

THE STATUTORY FOUNDATION OF PRIVACY IN THE ELECTRONIC WORKPLACE

Tammy Lennon

A. Federal Law - The Electronic Communications Privacy Act of 1986 (“ECPA”), which encompasses the Wiretap and Stored Communications Act.

1. Generally

The Electronics Communication Privacy Act (“ECPA”), 18 U.S.C. §2701, et. seq., which was signed into law on October 21, 1986, prohibits the interception, access, disclosure, or use of another’s wire or electronic communication. The Act also prohibits entry into an electronic system to alter or obtain stored communications.

In general, The Act prohibits three types of activities. First, it prohibits any person from “intentionally intercept(ing)” or attempting to intercept “any wire, oral, or electronic communication.” 18 U.S.C. §2511(1)(b). “Intercept” is defined as the “aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device.” 18 U.S.C. §2510(4). An "electronic communication" is "any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system." The ECPA also prohibits any person from intentionally disclosing or attempting to disclose the contents of any wire, oral or electronic communication known to have been unlawfully intercepted. 18 U.S.C. §2511(c). Third, The Act prohibits any one from “intentionally access[ing] without authorization a facility through which an electronic communication service is provided” or to access, without authorization, “a wire or electronic communication while it is in electronic storage.” 18 U.S.C. §2701(a). As it is used in identifying all three types of activities,

an "electronic communication" is "any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system."

The Federal Act does not require employers to give employees prior notice about electronic surveillance, and in some situations allows employers to imply employee consent to surveillance. See 18 U.S.C. §2511(2)(d). Any surveillance or monitoring of employee activity or communications must, however, be within that employer's ordinary course of business. See U.S.C. §2510(5)(a).

2. Electronic Mail

The ECPA protects the transmission and storage of digitized textual information contained in electronic mail. The Act amended the definition of "intercept" to clearly make illegal the interception of the non-voice portion of a wire communication (i.e., the data or digitized portion of a voice communication). The "non-voice portion" includes "electronic communication," which is defined as "any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system."

The Act was designed to protect the contents of stored electronic mail, voice mail and remote computing services. It was also intended to prohibit providers of the electronic communication services from disclosing the contents of communication that has been stored electronically without the lawful consent of the person who originated the communication.

3. Cellular Telephones

In Hall vs. U.S., a 1973 U.S. Circuit Court of Appeals held that mobile telephone conversations are protected under Title III when part of a communication is carried to or from a

'landline' telephone." In 1986, the ECPA broadened the definition of protected "wire communication" to "include communications utilizing wires, cables, or other line connections within a switching office . . . regardless of whether the communications are between two cellular telephones or between a cellular telephone and a 'landline' telephone." While the Act protects the wire portion of cordless phone conversations, it excludes from the definition of "wire communication" "the radio portion of a telephone that is transmitted between the cordless telephone handset and the base unit."

B. State Law - The Maryland Wiretapping and Electronic Surveillance Act

The Maryland Wiretapping and Electronic Surveillance Act, Md Code Ann., Cts & Jud. Proc. §§10-401, et seq. (hereinafter "The Maryland Wiretap Act") makes it a felony to "wilfully" [sic] intercept, attempt to intercept, or have someone else intercept on one's behalf any wire, oral or electronic communication. In addition, one may not "willfully" use or disclose any information concerning the identity of the parties or the existence, substance, purport, or meaning of such a communication if one knows or has reason to know the information was obtained illegally.

Unlike the ECPA, the Maryland Wiretap Act requires a violation to have been willful. Deibler v. State, 365 Md. 185, 776 A.2d 657 (2001). An interception is "willful" if it was done intentionally or purposely; an interceptor need not have been aware that his or her conduct was unlawful. Id. "Oral communication" includes any conversation or words spoken to or by any person "in private conversation." For a conversation to be private and thus protected under the statute, the parties to that conversation must have had a reasonable expectation of privacy in it.

Nonetheless, it is not a violation of the statute for a person to intercept a communication if the person is a party to the communication *and* all the parties to the communication have given

prior consent to the interception, unless the communication is intercepted for the purpose of committing a criminal or tortious (wrongful) act. 18 U.S.C. §2511(2)(c). Thus, one who consents at the time of recording cannot later cause that conversation to be suppressed from evidence in court on the basis that the other party did not consent to the recording. *State v. Maddox*, 517 A.2d 370 (Md. Ct. Spec. App. 1986).

The statute prohibits the interception of a radio communication that is transmitted by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire department systems, that is readily accessible to the general public. "Readily accessible" means, among other things, that the communication is not scrambled or encrypted. Because merely listening in on an ordinary telephone extension is not an interception, the statute does not protect the radio portions of cordless telephone communication. Put differently, the Maryland Wiretap Act reaches only oral and wire communications; it does not regulate silent video surveillance. *Ricks v. State*, 537 A.2d 612 (Md. 1988).

The statute furthermore prohibits possession of a device if the possessor knows or has reason to know that its design makes it "primarily useful for the purpose of the surreptitious interception of wire, oral or electronic communications."

Since violation of the Maryland Wiretapping and Electronic Surveillance Act is a felony, it is punishable by imprisonment of not more than five years, a fine of up to \$10,000, or both. Anyone whose communication is illegally intercepted, disclosed or used can sue to recover either actual damages or statutory damages, calculated at the rate of \$100 per day of violation or \$1,000, whichever is greater. The statute also provides for punitive damages, reasonable attorney's fees and court costs. See Md Code Ann., Cts & Jud. Proc. §§10-401, et seq. (1997);

Fearnow v. C&P Telephone Co., 655 A.2d 1 (Md. Ct. Spec. App. 1995); *Ricks v. State*, 537 A.2d 612 (Md. 1988); *Adams v. State*, 406 A.2d 637 (Md. Ct. Spec. App. 1979), *aff'd*, 424 A.2d 344 (Md. 1980); *Benford v. American Broadcasting Co.*, 649 F. Supp. 9 (D. Md. 1986); *Earley v. Smoot*, 846 F. Supp. 451 (D. Md. 1994); *Hawes v. Carberry*, 653 A.2d 479 (Md. Ct. Spec. App. 1995); *State v. Maddox*, 517 A.2d 370 (Md. Ct. Spec. App. 1986).

C. Employees' Common Law Privacy Claims - Invasion of Privacy and Intentional Intrusion Upon Seclusion.

An employee who perceives that his employer has intruded upon his reasonable expectation of privacy may sue under the common law claims of "Invasion of Privacy"/"False Light," or "Intrusion Upon Seclusion."

1. Invasion of Privacy / False Light

To maintain a claim a claim for "Invasion of Privacy" or "False Light," a plaintiff must show that his private matter was publicly disclosed. To be "private," an individual must have had "more than just a desire to keep a particular fact private, but the matter revealed must be a personal matter that would be highly offensive for a reasonable person to have disclosed to others." See *Taylor v. Nations Bank*, 365 Md. 166, 776 A.2d 645 (2001).

2. Intrusion Upon Seclusion

"Intrusion Upon Seclusion" is "the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be highly offensive to a reasonable person." See *Furman v. Sheppard*, 130 Md. App. 67, 77, 744 A.2d 583, 586 (2000). To determine whether an intrusion was "offensive to a reasonable person," a court will examine the degree of the intrusion, surrounding circumstances, and the accused's motives. A court will rely most

heavily, however, upon whether the victim's reasonable expectation of privacy was invaded. O'Connor v. Ortega, 480 U.S. 709 (1987).

Generally, a plaintiff-employee must show that his expectation of privacy was not only reasonable, but objectively reasonable. Where an employee challenges an employer's monitoring of his e-mail or voice mail, courts ask first, whether the employee had a reasonable expectation of privacy, and second, whether the employer had a legitimate business justification for monitoring that outweighed any privacy interest that the employee may have had. See Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

1. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

Smyth arose when an employee sent an e-mail to his supervisor on the company's computer system. In that e-mail, the employee threatened "to kill the backstabbing bastards" and compared an upcoming holiday party to a "Jim Jones Kool-Aid affair." The employee's company discovered the e-mail, and the employee was fired. The employee thereafter sued on a number of bases, including wrongful termination.

In considering the first prong of the two-part analyses -- whether the employee had a reasonable expectation of privacy in the e-mail, the District Court considered that: (a) the company informed its employees that all e-mail communications would remain confidential and privileged, and (b) the employee's communications were made voluntarily to a supervisor over a company-wide e-mail system. On this basis, the court held that the employee therefore did not have a reasonable expectation of privacy in his e-mail, *even though* the company's standard practice was to assure its employees that e-mails would be kept confidential. As to the second prong of the two-part analysis, the court held that the company's interest in preventing inappropriate and unprofessional comments and activities over the company-wide e-mail system

outweighed any privacy interest the employee may have had in his communication. The employee's claim was dismissed.

2. Bourke v. Nissan Motor Corp., No. B068705 (Cal. Ct. App. July 26, 1993).

In Bourke, the employee plaintiffs sent e-mails to their supervisor of a sexual nature, including messages containing inappropriate jokes and language. Upon receiving these e-mails, the supervisor printed and showed them to Nissan. The employees complained that their personal e-mails were being monitored, and were thereafter fired. The Court of Appeals dismissed the plaintiff's claims primarily on the basis that: (a) the plaintiffs received training seminars about the use of e-mails systems, and because (b) the plaintiffs signed a "computer registration form" on which the company's policy "that employees and contractors restrict their use of company-owned computer hard-ware and software to company business" was stated.

3. McLaren v. Microsoft Corporation, 1999 W.L. 339015 (Tex. App. - Dallas 1999).

The employee in McLaren stored personal e-mail messages on his office computer. Microsoft discovered these e-mails, and McLaren sued. In court, McLaren claimed that he had a reasonable expectation of privacy in those e-mails because he stored the e-mail in "personal folders" on his computer, and because Microsoft consented to such storage. The Court of Appeals held that because the plaintiff's e-mail messages were stored on property that was part of the office environment (rather than on the employee-plaintiff's personal property), he did not have a reasonable expectation of privacy in those messages.

In Maryland, to establish a cause of action for "Unreasonable Intrusion Upon Seclusion," a plaintiff must show: 1) that there was an intentional intrusion upon seclusion; and 2) that the

intrusion would be highly offensive to a reasonable person. Pemberton v. Bethlehem Steel Corp., 66 Md. App. 133 (1986). The intrusion must be into a private place or a private seclusion. Whether there is “seclusion” in turn depends upon whether the employee-plaintiff had a reasonable expectation of privacy in it. Furman v. Sheppard, 130 Md. App. 67, 77, (2000).

Where an employer puts his employees on notice that certain areas may be searched or inspected, an employee’s expectation of privacy in those areas will probably not be “reasonable.” Faulkner v. State, 317 Md. 441 (1989). A prudent employer will thus take care to give his employees notice and/or warning that certain areas are under surveillance.