

Monitoring E-Mail In The Workplace: Privacy Rights And Employer Responsibilities


Claire R. La Roche, (E-mail: claroche@longwood.edu), Longwood University

Mary A. Flanigan, (E-mail: mflaniga@longwood.edu), Longwood University

Abstract

Two important legal issues with significant implications for both employers and employees are whether employers have a right to access their employees' e-mail correspondence and whether employers should monitor their e-mail systems. Many people assume that e-mail messages sent and received at work are afforded the same legal protection from invasion of privacy afforded traditional letters. This assumption could not be further from the truth. Privacy law, case law, and Title VII responsibilities are discussed. Suggestions are made for procedures employers should follow to ensure the proper use of e-mail in the workplace.

Introduction

 -mail is one of the most commonly used forms of communication for both business and personal correspondence. Electronic messages differ from formal letters in several respects. First, e-mail messages are informal and frequently sent without due reflection or thought as to the appropriateness of the contents. Unlike a formal letter, recipients may forward e-mail messages to unintended third parties in a matter of seconds. In addition, there is also a tendency to tell jokes or express thoughts in an e-mail that one would be reluctant to say in a formal letter or in person. Two important legal issues with significant implications for both employers and employees are: 1) whether employers have a right to access their employees' e-mail correspondence and 2) whether employers should monitor their e-mail systems.

Employees are often shocked when they are disciplined for the unauthorized use of their employer's e-mail system. To begin with, many people assume that e-mail messages sent and received at work are afforded the same legal protection from invasion of privacy as traditional letters. This assumption could not be further from the truth. Many e-mail users also mistakenly believe that when a message has been "deleted", that it has been permanently purged from the system. Once these messages have been received, a back-up copy may in fact be stored for an indefinite period of time and has the potential to be examined without the knowledge of the communicators. Unlike oral statements that may be forgotten, e-mail leaves a relatively permanent record of what was said.

Several discrimination and sexual harassment cases under Title VII have been based on offensive e-mail messages contributing to a hostile working environment. For this reason, a company has a vested interest in preventing inappropriate comments and material being sent over its e-mail system. This vested interest outweighs any individual's right to privacy.

E-Mail Privacy Laws

An employee may file a complaint under the Electronic Communications Privacy Act (ECPA) and/or institute a common law action for invasion of privacy for the unauthorized reading of e-mail. The first, the ECPA, was passed in 1986 and prohibits the *interception* of e-mail messages by unauthorized individuals and by government officials without a proper warrant. The act of interception must occur during transmission. After e-mail is received, it is impossible for it to be "intercepted" within the meaning of the ECPA. (*Garrity v. John Hancock Life*

Insurance Company, 2002) The ECPA permits an employer to access employees' e-mail in the workplace when (1) one of the parties consents, (2) where the employer is providing the service, or (3) when the monitoring is done in the ordinary course of business. This gives employers broad discretion to read and disclose the contents of employees' e-mail messages. Thus, the ECPA provides limited protection for electronic messages and has proven to be inadequate in establishing e-mail privacy rights for employees.

As public servants, federal and state employees have even more limited privacy rights associated with electronic communications. In fact, not only are employers entitled to examine their e-mail messages, under the provisions of the Federal Records Act (FRA), the public may also access many of these messages through a proper Freedom of Information Act request. According to the FRA, all e-mail sent and received by federal employees must be stored.

Employees also have attempted to hold employers responsible for intercepting employees' e-mail messages under the common law tort of invasion of privacy. Under this theory, employees must prove that the invasion was (1) highly offensive to a reasonable person, and (2) there was a reasonable expectation of privacy on behalf of the employee. (*Borse v. Piece Goods Shop, Inc.*, 1992)

Although there is limited case law, when confronted with the issue of whether employees have a reasonable expectation of privacy, courts have consistently held that e-mail is afforded very little, if any, protection. For example, the plaintiffs in *Bourke v. Nissan* (1993), alleged that their right of privacy was violated by Nissan's periodic review of employees' e-mail messages. Specifically, Bonita Bourke and Rhonda Hall alleged that they were wrongfully terminated and suffered an invasion of their privacy when Nissan retrieved, printed, and read their e-mail containing a number of personal, sexually explicit messages. At trial, Bourke and Hall testified that they were aware that e-mail messages were read from time to time by other than the intended recipients. Furthermore, all employees signed a Computer User Registration Form that restricted their use of company-owned computers and software to company business. In reaching their decision, the court indicated that Nissan was correct in its assertion that employees did not have a reasonable expectation of privacy that was infringed. (*Bourke v. Nissan*, 1993)

In *Smyth v. Pillsbury* (1996), the employer repeatedly told employees that all e-mail communications would remain confidential and would not be used against employees as grounds for termination or reprimand. Pillsbury read Smyth's e-mail messages and terminated him for transmitting inappropriate comments to his supervisor over Pillsbury's e-mail system. (*Smyth v. Pillsbury*, 1996) Despite Pillsbury's assurances of confidentiality, the United States District for the Eastern District of Pennsylvania held that the interception of Smyth's messages did not constitute an invasion of privacy.

In *Garrity v. John Hancock Mutual Life Insurance Company* (2002), Garrity and Clark were terminated for receiving and transmitting sexually explicit e-mail messages and jokes in violation of Hancock's E-Mail Policy. The plaintiffs alleged in part, that viewing their personal e-mail was a violation of their right to privacy. Garrity and Clark admitted that it was likely that these e-mail messages would be forwarded to other recipients. On a motion for summary judgment, the U.S. District Court for the District of Massachusetts dismissed the plaintiffs' complaint. The court noted that Garrity and Clark did not have a reasonable expectation of privacy in their work e-mail.

In *McLaren v. Microsoft* (1999), Bill McLaren stored his e-mail in a private folder that was protected by a password that he created. McLaren assumed that use of a personal password would give him an expectation of privacy. However, the court noted that since the e-mail messages were sent over the network, they were at some point accessible by a third-party. Thus, they were available to the employer and McLaren had no reasonable expectation of privacy.

Guzman and King were terminated from Autoliv ASP, Inc., for sending sexually explicit e-mail messages while at work. Autoliv had an anti-harassment policy and expressly prohibited employees from sending chain letters, jokes, and non-business related messages over their system. Autoliv successfully argued that Guzman and King were discharged for just cause and thus not eligible for unemployment benefits. The court concluded that, "in today's workplace, the e-mail transmission of sexually explicit and offensive jokes, pictures, and videos constitutes

a flagrant violation of a universal standard of behavior.” (*Autoliv, ASP, Inc. v. Department of Workforce Services*, 2001, p. 10)

Title VII Liability Due to Employee’s Use of E-Mail

According to Title VII of the Civil Rights Act of 1964, employers have an affirmative duty to maintain workplace free from sexual harassment and discrimination. A hostile work environment can constitute a form of sexual harassment and discrimination. Electronic transmission of sexually explicit material, suggestive pictures, offensive jokes or comments has exposed employers to Title VII lawsuits.

In several instances, employers have faced significant legal liability for the inappropriate use of e-mail by their employees. In 1995, Chevron paid an out of court settlement totaling \$2.2 million to four plaintiffs for sexual harassment claims in part based on offensive e-mail jokes being forwarded at work. One of these jokes was entitled “25 reasons beer is better than women” (Kunde, p. F-7).

Strauss v. Microsoft (1993) documents another example of a discrimination claim against an employer supported by an employee’s misuse of e-mail containing sexual innuendo. Karen Strauss, the plaintiff in this case, sought relief under Title VII for sex discrimination. She asserted that Microsoft’s alleged non-discriminatory reasons for denying her promotion were merely a pretext. The evidence supporting her assertion consisted of offensive e-mail messages sent by Lazarus, her supervisor. One of the messages sent to his entire staff was entitled “Mouse Balls”, and contained sexual innuendo about male genitalia. Strauss received another e-mail message from Lazarus entitled “Alice in UNIX Land”, which combined computer jargon with sexual innuendo.

The inappropriate use of e-mail has also prompted racial discrimination lawsuits under Title VII. A racist e-mail joke provoked two employees to file a lawsuit against Morgan Stanley. Another “Ebonics joke” disseminated via e-mail at Citibank prompted two employees to file a lawsuit in federal court in New York. (Rapoport, p. C-4) Although the courts in both the Morgan Stanley and Citibank cases held that these e-mail incidents standing alone were insufficient to support a claim of discrimination, the offensive e-mails required the employers to set forth an expensive and time-consuming legal defense of the claims.

Conclusion

E-mail is a fast and effective way to communicate; however, due to the informal nature of this means of communication, e-mail users frequently send messages without giving much thought to the contents. Any time an e-mail is sent, the person composing the message should assume that it will be forwarded. As a rule of thumb, e-mail should not be sent unless it would be appropriate to post it on the bulletin board in the employee lounge. Case law has consistently held that employees do not have a reasonable expectation of privacy when using their employer’s e-mail system. Thus, employees should consider all e-mail sent or received on their company’s system to be legally accessible by their employer and in some cases unintended third parties.

What one person considers to be a funny joke, is often objectionable to someone else. Businesses that tolerate offensive or discriminatory e-mail communications may find themselves as defendants in an unwanted lawsuit. In light of recent case law, employers should implement and monitor an e-mail policy that clearly delineates the boundaries of employee conduct. This policy should notify employees that the system is primarily (or solely) for business purposes and that the employer reserves the right to review and/or disclose messages on the system. Furthermore, the policy should provide that messages containing defamatory, unprofessional, discriminatory, or obscene content are inappropriate and actionable. The manner in which employees will be punished for violating the policy should be outlined. Certainly, employees should be held accountable for their behavior in the workplace. Unfortunately, their behavior often creates a legal exposure for the employer. Litigants have a tendency to follow the “deep pockets” rule and will file suit against the company. The prudent organization will clarify its e-mail policy. Taking the steps listed above may pre-empt a lawsuit or mitigate damages.

References

1. Autoliv, ASP, Inc. v. Department of Workforce Services, 29 P.3d 7 (2001)
2. Borse v. Piece Goods Shop, Inc., 963 F. 2d 611 (3d Cir. 1992).
3. Bourke v. Nissan, California Court of Appeal, No. B068705, July 26, 1993. Reported at www.law.seattleu.edu/chonm/Cases/bourke.html.
4. Federal Records Act, 44 USC Section 2101, et seq.
5. Garrity v. John Hancock Life Insurance Company, 2002 U.S. Dist. LEXIS 8343; 146 Lab. Cas. (CCH) P59, 541 (2002).
6. Kunde, Diana, "Battle brews over e-mail privacy right", *The Dallas Morning News*, p. F-7, August 10, 1998.
7. McLaren v. Microsoft, No. 05-97-00824-CV, 1999 Tex App. LEXIS 4103 (1999)
8. Rapoport, Michael, "Hate E-Mail; Employees' Racist, Sexist Messages Providing Evidence for Bias Suits", *Pittsburgh Post-Gazette*, p. C-4, March 2, 1997.
9. Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996).
10. Strauss v. Microsoft Corp., 814 F. Supp. 1186 (S.D.N.Y. 1993). *Title VII of the Civil Rights Act of 1964*, 42 USC Section 2000(e) et seq