

**AN INTRODUCTION FOR VIRGINIA EMPLOYERS TO
THE FEDERAL WIRETAPPING ACT AND
THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**

or

why they tell you “this call may be monitored for quality control purposes”

January 2001

By Raymond L. Hogge, Jr.
Payne, Gates, Farthing & Radd, P.C.
Attorneys and Counsellors at Law
Dominion Tower, Suite 1515
999 Waterside Drive
Norfolk, Virginia 23510-3309
(757) 640-1500
RHogge@PayneGates.com
www.VirginiaLaborLaw.com

**This article is intended solely for educational purposes,
and does not constitute or contain legal advice.**

INTRODUCTION

The Omnibus Crime Control and Safe Streets Act of 1968 (“the Federal Wiretapping Act”), 18 U.S.C. Section 2510 *et seq.*, deals with wire and electronic communication interceptions. A violation of the Wiretap Act is punishable by a fine, imprisonment for up to five years, or both. Congress amended the Wiretap Act when it passed the Electronic Communications Privacy Act of 1986 (“ECPA”), 18 U.S.C. Section 2701 *et seq.*, which prohibits certain access, use and distribution of wire and electronic communications. A violation of it is punishable by a fine, imprisonment for up to one year, or both. Each statute grants a private cause of action to aggrieved individuals. There also is a Virginia statute governing interception of electronic communications, Va. Code Section 19.2-61 *et seq.* (“Interception of Wire, Electronic, or Oral Communications”).

THE FEDERAL WIRETAPPING ACT

In *Katz v. United States*, 389 U.S. 347 (1967), the United States Supreme Court ruled that interception of a telephone conversation in a public telephone booth constituted a search and seizure under the Fourth Amendment if the caller had a “reasonable expectation of privacy.” In *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court extended Fourth Amendment protection to electronic eavesdropping of oral communications. In 1968, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“the Federal Wiretapping Act”), 18 U.S.C. Section 2510 *et seq.*, was enacted to regulate the use of telephone wiretaps and hidden microphones in communications transmitted through a “common carrier” in a manner consistent with the rulings in *Katz* and *Berger*. Although the Federal Wiretapping Act was enacted to address government wiretaps and surveillance, it also applies to private individuals and businesses.

The Federal Wiretapping Act prohibits the intentional interception of wire, oral, or electronic communications, and provides a civil remedy against any person who violates it. *Abraham v. County of Greenville*, No. 00-1150, 2001 U.S. App. Lexis 323 (4th Cir. 1/10/01); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994). In addition, it prohibits the disclosure and use of the contents of wire, oral or electronic communications if “intercepted.” There are a number of limited exceptions to these prohibitions, including a “law enforcement” exception, see *Abraham v. County of Greenville, supra*, and a “business-use” exception, see *Sanders v. Robert Bosch Corp., supra*.

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit ruled that an electronic communication can be “intercepted” only when it is in transit, and not when it is already in storage. Therefore, the court ruled, no “interception” of e-mail occurred when the Secret Service seized a computer containing unread e-mails. This reasoning was followed in *United States v. Reyes*, 922 F. Supp. 818 (S.D.N.Y. 1996), in which the court ruled that pressing a button on a pager to access its memory did not constitute “interception” within the meaning of the ECPA. See also *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996). Thus, under these cases, in order to violate the Wiretap Act an employer probably would have to intercept the e-mail or other electronic communication while the transmission was actually occurring. This could occur, for example, if the employer monitored an employee’s e-mail, internet activity, or FTP download while it was actually taking place. Accessing e-mail that already was downloaded, on the other hand, may not be covered. This was one of the gaps in the Federal Wiretapping Act that was intended to be filled by the Electronic Communications Privacy Act of 1986, discussed below.

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

In response to the growth of technology, Congress passed the Electronic Communications Privacy Act of 1986 (“ECPA”), 18 U.S.C. Section 2701 *et seq.* Like the Wiretapping Act, the ECPA applies to private individuals and businesses as well as to government entities. To the existing protections governing wire and oral communications under the Federal Wiretapping Act, the ECPA added new protections against interception and disclosure of *electronic communications*. It also added new protections against access and disclosure of *electronically stored* electronic communications, primarily to address situations involving e-mail.

Although neither the Wiretapping Act nor the ECPA specifically refer to e-mail, courts have held e-mail to be included within the definition of covered electronic communications. See, e.g., *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997).

Once an e-mail is received into “electronic storage,” it can become subject to the ECPA. The ECPA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incident to the electronic transmission thereof,” and “any storage of such communications by an electronic communications service for purposes of backup protection of such communication.” 18 U.S.C. Section 2710(17). With certain exceptions, it provides that a violation occurs if any person “intentionally accesses without authorization a

facility through which an electronic communication service is provided, or 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 the system....” 18 U.S.C. Section 2702(a).

The issue for the employer therefore may become one of authorization. If the employer has a specific written authorization signed by the employee, the employer probably is reasonably safe. Will an e-mail policy statement in an employee handbook suffice? The answer to this question is not yet certain.

Other questions also remain unanswered under the ECPA. For example, the ECPA, under some circumstances, makes the use or disclosure of the contents of electronic communications a separate offense. This would apply where, for example, the party using or divulging the information is an “electronic communications service.” But when is an employer an “electronic communications service” covered by the ECPA? The answer may not always be clear, but there are some case providing guidance. This issue arose, for example, in *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998). In *Anderson Consulting*, Anderson Consulting was hired by UOP to perform a systems integration. As part of that work, UOP allowed Anderson Consulting’s employees to use UOP’s e-mail system to communicate with one another and with outside persons. Litigation arose after the project was terminated by UOP, and UOP divulged to the Wall Street Journal certain e-mails of Anderson Consulting’s employees remaining on UOP’s computer system. UOP sued under the ECPA, alleging unauthorized disclosure in violation of the ECPA. The court, however, ruled that UOP was not providing electronic communications services to the public merely because it allowed Anderson Consulting’s employees to use its e-mail system. The court also noted that Anderson Consulting was a contractor, not a member of the public at large intended to be protected by the ECPA.

The ECPA contains three exceptions to its prohibitions: (a) the provider exception, (b) the ordinary course of business exception, and (c) the consent exception. *See generally*, Alexander Rodriguez, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 Emory L. J. 1439 (Fall 1998).

The “provider exception” is established in Section 2511(2)(a)(i). It allows “network providers” to intercept, disclose, or use employees’ e-mail, if done during the ordinary course of business, and if either necessary to the rendition of service or necessary to the rights or property of the company. For example, interception or access could be justified if necessary to protect against security breaches, to prevent disclosure of trade secrets, or for system maintenance. Employers, however, should proceed with caution in relying upon the provider exception, since there remains disagreement regarding its proper interpretation. One issue on which there is disagreement is when a company is appropriately regarded as a “network provider.” There is authority indicating that companies maintaining their own computer networks are within the definition. *See, e.g., Unites States v. Mullins*, 992 F.2d 1472 (9th Cir. 1992); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392 (W.D. Okla. 1978), *aff’d*, 611 F.2d 342 (10th Cir. 1979). But what if the company outsources its network? It is not clear whether the company then would qualify as a “network provider,” although it seems logical that it should.

The “ordinary course of business exception” is established in Section 2510(5)(a)(1). In order to establish a claim under the ECPA, a plaintiff must prove the defendant accessed the electronic communication with an “intercepting device.” Excluded from the definition of such devices, however, is “any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider or wire or electronic communication service in the ordinary course of business and being used by the subscriber or user in the ordinary course of business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business.” To determine whether the device is used in the ordinary course of business, courts have examined the employer’s legal interest at stake, and have taken a number a approached to analyzing the issue.

The Fourth Circuit addressed this exception in *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994). In *Sanders*, the plaintiff, Beverly Sanders, was a security officer employed by Gaurdsmark, Inc., which provided security services to Bosch Corporation in South Carolina. Without Sanders’ knowledge or consent, Bosch installed a tape recording device known as a “voice logger” that recorded all telephone conversations on some of the telephone lines going to the security office where she worked. Sanders learned of the recording, and sued Bosch, claiming it unlawfully intercepted her communications. Bosch defended on the grounds that the voice logger fell within the business-use exception of the Act. The Fourth Circuit rejected that argument, for two reasons.

First, the voice logger was not a telephone or telegraph instrument, equipment or facility or a component thereof provided by and installed by BellSouth (which provided the plant’s communications system) in the ordinary course of its business, and was not supplied by Bosch for connection to BellSouth facilities. Bellsouth, the court noted, did not sell such items in the ordinary course of its business, and even if BellSouth did sell such equipment, such equipment did not serve to further the plant’s communications system. Furthermore, the voice logger was not used in the ordinary course of Bosch’s business. Although Bosch claimed it used the device because it was concerned about bomb threats, the court found that claim unsupported by the evidence.

“Second, and of greater import, is the fact that Bosch never notified the security guards, other than the Guardsmark supervisors, that the recordings were being made. In light of the Act’s clear purpose of protecting individuals’ privacy interests, the determination of whether the use made of a surveillance device falls within the ordinary course of business so as to satisfy section 2510(5)(a)(i) necessarily entail examination of whether such use was covert or open. Covert use of a surveillance device must be justified by a valid business purpose. Here, the justification advanced for the ongoing interception of telephone calls, i.e., the fear of bomb threats, does not in any way explain the fact that Bosch failed to inform any Gaurdsmark personnel, other than supervisors, of the use of the voice logger. In short, there is no business reason asserted for the decision not to notify all the Gaurdsmark employees of the use of the voice logger.”

The “consent exception” is met when one party to a communication has given prior consent to the interception be a third party. The Act provides:

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18. U.S.C. Section 2511(2)(d). It is notable, however, that this “consent” exception does not apply if the communication is intercepted “for the purpose of committing any criminal or tortious act...” In *Carter Machinery Co. v. Gonzales*, Civ. Action No. 97-0332-R, 1998 U.S. Dist. Lexis 8106 (W.D. Va. 3/27/98), the court held that “parties proceeding on a theory of ‘recording for a tortious purpose’ ... must in most cases base any such claim on underlying state tort law.” Although the plaintiff in this case alleged fraud, constructive fraud, interference with business relationships, and civil conspiracy in support of his wiretapping claim, the wiretapping claim failed because he failed to sufficiently allege the state tort claims. However, it appears from the decision that any well-pled claims for state tort actions could serve as the basis for a “tortious purpose” wiretapping claim even where one of the parties consented to the recording.

One issue that arises frequently in the workplace context is whether consent to monitoring must be expressly granted by the employee, or whether it can be implied from the fact that the employer has issued a policy notifying employees that monitoring may occur. One early case on point is *Watkins v. L.L. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983). In *Watkins*, the employer had an established policy that all business calls would be monitored and personal calls would be monitored only to the extent necessary to determine whether the call was for business or personal purposes. (This is an appropriate policy, since in most circumstances an employer has little legitimate business interest in listening to the entirety of any employee’s personal calls.) The employee sued, claiming unlawful interception of a personal call. The employer defended on the grounds that the circumstances of the employment demonstrated implied consent by the employee for monitoring of all calls. The court rejected that argument, holding that the implied consent of the employee was limited to the monitoring described in the company policy. Similarly, in *Deal v. Spears*, 980 F.2d 1153 (8th Cir 1992), the court rejected the employer’s argument that consent could be implied from the fact the employer notified its employees that monitoring might be necessary to reduce the number of personal calls made during working hours.

CONCLUSION

These cases call for caution on the part of employers who wish to obtain the consent of employees to workplace monitoring. While monitoring announcements to employees may be sufficient, the safer course of action is to obtain a specific written consent to monitoring from each employee, which should be retained in the personnel file. For convenience, this affirmative consent may be obtained by including appropriate language in the employee handbook acknowledgement signed by each employee, provided the monitoring policy is included in the employee handbook.