Employer monitoring of telephone calls and electronic mail: Staying within the employer exceptions under federal law

Author: David P. Twomey

Persistent link: http://hdl.handle.net/2345/1492

This work is posted on eScholarship@BC, Boston College University Libraries.

Published in Business Law Review, vol. 28, pp. 119-125, Spring 1995

Use of this resource is governed by the terms and conditions of the Creative Commons "Attribution-Noncommercial-No Derivative Works 3.0 United States" (http://creativecommons.org/licenses/by-nc-nd/3.0/us/)
EMPLOYER MONITORING OF TELEPHONE CALLS AND ELECTRONIC MAIL: STAYING WITHIN THE EMPLOYER EXCEPTIONS UNDER FEDERAL LAW

by DAVID P. TWOMEY*

I. INTRODUCTION

Employers may desire to monitor (intercept, record and listen to) employee telephone conversations in the ordinary course of their business in order to evaluate employee performance and customer service; or document business transactions between employees and customers; or to meet special security, efficiency or other needs. Electronic mail (E-mail) is the fastest growing form of electronic communication in today's workplace. Employers may desire to monitor E-mail for what employers perceive to be sound business reasons, while employees may believe that such monitoring is illegal. This paper analyzes the extent to which an employer can legally monitor employee telephone conversations and E-mail under federal law.

II. EMPLOYER TELEPHONE MONITORING

Employer monitoring of employee telephone calls is subject to Title III of the Omnibus Crime Control and Safe Streets Act of 1968,1 commonly known as the "federal wiretapping statute." Section 2511 of this Act makes it unlawful for any person to willfully intercept, use or disclose any wire, oral or electronic communication. Any person found in violation of this statute may be imprisoned for not more than five years, fined not more than $10,000 or both.2 Addi-

* Professor, Carroll School of Management, Boston College.

tionally, persons whose conversations are illegally intercepted can seek civil damages including the recovery of actual damages plus any profits made by the violator. Or, if statutory damages will result in a larger recovery than actual damages, the violator must pay "the greater of $100 a day for each day of violation or $10,000."**

A. Ordinary Course of Business Exception

Section 2510 (5)(a)(i) of the Act allows an employer to monitor a firm's telephones in the "ordinary course of business" through the use of extension telephones. In *Watkins v. L. M. Berry & Co.*, the Court set forth the general rule that if the intercepted call was a business call, the employer's monitoring of the call was in the "ordinary course of business." However, if it was a personal call, "...the monitoring was probably, but not certainly, not in the ordinary course of business." The Court explained that personal calls may only be monitored "to the extent necessary to guard against unauthorized use of the telephone or to determine whether the call is personal." However, once the employer determines that the call is personal, it is obligated to cease listening immediately, regardless of the content of the legitimately heard conversation. Thus, remarks about a job interview were personal and not within the ordinary course of business exception. However, derogatory remarks about a supervisor as a supervisor were within the ordinary course of business exception, and thus not in violation of the Act.

In *Deal v. Spears*, Newell Spears listened to virtually all twenty two hours of intercepted and recorded telephone conversations between his employee Sibbie Deal and her boyfriend Calvin Lucas without regard to the conversations' relation to Spears' business interest. While Spears might well have legitimately monitored Deal's call to the extent necessary to determine that the calls were personal and made or received in violation of store policy, the scope of the interception in this case was well beyond the boundaries of the ordinary course of business and in violation of this Act.

---


**4** 704 F.2d 577 (11th Cir. 1983).

**5** Id. at 582.

**6** Id.

**7** Id. at 584.

**8** Watkins v. L. M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

**9** Epps v. St. Mary's Hospital of Athens, Inc., 802 F.2d 412 (11th Cir. 1986).

**10** Deal v. Spears 980 F.2d 1153 (8th Cir. 1992).

**11** Id. at 1158.
B. Consent

Under the federal wiretapping statute it is not unlawful "to intercept a wire, oral, or electronic communication...where one of the parties to the communication has given prior consent to such interception." Actual consent may be implied from all of the circumstances, but it may not be cavalierly implied. In Deal v. Spears there was no actual consent because Spears did not inform Deal he was monitoring the phone. Nor was there implied consent, because Spears anticipated that Deal would not suspect that her calls were being monitored.

C. Extent of Prudent Employer Activity

Employer monitoring of employee phone calls can be accomplished without risk of violating the federal wiretapping statute if consent to the monitoring is established. Consent may be established by giving employees prior written notice describing the forms of telephone monitoring to be used, and may well set forth the purposes of the monitoring. It is prudent under ordinary circumstances to advise customers of the employer's monitoring policy through a recorded message as part of the employer's phone answering system.

Where obtaining consent is not possible, employer's monitoring of telephone calls should be carefully restricted to intercepting only business telephone calls.

III. EMPLOYER ELECTRONIC MAIL MONITORING

Electronic mail (E-mail) network systems are a primary means of communication in many of today's businesses, and are deemed alternatives to fax, telephone, or U.S. Mail by some employers. E-mail allows users to send messages from one computer to another any time of the day or week. Recipients need not be simultaneously present at their computers in order to receive their messages. By use of a password, a recipient may access the system to receive messages. Employers receive the benefits of improved productivity and efficiency through the use of E-mail. Owners of corporate E-mail systems, however, may also see this as an opportunity to monitor

---

13 Deal v. Spears at 1157.
14 Basically a sender keys a message into a computer terminal and transmits the message to the recipient over a public network system such as MCI-Mail, Sprint-Mail or AT&T-Mail or a private or corporate mail system. The message is then stored in a computer mailbox and is retrieved by the recipient, who gains access to the system by keying in a password. A password or multiple-level password entry provides security for the system.
the intercompany or intracompany E-mail messages of their employ­ees in order to evaluate the efficiency and effectiveness of the employees, or for corporate security purposes, including the protection of trade secrets and other intangible property interests. When employees are disciplined or terminated for alleged wrongful activities discovered as a result of E-mail searches, or when employees simply find out that an employer has read his or her private E-mail message, the employee may inquire about possible legal redress.

A. The ECPA

The Electronic Communications Privacy Act (ECPA) of 1986 amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The ECPA was enacted in response to the threats to privacy of citizens emanating from the use of more sophisticated surveillance technology. Moreover, the 1968 federal wiretapping law itself needed to be updated to protect citizens subject to the use of new electronic means of communication. The Senate Report on the ECPA made clear that the Act was intended to apply to E-mail. ECPA protection covers intentional actions to intercept communications by unauthorized individuals and individuals acting on behalf of the government. The ECPA also protects electronic communications, including E-mail, that are stored in the computer system for later retrieval or for purposes of backup protection. Violations of the EPCA will subject the violator to both criminal and civil liability. However, exceptions exist for employers, in the ordinary course of

15 Bouke v. Nissan Motor Corp., No.YC003979, slip op. (D.C. Cal. 1993) a trial court rejected a privacy claim of two employees who were fired after the employer read their personal E-mail message. In Plymouth Police Brotherhood v. Labor Relations Commission, 417 Mass. 436 (1994), a union president was suspended for insubordinate remarks contained in an electronic mail message he sent to union members. The union president’s contention that the remarks were protected union activity was not accepted by the Supreme Judicial Court of Massachusetts. 
16 In Shoars v. Epson America, Inc. No. SWC112743, slip op. (D.C. Cal. 1990) it was contended that Alana Shoars, an E-mail administrator for Epsom America Inc., was fired for complaining about her supervisor's reading of employee E-mail messages. Her state court invasion of privacy case was dismissed, and it was later withdrawn on appeal.
business, which allow employers to monitor or read their employees' E-mail without criminal or civil liability.

B. EPCA Exceptions

Two exceptions exist to the EPCA that allow employers freedom to monitor or read their employees' E-mail without suffering criminal or civil liability. Exceptions exist for consentual interceptions and for the property protection of companies operating their own communication systems.\(^24\)

An employer may take advantage of the "consentual interception" exception by directly obtaining each employee's consent to the company's monitoring program. Notice to employees set forth in a comprehensive E-mail Monitoring Policy distributed to all employees is sufficient to establish employee consent and should insulate the employer from liability under the ECPA. Employers must be careful, however, to act in conformity with their own E-mail policy statements for the exception to apply.

The ECPA sets forth a property protection exception for employers operating their own E-mail Systems as follows:

> It shall not be unlawful under this chapter for an...officer, employee, or agent of a provider of [an] electronic communication service...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...\(^26\)

While this statutory language allows for the interception of messages in the normal course of employment in order to protect the employer's rights or property, employers may be justifiably cautious in establishing a monitoring policy based on this statutory language because no court has yet construed the scope and meaning of this language.

C. Extent Of Prudent Employer Activity

An employer who needs to monitor employee E-mail in the ordinary course of its business is not advised to rely solely on the property

---


\(^{25}\) Id. at 2511 (2)(a)(i).

\(^{26}\) Id. Public E-Mail networks such as Prodigy, CompuServe, MCI-Mail, Sprint-Mail and AT&T-Mail are "providers" under the clear language of this exception, along with employers who operate their own E-mail systems. It is not clear whether or not employers who subscribe to one of the public E-mail networks are "agents of a provider" and thus eligible to rely on the property protection exception, or if the employer is a "provider" so long as the employer's monitoring "tap" is used on its own equipment before the message interfaces with the outside E-mail communication service.
protection exemption of the ECPA. A comprehensive policy statement on the employer's justification for monitoring and the methods it will use to monitor the system, may assure that the company is protected under the employee consent exemption to the Act. The employer policy statement may inform employees that the employer's E-mail system is costly for the employer and to be used for business purposes only and not for private communications. Moreover, the employer can articulate that it has no intention of invading employee privacy, but, in the interest of an efficient work place, it will monitor employee E-mail while an employee is under pay and using the employer supplied communication equipment.

IV. CONCLUSION

When employees are at work and being paid, employers have a very significant business interest in monitoring employee activity relating to telephone and E-mail communications in order to efficiently and effectively manage their workforces. The Supreme Court, while recognizing that "not everything that passes through the confines of the business address can be considered part of the workplace context," nonetheless has decided that the balance of interests between an employer's needs and employee privacy should favor the employer. In a public sector case where an employer searched an employee's office, desk and file cabinets for a work related purpose, the Court plurality determined that the balance of interests should favor the employer because the public employer's interest in an efficient workplace outweighed the employee's privacy interest.

The federal law relating to the monitoring of employee telephone conversations in the workplace is now settled. If the employer monitoring results in intercepting a business call, it is within an exception to the federal wiretapping statute that allows such monitoring in the ordinary course of business. Personal calls can be monitored however, only to the extent necessary to determine that the call is personal, and the employer must then cease listening. What is or is not a personal call may well lead to litigation. Employers may avoid this risk by obtaining consent from their employees and customers.

The federal law relating to the monitoring of employee E-mail in the workplace is not clearly settled at this writing as there is no case law directly dealing with this precise matter. If broadly interpreted by the courts, the property protection exception to the ECPA could provide employers with carte blanche rights to monitor and

28 Id. at 717-722.
read workplace E-mail. If the courts apply a rule that allows an employer to read E-mail only to the extent necessary to determine that the communication is personal, then many employers with broad monitoring programs may be exposed to civil and criminal liability. It is thus recommended that employers be certain that they do all that is necessary to come within the consentual interception exception to the EPCA.