to five years,[18] and up to 10 years for subsequent offenses.[19] The ECPA also authorizes persons whose communications are intercepted or unlawfully accessed while in electronic storage to bring civil actions.[20] Although these provisions appear on their face to expose an employer who monitored employee e-mails to both criminal and civil liability, there are a number of exceptions and defenses on which an employer may rely to avoid liability.

A major limitation of the ECPA is that 18 U.S.C. § 2511 prohibits only the *interception* of electronic communications. All the courts that have considered the issue have agreed that "an 'intercept' under the ECPA must occur contemporaneously with the transmission."[21] Generally, employer monitoring of employee e-mails will not occur during the course of transmission, but will instead be accomplished through a later search of the employee e-mails on either the employer's server or on the employee's computer. Thus, it would be unusual for employer monitoring of employee e-mails to constitute a violation of 18 U.S.C. § 2511.

Employer monitoring of employee e-mails could potentially violate 18 U.S.C. § 2701, however, which imposes liability on 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 authorized access to a wire or electronic communication while it is in electronic storage in such system ....[22]

Whether an employer's reading of employee e-mails violated § 2701 would turn on whether the e-mails were in electronic storage. The term "electronic storage" is defined in the EPCA as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of back-up protection of such communication."[23] An e-mail message is in "temporary, intermediate storage ... incidental to the electronic transmission thereof" under paragraph (A), when it has been received by the recipient's e-mail system, but has not yet been read by the recipient. In *Fraser v. Nationwide Mutual Ins. Co.*,[24] the trial court explained paragraph (A) by drawing an analogy to a voice-mail system. When a voice-mail is received, it is recorded in the recipient's mailbox and stored until the recipient retrieves the messages from the voice-mail system. At this point, they are in "temporary, intermediate storage," for purposes of paragraph (A) above. When the recipient retrieves the messages, the recipient may either delete them or save them. Once the recipient opens and saves e-mail messages, they are in "permanent storage" for purposes of paragraph (B) above.[25]

Section 2701 expressly provides for an exception, though, if the unauthorized access was "by the person or entity providing a wire or electronic communications service." The court relied on this exception in *Fraser v. Nationwide Mutual Ins. Co.*[26] to find that an employer was not liable under § 2701 for searching through an employee's e-mails, because the e-mails were stored on the employer's e-mail system, which the employer administered. The *Fraser* court cited to an earlier decision, *Bohach v. City of Reno*,[27] in which the City of Reno was found not liable to two police officers for retrieving text messages from an "Alphapage" message system that were stored on the police department's computer system. The *Bohach* court decided that the City of Reno was within the exception in 18 U.S.C. § 2701, because the department was the provider of the message system.

In addition, the ECPA has an express exception for employee consent to the interception of electronic communications. Section 2511(2)(d) provides: "It shall not be unlawful ... to intercept a wire, oral or electronic communication ... where one of the parties to the communication has given prior consent to such interception."[28] Thus, either party to a telephone or e-mail communication may record it and share it with others, or consent to its mon-

itoring by others. Consent to monitoring may be either express or implied from the circumstances.

In *Watkins v. L.M. Berry & Co.*,[29] the court emphasized that the scope of an employee's consent to an employer's monitoring of telephone calls may be limited. Ms. Watkins was employed as a sales representative to solicit advertising in the Yellow Pages. Her employer had informed all of its employees of its policy of monitoring their sales calls as part of its regular training program. The court ruled that although Ms. Watkins had consented to the monitoring of her sales calls, she had not consented to the monitoring of her personal calls. Her consent to the monitoring of sales calls implicitly would cover an inadvertent interception of a personal call, but only for the time that was needed to determine the nature of the call. To the extent that an employer's interception of a telephone call went beyond ascertaining its nature, however, it was outside of the employee's consent for purposes of the ECPA. Similarly, the court ruled in *Deal v. Spears*[30] that an employer's taping of telephone calls was outside of the scope of the employee's consent. Therefore, if an employer is going to rely on the consent exception in 18 U.S.C. § 2511(2)(d), the employer should make sure that the scope of the employee's consent to monitoring is sufficient to cover the monitoring that the employer intends to do.

In summary, an employer will not be subject to liability under § 2511 of the ECPA if it does not monitor the e-mails while they are in the course of being transmitted, and it will not be subject to liability under § 2701 of the ECPA if it is the provider of the e-mail communications system. An employer may also avoid liability under the ECPA for monitoring employee e-mails by obtaining employee consent to the monitoring that the employer intends to do.

CONCLUSION

Although there is a potential for employer liability for searching employee computers and e-mail records, employees face an uphill battle on account of the various defenses employers may have. An employee's expectation of privacy in an employer-provided computer and e-mail records may be negated by an announced company policy. Even in the absence of a company policy regarding computer and e-mail privacy, an employer will probably not be liable to an employee for searching an employer-provided computer or e-mail records if it does so pursuant to a legitimate business purpose. Thus, a company policy regarding computer and e-mail privacy may not be absolutely necessary from a legal standpoint. Nevertheless, having a company policy is desirable, because it helps to avoid misunderstandings by clarifying employer and employee expectations, and therefore, it likely would contribute to better employer-employee relations.

1. 677 S.W.2d 632 (Tex. App. 1984).
2. *Id.* at 638.
3. 1999 WL 339015 (Tex. App. 1999).
4. 914 F. Supp. 97 (E.D. Pa. 1996).
5. 280 F.3d 741 (7th Cir. 2002).
6. 96 Cal.App.4th 443 (2002).
7. 2002 WL 1067442 (E.D. Pa.).
8. 2002 WL 974676 (D. Mass.).
9. 480 U.S. 709 (1987).
10. 281 F.3d 1130 (10th Cir. 2002).
11. 266 F.3d 64 (2nd Cir. 2001).
12. 206 F.3d 392 (4th Cir. 2000).
13. The *Simons* case was followed in *United States v. Slanina*, 283 F.3d 670 (5th Cir.), *judgment vacated on other grounds*, 537 U.S. 802 (2002).
14. 18 U.S.C. §§ 2510 - 2520 (1976).
15. 18 U.S.C. § 2510(4) (1976).
16. 18 U.S.C. § 2510(4) (2000).
17. 18 U.S.C.A. §§ 2701 - 2711 (2000 & 2004 Supp.).
18. 18 U.S.C.A. §§ 2511 (4), 2701 (b)(1)(A) (2000 & 2004 Supp.).
19. 18 U.S.C.A. § 2701 (b)(1)(B) (2004 Supp.).
20. 18 U.S.C.A §§ 2520, 2707 (2000 & 2004 Supp.).
21. Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 113 (3rd Cir. 2004).
22. 18 U.S.C. § 2701(a) (2000).
23. 18 U.S.C.A. § 2510(17) (2004 Supp.).
24. 135 F.Supp.2d 623, 635 (E.D. Pa. 2001), *aff'd in part, vacated in part*, 352 F.3d 107 (3rd Cir. 2004).
25. Theofel v. Farey-Jones, 359 F.3d 1066, 1074-77 (9th Cir. 2004); Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 114 (3rd Cir. 2004).
26. 135 F.Supp.2d 623, 635 (E.D. Pa. 2001), *aff'd in part, vacated in part*, 352 F.3d 107 (3rd Cir. 2004).
27. 932 F. Supp. 1232, 1236 (D. Nev. 1996).
28. 18 U.S.C. § 2511 (2)(d) (2000).
29. 704 F.2d 577, 581-82 (11th Cir. 1983).
30. 980 F.2d 1153, 1156-57 (8th Cir. 2002).

ABOUT THE AUTHOR

Charles W. Adams has been a professor at TU College of Law since 1979. His courses include civil procedure, evidence and Internet law. Professor Adams has been a member of the OBA Civil Procedure Committee since 1983, and was its chairman from 1987-1989 and 1994-2001. Professor Adams has also served as the reporter for the Uniform Jury Instruction Committees for civil, criminal and juvenile cases.