

PRIVACY LIMITATIONS FOR ELECTRONIC SURVEILLANCE AND GENETIC TESTING IN THE WORKPLACE

by
Steven Hymowitz*
David Bendana

McCalla, Thompson, Pyburn, Hymowitz & Shapiro, L.L.P.
Attorneys at Law
Poydras Center
Suite 2800
650 Poydras Street
New Orleans, Louisiana 70130

ELECTRONIC SURVEILLANCE

In today's workplace, employee productivity and efficiency are at a premium. As a result, employers are constantly presented with circumstances requiring scrutiny of an employee's activity at work. Circumstances can range from suspicion of drug use, excessive personal phone calls, or revealing trade secrets to a competitor. Additionally, with personal computers complete with Internet access, games and e-mail capabilities on employees' desks, employers are increasingly vulnerable to employees engaging in non-productive activities in the workplace.

However, an employer's right to inquire and obtain information about its employees is limited by the right of privacy. The U.S. and State Constitutions, various Federal and state statutes, and even common law provide employees protections against intrusions into their privacy. For example, improperly conducted investigation, or the improper disclosure of the

* Steven Hymowitz is a senior partner in the law firm of McCalla, Thompson, Pyburn, Hymowitz & Shapiro, which specializes in representing management in the field of labor and employment law. He received his B.S. degree from Fordham University and graduated from Memphis State University School of Law in 1974, where he was an associate editor for the The Memphis State Law Review. Mr. Hymowitz is a former Management Co-chair of the Committee on Employee Rights and Responsibilities of the American Bar Association Labor and Employment Law Section

results of an investigation, could expose an employer to liability. This paper discusses the scope of an employee's right to privacy in the context of three types of electronic surveillance: telephone or audio surveillance, video surveillance, and e-mail monitoring. Further, this paper suggests techniques and proactive steps which employers may use to monitor employee activity and conduct investigations without unlawfully infringing upon an employee's right to privacy.

I. Limitations on Electronic Surveillance

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2520, commonly referred to as the Federal Wiretapping Act, generally prohibits the interception, disclosure or intentional use of wire, oral or electronic communications, including those which occur in the workplace. A wire communication or the attempted interception of same, is one that carries a person's oral communication over a wire cable or like facility such as a phone call. The definition of a wire communication includes the "electronic storage of such communication." *See* 18 U.S.C. § 2510(1). An "oral communication" is an oral communication made in circumstances indicating the individual uttering the communication expected it would be private. *See* 18 U.S.C. § 2510(2). Private conversations between two individuals are "oral communications." *See Dorris v. Absher*, 959 F. Supp. 813 (M.D. Tenn. 1997), *rev'd on other grounds*, 1999 WL 349955 (6th Cir., June 2, 1999)(employees of county office had reasonable expectation of privacy in conversations tape-recorded by office director in the office, and therefore such conversations were "oral communications" entitled to protection under federal wiretapping statute). An electronic communication is the transfer of information (writing, images, signals, sounds, data, etc.)

transmitted by electronic means including radio waves but is not an oral or wire communication. E-Mail is an example of an “electronic communication.”

“Interception” is also a defined term. It means the aural or other acquisition of the contents of any oral, wire or electronic communication, through the use of any electronic or mechanical device. *See* 18 U.S.C. § 2570 (4). *See also Fields v. The Atchison, Topeka & Santa Fe Ry.*, 985 F. Supp. 1308 (D. Kan. 1997), *withdrawn in part on other grounds*, 5 F. Supp. 2d 1160 (D. Kan. 1998)(individual's conduct in merely listening to allegedly illegally-obtained audiotape of private telephone conversations did not amount to "use" of such communication in violation of the Act). However, the Act has an exception for employers who act in the "ordinary course of business." This term has been interpreted to mean that an employer can electronically monitor any business-related communication without the employee's knowledge or consent. An employer may not, however, monitor communications of a purely personal nature. *See, e.g., Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992)(exemption does not apply where employer intercepted calls beyond its business necessity of determining whether employee was stealing from employer). An employer does not violate the Act if it terminates electronic monitoring once it is determined a monitored call is purely personal.

The Act provides a civil cause of action to anyone whose communications are unlawfully intercepted. *See* 18 U.S.C. § 2520. Successful plaintiffs may recover actual or statutory damages (\$10,000 or \$100 a day for each day of violation, whichever is greater), punitive damages, and attorney's fees. The Act also makes the unlawful interception of an oral, wire, or electronic communication, or the attempted interception of same, a crime punishable by fine and/or imprisonment.

The Act provides two other defenses to employers. First, the Act does not apply if the employer has the consent of one party to the communication. *See* 18 U.S.C. § 2511(2)(d). In addition, under the "provider" exemption, telephone companies and other employers that provide wire communication services may monitor calls for service checks. *See* 18 U.S.C. § 2510(5).

While the Federal Wiretapping Act serves as the most important limitation to electronic surveillance in the workplace, the U.S. and state constitutions, other statutes, and common law claims for "invasion of privacy" also limit employers' rights to electronic surveillance in the workplace.

A. Telephone/Audio Surveillance

Certain general rules applicable to wiretapping or eavesdropping on telephone calls in the workplace have evolved under the case law. For example, the courts have drawn a distinction between business and personal telephone calls, generally frowning on employers who monitor personal phone calls. *See Watkins v. L. M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) ("a personal phone call may not be intercepted in the ordinary course of business ..., except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not"). Similarly, the courts consider a "general practice of surreptitious monitoring" more egregious "than monitoring limited to specific occasions." *See Briggs v. American Air Filter Co., Inc.*, 630 F.2d 414 (5th Cir. 1980). Additionally, a narrow and limited "telephone extension in the ordinary course of business" exception to the federal wiretapping statute has developed in the employment context. In the *Briggs* case, the Fifth Circuit defined the limited circumstances under which an employer's monitoring of a telephone call may be permissible:

...when an employee's supervisor has particular suspicions about confidential information being disclosed to a business competitor, has warned the employee not to disclose such information, has

reason to believe that the employee is continuing to disclose the information, and knows that a particular phone call is with an agent of the competitor, it is within the ordinary course of business to listen in on an extension phone for at least as long as the call involves the type of information he fears is being disclosed.

Id. at 420; *see also James v. Newspaper Agency Corp.*, 591 F.2d 579, 582 (10th Cir. 1979) ("Here the installation was not surreptitious, but with advance knowledge on the part of both management and its employees, and was for a legitimate business purpose"); *Epps v. St. Mary's Hospital of Athens, Inc.*, 802 F.2d 412, 416-17 (11th Cir. 1986) ("this was not a personal call. It occurred during office hours, between co-employees, over a specialized extension which connected the principal office to a substation, and concerned scurrilous remarks about supervisory employees in their capacity as supervisors. Certainly the potential contamination of a working environment is a matter in which the employer has a legal interest"); *Jandak v. Village of Brookfield*, 520 F. Supp. 815, 824 (N.D. Ill. 1981) ("routine, nonsurreptitious recording of a police investigative line which results in the recording of a conversation of an officer misusing the line for private purposes, where the officer should have known that the line was monitored, was in the ordinary course of the police chief's duties as a law enforcement officer, and is exempted from the statute"); and *Simmons v. Southwestern Bell Telephone Co.*, 452 F. Supp. 392, 396 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979) ("Defendant's monitoring activities must be considered reasonable, when the nature of plaintiff's employment is considered with the fact that all employees at his station knew, and had acquiesced to, defendant's monitoring of their incoming and outgoing calls, while at the test board, both for the purpose of preventing his persistent use of the test board phones for personal calls, a practice against which plaintiff had been warned several times.") *C.f. Deal v. Spears*, 780 F. Supp. 618 (W.D. Ark. 1991), *aff'd*, 980 F. 2d 1153 (8th Cir. 1992) (Employer's interception and disclosure of plaintiff's phone conversations of a sexual nature was not within the exception).

While acknowledging the "business extension" exception, other courts have refused to grant summary judgment due to the existence of disputed material facts. *See, e.g., Watkins v. L. M. Berry & Co.*, 704 F.2d 577, 585 (11th Cir. 1983); *see also Abel v. Bonfanti*, 625 F. Supp. 263, 270 (S.D. N.Y. 1985) ("Abel has asserted that his personal calls were intercepted without his consent or knowledge through Bonfanti's use of a tape recorder on his office extension. While Bonfanti has proffered a business purpose for using the recorder and has claimed that he minimized his intrusions on personal calls, these rationales are sharply disputed by affidavits submitted by Abel. Therefore, a factual dispute is present as to whether Bonfanti's recording of Abel's telephone calls was in the ordinary course of business.").

In *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992), the Eighth Circuit considered the scope of the business use exception. In that case, Plaintiff was an employee of a liquor store that was broken into and burglarized. Defendants, owners and operators of the store, suspected the theft was an inside job orchestrated by Plaintiff. Defendants decided to use a recording device to monitor the telephone calls to and from the store. The interception and taping of calls went on for approximately two and one-half months. Defendants terminated Plaintiff after intercepting and taping a phone call in which Defendant sold a keg of beer at a reduced price to a person with whom Plaintiff was having an extra-marital affair. In addition to this particular telephone call, defendants taped numerous calls between Plaintiff and her lover that were sexually provocative in nature. The Court described the case as one of "sex, lies, and audio tapes." Plaintiff brought an action pursuant to the Act alleging an unlawful interception of the phone calls. Defendants asserted two defenses: (1) that Plaintiff impliedly consented to the taping of her phone calls and (2) that the use of the telephone extension to tape the calls of employees was an action taken in the ordinary course of business. The trial court rejected both defenses, finding that the vast majority of the intercepted calls were

personal in nature and Defendants did not take any steps to limit their intrusion on the privacy of the callers. Accordingly, the trial court found each Defendant liable for statutory damages both to Plaintiff and Plaintiff's paramour. The trial court rejected Plaintiff's claim for punitive damages stating that Defendants' conduct was "inexcusable" but not "wanton, reckless, or malicious." On appeal, Defendants argued the "telephone extension" or "ordinary course of business" exception that should apply to this case. In rejecting this argument, the Eighth Circuit held it was the tape recorder rather than the extension phone which caused the interception of the calls since the telephone calls were not listened to until the tape recorder was subsequently played back. Second, the court held that even if the extension phone caused the interception, listening to 22 hours of continuous tape recordings far exceeded the scope of the "ordinary course of business" exception. The court suggested that the "ordinary course of business" exception may have permitted Plaintiffs to have monitored Defendant's calls but only to the extent necessary to determine that the calls were made and/or received in violation of store policy.

In *Dorris v. Absher*, 1999 WL 349955 (6th Cir., June 2, 1999), the Sixth Circuit recently considered the definition of the term "use" under the Act. In that case, Charles Absher had secretly recorded conversations of four employees by placing a tape recorder in a common office for the employees. After recording employee conversations criticizing him, Absher disclosed the tape recordings to his wife, Della Absher. Della Absher listened to the tape recordings. Also, from the tapes, Charles Absher dictated termination notices for two of the employees that Della Absher typed. Plaintiff alleged that Della Absher, by listening to the tapes and typing termination notices from the tapes, violated the Act by her intentional "use" of the intercepted communication. The Sixth Circuit first held that, as a matter of law, "listening alone is insufficient to impose liability for 'using' illegally intercepted communication". Moreover, the

Court held that Della Absher did not “use” the tapes when she dictated the termination notices because “it was Charles Absher who composed the letters, and that Della Absher did nothing more than take dictation from him”. Charles Absher, however, was found to have violated the Act.

Cordless phones operate by transmitting a person’s voice from the headset of the phone, over radio waves to the base of the headset, which then transmits the voice over the phone lines. Intercepting the communication between the headset of the phone and the base is extremely simple and often happens inadvertently. As a result, Congress initially exempted these transmissions from the class of protected transmissions under the Act.

In 1994, Congress removed the exemption for these transmissions and they are now protected wire communications. Under federal law, individuals who deliberately intercept these communications are now subject to a fine of up to \$500 as well as potential civil damages. *See* 18 U.S.C. §§ 2511(4) and 2520. Despite this, in cases brought outside the ambit of the Act, courts continue to hold that individuals using cordless phones have no expectation of privacy in those communications. *See e.g. McKamey v. Roach*, 55 F.3d 1236, 1239-40 (6th Cir. 1995)(no reasonable expectation of privacy in communications over a cordless telephone because such an expectation is not objectively reasonable); *Singleton v. Cecil*, 955 F. Supp. 1164 (E.D. Mo. 1997), *order rev’d on other grounds*, 155 F.3d 983 (8th Cir. 1998). The Louisiana Supreme Court follows this reasoning. “Under either the federal or state constitutions, however, we conclude that, given the nature of cordless telephone transmissions, the interception of such broadcasts does not constitute a ‘search’ because any expectation of privacy carried out in these communications is objectively unreasonable.” *State v. Niesler*, 1995 WL 118804, *9 (La. 1995), *withdrawn and rev’d on other grounds*, 666 So.2d 1064, 1067 (La. 1996).

Examples of cases involving claims of an unlawful interception or invasion of privacy through telephonic, audio, voice mail, pager, or other electronic surveillance include: *Pascale v. Caroline Freight Carriers*, 898 F. Supp. 276 (D.N.J. 1995)(employer violated Federal Wire Tapping Act by intercepting call with a tape recorder connected to a dispatch busboard without employees' knowledge); *Roberts v. Ameriable Int'l, Inc.*, 883 F. Supp. 499 (E.D. Cal. 1995)(employee could use, at her sexual harassment trial, secret tape recordings of conversation with her supervisor and others, however, supervisor was entitled to review the tape before his deposition); *Hart v. Clearfield City, Davis County*, 815 F. Supp. 1544 (D. Utah 1993)(telephone dispatcher had no reasonable expectation of privacy with respect to call she received, even if she wrongly believed that line on which she received call was unrecorded because dispatcher held sensitive position, critical issues were discussed on telephone, calls were routinely recorded, and they frequently were reviewed for business purposes). *Wesley v. WISN Division - Hearst Corp.*, 6 F. Supp. 812 (E.D. Wis. 1992)(court held employer did not violate the Electronic Communications Privacy Act where a conversation between two radio station employees was monitored, because employees did not have a reasonable expectation to be free from electronic interception of their oral communication when they knew that, under the circumstances, the monitoring device "might actually be in place"); *Moffett v. Gene B. Glick Co.*, 621 F. Supp. 244 (N.D. Ind. 1985)(employer's placement of intercom in office kitchen to overhear conversations was not an actionable invasion of privacy where no conversations were actually overheard); *Pemberton v. Bethlehem Steel Co.*, 66 Md.App. 133, 502 A.2d 1101, *cert. denied*, 107 S. Ct. 571 (1986)(employer's use of bugging device placed outside of union official's hotel room was an actionable invasion of privacy); *Earley v. Executive Bd. Of the United Trasp. Union*, 957 F. Supp. 997 (N.D. Ohio 1997)(union member and union's executive board violated Federal Wiretap Act by tape recording executive session of

the Public Law Board and by using and disclosing the contents of the tape, for purposes of request for permanent injunction, where member intentionally recorded meeting without knowledge and consent of any of the parties, and member and executive board disclosed contents of recording on numerous occasions with knowledge of how recording was made); *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996) (messages sent on police department's computerized paging system were "electronic communications" rather than "wire communications" or "oral communications" for purposes of wiretap statutes); *Payne v. Norwest Corp.*, 911 F. Supp. 1299 (D. Mont. 1995), *aff'd in part, rev'd in part*, 113 F.3d 1079 (9th Cir. 1997)(employee's recording of messages left on his voice mail at work was not an "interception" within meaning of federal wiretap statute because "interception" requires, at the least, involvement in initial use of device contemporaneous with communication to transmit or preserve the communication, employee's use of handheld recorder to record voicemail messages did not occur contemporaneously with leaving of the messages, and persons leaving message consented to recording of their message by fact that they left a message); *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995)(use of pager clones to intercept numeric transmissions to suspect's digital display pagers was unauthorized interception of electronic communications under ECPA as a matter of law); *U.S. v. Reyes*, 922 F. Supp. 818 (S.D.N.Y. 1996) (pressing button on pager to access its memory is not an "interception" within meaning of ECPA); *Gamb v. Hilton Hotels*, 13 I.E.R. (BNA) 1417 (M.D. Fla. 1997)(fact that employee found tape recorder in his office and that there were memoranda dealing with two in office conversations does not prove that employer tape recorded those conversations); *Gross v. Taylor*, 1997 WL 535872 (E.D.Pa. 1997)(police officers did not have a reasonable expectation of privacy or non-interception while on duty in a patrol car when electronic equipment in police car placed a reasonable person on notice

that there was a strong possibility that conversations could be intercepted); *O'Sullivan v. NYNEX Corp.*, 426 Mass. 261, 687 N.E.2d 1241 (1997) (telephone company did not violate wiretap statute by recording telephone calls between employees and customers when monitoring was conducted in ordinary course of telephone company's business); *Briggs v. American Filter Co.*, 630 F.2d 414 (5th Cir. 1980)(where branch manager had particular suspicions about confidential information being disclosed to a business competitor, had warned employee not to disclose such information, and knew that a particular phone call was with an agent of the competitor, it was within the ordinary course of business for the branch manager to listen in on an extension phone for at least as long as the call involved the type of information he feared was being disclosed and extension telephone exception was applicable such that there was no violation of the Act); *Lane v. Allstate Insurance Co.*, 14 I.E.R. (BNA) 1134 (Nev. 1998)(employee violated state statute when he tape recorded telephone conversation with witnesses as evidence to support his wrongful discharge allegations; state law did not adopt provision in federal wiretapping act that permits interception of wire communications with one party's consent); *Arias v. Mutual Central Alarm Services*, 14 I.E.R. (BNA) 1618 (S.D.N.Y. 1998)(listening to phone calls to determine loyalty of employee falls within Act's exception that permits interception in ordinary course of business).

B. Video Surveillance

The Federal Wiretapping Act has much less an impact on video surveillance of employees. Indeed, the Act does not apply to video-only surveillance because the act of making a silent video does not constitute an interception of an oral, wire, or electronic "communication". See *U.S. v. Koyomejian*, 970 F.2d 536, 537 (9th Cir.), *cert. denied*, 506 U.S. 1005 (1992)(silent video surveillance is neither prohibited nor regulated by the Act); *Thompson v. Johnson County*

Community College, 930 F. Supp. 501 (D. Kan. 1996), *aff'd*, 108 F.3d 1388 (10th Cir. 1997)(no violation of act in installing video-only surveillance camera in locker room because it is interception of oral communication that subjects interceptor to liability, and act does not prohibit silent video surveillance).

Other statutes, like the National Labor Relations Act (“NLRA”), may limit employer use of silent video surveillance. The NLRA provides protections to employees who engage in certain protected activity, *i.e.*, self-organization, form, join, or assist unions, bargain collectively, and engage in other protected concerted activities. *See* 29 U.S.C. § 157. The NLRA prohibits employers from engaging in any practice that interferes with, restrains, or coerces employees in the exercise of these rights. *See* 29 U.S.C. § 158(a)(1). Courts generally have held that video surveillance of employees engaging in these protected activities violates the act because the act of surveillance tends to interfere, restrain, or coerce employees in exercising these rights. *See, e.g., NLRB v. Associated Naval Architects, Inc.*, 355 F.2d 788 (4th Cir. 1966); *NLRB v. Frick Co.*, 397 F.2d 956 (3rd Cir. 1968); *Sunbelt Mfg., Inc.*, 308 NLRB No. 110, 141 LRRM (BNA) 1105 (1992)(videotaping of employee handbilling activity at gate violated the act).

Notwithstanding this general prohibition, Courts have held that it is not a *per se* violation of the NLRA to photograph protected activity if the photography does not interfere with, restrain or coerce employees in the exercise of their rights under Section 7 of the Act. *See, e.g., U.S. Steel Corp. v. NLRB*, 682 F.2d 98 (3rd Cir. 1982); *Aladdin Industries, Inc.*, 147 NLRB 1392, 56 LRRM (BNA) 1388 (1964)(allowing videotaping in anticipation of acts of violence by employees distributing handbills because act of preparatory focusing of camera and any impression of surveillance created thereby was at worst a fleeting one). Clearly, Courts do not prohibit video surveillance of unlawful activity or activity not protected by the Act or for other legitimate

purposes. *See, e.g., Larland Leisurelies, Inc. v. NLRB*, 523 F.2d 814 (6th Cir. 1975)(no violation in photographing picketers where photographs taken to establish pickets engaged in violence for injunction suit); *M.P. Building Corp.*, 165 NLRB 829, 65 LRRM (BNA) 1581 (1967)(no violation in taking pictures of employees while they were performing their required job assignments where no evidence pictures connected with union activities in progress).

Video surveillance of employees in their workplace can be considered a subject of bargaining. *See In re Amoco Petroleum Additives Co.*, 7 I.E.R. (BNA) 854 (7th Cir. 1992)("privacy in the workplace ... is an ordinary subject of bargaining [and] the extent of privacy is a 'condition' of employment").

In addition to statutory protections, individuals claim constitutional and common law rights to privacy from video surveillance. In *Saldana v. Kelsey-Hayes Co.*, 443 N.W.2d 382, 4 I.E.R. (BNA) 1107 (Mich. Ct. App. 1989), after plaintiff sustained a work-related injury, the employer began surveillance of the plaintiff to determine whether he was malingering. The surveillance included observing plaintiff through an open window of his house with a telephoto lens. The employer also sent a letter to plaintiff's physician, outlining the results of the employer's surveillance and suggesting plaintiff could return to work. Plaintiff sought to recover for common law claim "intrusion upon seclusion" of the employee. Rejecting the plaintiff's claim, the court concluded the intrusions did not concern matters which plaintiff had a right to keep private. The court concluded the employer had a legitimate right to investigate plaintiff's physical condition. According to the court, "plaintiff's privacy was subject to the legitimate interest of his employer in investigating suspicions that plaintiff's work-related disability was a pretext." Additionally, concerning plaintiff's allegation that the employer intruded upon his physician-patient privilege by sending a letter to his doctor, the court dismissed this "intrusion upon seclusion" cause of action because the sending of an

unsolicited letter is not obviously objectionable to a reasonable person and the employer received no response to the letter's request for information.

Examples of cases involving claims of privacy against video surveillance include: *McLain v. Boise Cascade Co.*, 271 Or. 549, 533 P.2d 343 (1975)(motion picture surveillance of a workers compensation claimant while he was outdoors exposed to public view does not violate plaintiff's right to privacy); *State of Hawaii v. Bonnell*, 856 P.2d 1265 (Haw. 1993)(year-long, warrantless video surveillance of postal employees' break room for gambling activities was illegal search under Fourth Amendment and Hawaii Constitution); *Vega-Rodriguez v. Puerto Tel. Co.*, 110 F.3d 174 (1st Cir. 1997) (employees of quasi-public telephone corporation lacked objectively reasonable expectation of privacy against disclosed, soundless video surveillance while toiling in open and undifferentiated work area); *Meche v. Wal-Mart*, 692 So.2d 544 (La. App. 3rd Cir.), *writ denied*, 693 So.2d 760 (La.), *cert. denied*, 118 S. Ct. 574 (1997) (store was not liable for invasion of privacy, where video equipment in loss prevention room was never configured so that it could receive pictures from employee restroom in whose ceiling store security had placed closed circuit television camera); *Sacramento County Deputy Sheriff's Ass'n v. County of Sacramento*, 12 I.E.R. (BNA) 723 (Cal. App. 3rd Dist. 1996)(placement of video camera in office did not violate Fourth Amendment rights where employee had no objectively reasonable expectation of privacy against being videotaped in office); *Brazinko v. Amoco Petroleum Additives Co.*, 6 F.3d 1176 (7th Cir. 1993)(no claim for invasion of privacy for video in women's locker room pointed so it would only film women entering and leaving restroom where employer installed video for legitimate reason); *Liberti v. Walt Disney World Co.*, 912 F. Supp. 1494 (M.D. Fla. 1995)(finding claim for invasion of privacy where employer did not notify female

employees of co-employee video taping women through peep hole in women's change room after employer knew of conduct but waited to catch employee in the act).

C. E-mail Monitoring

Employers face both high reward and high risk from maintaining a workplace E-mail system. The reward is obvious - a more efficient means for communicating with employees and customers. The risks are less obvious - loss of productivity and efficiency from personal use of E-mail, maintaining security of confidential information, and liability for sexual harassment through dissemination of inappropriate information. A principal risk from employers' interception, use, or disclosure of employee E-mails, however, arises from potential claims for invasion of privacy. This section discusses the scope of an employee's right to privacy and suggests techniques and proactive steps which employers may use to monitor employee activity through E-mails without unlawfully infringing upon an employee's right to privacy. The Electronic Communications Privacy Act of 1986 extended coverage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to electronic communications, including e-mail. Importantly for employers, the Act provides many loopholes for employers in accessing employee E-mails.

First, the Act narrowly defines the term "interception" so that employers rarely violate the Act when reviewing employee E-mails in the workplace. The Act defines an "interception" to mean the aural or other acquisition of the contents of any oral, wire or electronic communication, through the use of any electronic or mechanical device. *See* 18 U.S.C. § 2510(4). The interception, however, must be a "contemporaneous acquisition of the communication" to constitute a violation of the Act. *See Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

Accordingly, an “interception” takes place if an individual sends an E-mail and a third party obtains a copy of the e-mail at the time it is sent. An “interception” does not take place, however, if an individual obtains a copy of the stored E-mail from the network computer. This is true even if the transmission has not been read by its intended recipient. *See id.*, at 462 (Secret Service did not intercept private e-mails, including those not read by their intended recipients, by retrieving them from Bulletin Board Service’s computer).

In addition, the Act provides a safe haven for employers who obtain consent from one of the parties to the communication before reviewing the E-mails. Specifically, the Act states that it shall not be unlawful for a person to intercept an electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. *See* 18 U.S.C. § 2511(2)(d). Consent may be express (i.e., signed, written acknowledgment) or implied (i.e., distribution of handbook or policy on use of E-mails).

Also, the Act has a “business extension” exception for employers who intercept a wire, oral, or electronic communication in the “ordinary course of business.” Courts have interpreted this term to mean that an employer can electronically monitor any business-related communication without the employee’s knowledge or consent. Under this exception, however, an employer may not monitor communications of a purely personal nature. *See, e.g., Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992)(exemption does not apply where employer intercepted calls beyond its business necessity of determining whether employee was stealing from employer). An employer does not violate the Act if it terminates electronic monitoring once it is determined a monitored communication is purely personal. *See Watkins v. L. M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) (“a personal phone call may not be intercepted in the ordinary course of business ..., except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is

personal or not"). The courts consider a "general practice of surreptitious monitoring" more egregious "than monitoring limited to specific occasions." *See Briggs v. American Air Filter Co., Inc.*, 630 F.2d 414 (5th Cir. 1980).

The Act also contains an important exception that allows the provider of an E-mail service to monitor communications made through that service "while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or the property of the provider of that service." *See* 18 U.S.C. § 2511(2)(a)(i). It would seem this exception would allow an employer very broad authority to monitor an employee's E-mails when the employer provides the E-mail service. If the E-mails were sent through an outside E-mail service, such as America Online, the results would be different because the employer is not the service provider. Although the Act allows an entity who provides electronic mail services to access communications on his own service, it is not clear which employees may lawfully have such access. It is permissible for a systems administrator to have such access. However, if the administrator were to permit a clerical employee to monitor the same communication, an employer could face liability.

Finally, in addition to the Federal Wiretap Act, most states have enacted similar statutes. For example, the Louisiana Electronic Surveillance Act is similar to the Federal Wiretap Act. La. R.S. 15:1301 *et seq.* There are significant distinctions, however, between state and Federal law. For example, while Louisiana amended its Act to include a definition of electronic communication, it did not amend the statutory prohibition on interceptions to include electronic communications. As a result, Louisiana's Act arguably does not prohibit interception of E-mail. *See Louis v. Neisler*, 1995 WL 18804 n. 13 (La. 1995), *withdrawn and rev'd on other grounds*, 666 So.2d 1064 (La. 1996).

There have been very few cases applying the Act to claims of unlawful interception, use, or disclosure of E-mails. In one recent case, a College sued a former clerical employee, current faculty member and former faculty member, alleging violations of the Act and various state statutes arising out of compromise of security of the college's E-mail system. In considering certain facts, the Court assumed that a college employee only inadvertently glimpsed E-mail displayed on the college president's computer screen. According to the Court, however, such an inadvertent glimpse could not constitute an "interception" of E-mail within meaning of the Act because a computer screen was a medium for information rather than "electronic device" capable of being used to "intercept" E-mail within the meaning of the Act. Next, the Court assumed that the college employee engaged in unauthorized access of the E-mail in the electronic storage in college's mainframe. Again, according to the Court, such access was not an unlawful "interception" of an electronic communication within meaning of the Act because it was not contemporaneous with transmission of the communications at issue. *See Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3rd Cir. 1998).

In another case, an employer operated an electronic bulletin board system from one of its computers. The employer used the system, for among other purposes, to communicate with customers and free-lance writers by E-mail. In fact, the system allowed customers to send and receive private E-mail. In an investigation, the U.S. Secret Service executed a warrant and seized the computer which contained 162 items of unread private E-mail stored on the system. In its review, the Court held that seizure of the computer containing the E-mail, but not read by the intended recipients, was not an unlawful "intercept" under the Federal Wiretap Act. According to the Court, Congress did not intend for "intercept" to apply to "electronic communication" when the

communications are stored in "electronic storage" and not reviewed contemporaneously with their transmission. *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

Even if it does not violate the Federal Wiretapping Act, an employer still could face liability for common law tort claims for invasion of privacy in reviewing, using, or disclosing employee E-mails. Generally, there are two types of conduct that may give rise to invasion of privacy claims of which would affect employers and E-mails: 1) public disclosure of private or embarrassing facts; and 2) unreasonable intrusion into the seclusion of another.

Employers have several defenses and strategies available to them when faced with an invasion of privacy lawsuit. In a recent case considering this issue, a court has held that employees "do not" have a "reasonable expectation of privacy in E-mail communications." In that case, the employer assured its employees that all E-mail communications would remain confidential, privileged, and would not be intercepted, or used as grounds for terminating an employee. Contrary to its policy, the employer discharged an employee for inappropriate and unprofessional comments over the E-mail system. According to the Court, however, once the employee communicated the alleged unprofessional comments to a second person over an E-mail system used by the entire company, "any reasonable expectation of privacy was lost." Moreover, because the employee voluntarily communicated the information, the Court found less reason to find an intrusion into the employee's private affairs. Finally, the Court held that, even had it found a reasonable expectation of privacy, a reasonable person would not consider the employer's interception of the E-mail to be a substantial and highly offensive invasion of his privacy. *Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996). Despite this court's decision, other jurisdictions could determine that the employer's assurances could create a reasonable expectation of privacy resulting in liability for using this information.

In another case, an employee had received permission to use one of the university's computers at home. When the university began an investigation of possible fraud and misuse of resources by the employee, a supervisor requested that the employee return the computer. The employee informed the supervisor he had personal information on the computer. The supervisor immediately sent someone with the employee to retrieve the computer from his home. Ultimately, the supervisor discovered sexually-explicit files stored on the computer and circulated a memo describing the information to higher officials. The employee filed suit against the supervisor based on a variety of claims. The Court dismissed the employee's claim against the supervisor based on qualified immunity in conducting the investigation. According to the Court, the supervisor's conduct in the investigation was not unreasonable because of the background evidence of fraud and misuse by the employee, including an investigation into the employee's use of his workplace computer indicating he had used it to access sexually explicit internet sites in violation of university policy. Moreover, the supervisor limited retrieval efforts to university property, allowed the employee to retrieve the computer himself, and chose the least threatening person to accompany the employee. Accordingly, "the intrusion, in light of all the circumstances, was not excessively intrusive when balanced against the [university's] legitimate interests in thoroughly investigating the allegations of serious workplace misconduct". *Clark v. Regents of the Univ. of California*, 1997 WL 564066 (N.D. Cal. 1997).

In an administrative hearing, however, the United States Air Force Court of Criminal Appeals held that, under the Fourth Amendment of the Constitution, a military officer had an objectively reasonable expectation of privacy in certain E-mail transmissions. The military tribunal found that the E-mail transmissions, which the officer alone could retrieve through use of his assigned password, were stored in private on-line computers in messages he transmitted to

other subscribers who had individually assigned passwords. Because there was virtually no risk that his E-mail transmissions would be received by anyone other than intended recipients, the Court held the accused had a reasonable expectation of privacy in the communication. *United States v. Maxwell*, 42 M.J. 568 (U.S.A.F. Ct. Crim. App. 1995).

In this arena, the best defense to claims may be a good offense. Employers should implement policies that diminish and/or eliminate any expectation of privacy by the employees in e-mail or from audio or video surveillance. This may be done via an executed consent form or well publicized policy. A good policy should specifically inform employees that the employer can and reserves the right to monitor and disclose information from telephone calls, e-mails, and use video surveillance in the work place. For example, for an e-mail policy, the policy should note that security functions such as passwords and message delete functions do not neutralize the employer's ability to access and use information in e-mails. Such reminder should be done in writing and, if possible, through an introductory message displayed on the user's computer monitor whenever he or she logs onto the system. Access to any electronic mail transmissions should be restricted to the systems administrator and management personnel who may have a need for such access in the course of internal investigation. Moreover, it would be safer to monitor only when a specific need arises. As the extent to which an employee's computer files and electronic mail are protected by the right to privacy is a developing issue, employers are advised to seek legal counsel before conducting any investigation which may involve access to an employee's e-mail or computer files.

D. LMRA PRE-EMPTION

Claims for invasion of privacy from electronic surveillance might be preempted by the Labor Management Relations Act ("LMRA"). *In re Amoco Petroleum Additives Co.*, 964 F.2d 706

(7th Cir. 1992)(Section 301 of the LMRA preempted union employees' challenge of installation of video camera in front hallway of women's locker room. The Court noted, "privacy in the workplace ... is an ordinary subject of bargaining [and] the extent of privacy is a 'condition' of employment."). *But see Schmidt v. Ameritech Corp.*, 115 F.3d 501 (7th Cir. 1997)(Court held that claims that company used employee's, wife's, and wife's employer's residential telephone records to investigate circumstance of employee's disability leave were completely independent of collective bargaining agreement between company and employee and thus not preempted by LMRA); *Morris v. Ameritech*, 1997 WL 652345 (N.D. Ill. 1997)(Section 301 of the LMRA does not preempt a claim regarding eavesdropping on an employee's private phone calls made from his home telephone).

GENETIC MONITORING

Employers and insurers increasingly have turned to genetic testing to obtain more medical information about employees. Genetic screening and monitoring can predict whether a person is susceptible to contracting, or has developed, a particular medical problem. By using genetic screening and monitoring, employers can review genetic traits inherited by employees from their parents and genetic changes caused by environmental conditions. Primarily, employers use genetic testing to monitor harm caused by chemical exposure in the workplace and to discover employees more susceptible to disease. Some employees and unions have requested that employers conduct the testing to discover these hazards.

The Departments of Labor, Health and Human Services, Justice, and the EEOC issued a report, dated January 20, 1998, called "Genetic Information in the Workplace". The report calls for federal legislation banning the use of genetic screening or monitoring by employers.

Several states regulate genetic testing by employers. See, e.g., Conn. Gen. Stat. §§ 31-51t to 31-55aa (allowing employers to conduct "medical screenings" in certain circumstances); Fla. Stat. § 760.40 (restricting use of genetic testing in employment); Iowa Code § 729.6 (prohibiting genetic testing as condition of employment); La. Rev. Stat. §§ 23:1001-23:1004 (prohibiting discrimination against individuals with sickle-cell trait); Me. Rev. Stat. Ann. Tit. 26, § 681 (allowing "medical screening" in certain circumstances); N.J. Rev. Stat. §§ 10:5-5 and 10:5-12 (prohibiting discrimination against individuals with sickle-cell, hemoglobin C trait, thalassemia trait, Tay-Sachs trait, and cystic fibrosis trait); N.Y. Civ. Rights Law § 48 (prohibiting discrimination against individuals with sickle-cell trait, Tay-Sachs disease, or trait for Colley's anemia which would not prevent individual from performing a particular job); N.C. Gen. Stat. § 95-28.1 (prohibiting certain actions based on sickle-cell trait and hemoglobin C trait); Or. Rev. Stat. §§ 659.010-110 and 659.227 (prohibiting use of genetic screening or obtaining or seeking genetic information in employment); R.I. Gen. Laws § 28-6.7-1 to 7-4 (prohibiting genetic testing as condition of employment); Tex. Lab. Code Ann. § 21.401 (prohibiting employment discrimination based on "genetic information"); Wis. Stat. § 111.372 (restricting use of genetic testing in employment).

A number of cases have held employees have an expectation of privacy in their genetic material. Indeed, the Supreme Court has held that requiring employees to provide blood and body fluid samples triggers an employee's rights against unreasonable searches and seizures under the Fourth Amendment. *See Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 616-17, 109 S. Ct. 1402 (1989); *National Treasury employees Union v. Von Raab*, 489 U.S. 656, 665, 109 S. Ct. 1384 (1989). *But see Mayfield v. Dalton*, 901 F. Supp. 300 (D. Haw. 1994), *vacated on other grounds*, 109 F.3d 1423 (9th Cir. 1997).

Various federal statutes also may protect employees' interests in genetic information. First, Title VII of the Civil Rights Act may affect genetic testing if a genetic trait or other condition occurs more regularly in a particular race or gender. In *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F.3d 1260 (9th Cir. 1998), employees of a research facility operated by state and federal agencies brought an action against the facility and others, alleging that nonconsensual testing for sensitive medical information violated Title VII, Americans with Disabilities Act (ADA), and right to privacy guaranteed in United States and California Constitutions. The Court held that the complaint alleging that the employer administered nonconsensual post-offer employment tests for sickle cell trait and pregnancy, thus selectively invading privacy of black employees on basis of race and of female employees on basis of sex and pregnancy, stated a cause of action for violation of Title VII. However, the Court held that the complaint alleging that the employer failed to provide or to adequately describe safeguards to prevent dissemination to third parties of sensitive medical information acquired in medical testing of employees failed to state cause of action for violation of ADA provision setting forth requirements for employer's maintenance of employee medical records. According to the Court, unlike examinations conducted at any other time, a post-offer employment entrance examination need not be concerned solely with the individual's "ability to perform job-related functions", nor must it be "job-related or consistent with business necessity," 29 U.S.C. § 12112(d)(2),(4). Thus, according to the Court, the ADA imposes no restriction on the scope of post-offer entrance examinations, but only guarantees the confidentiality and the use of the information gathered. 29 U.S.C. § 12112(d)(3)(B),(C). Because the ADA does not limit the scope of such examinations to matters that are "job-related and consistent with business necessity," the Court found dismissal of the

ADA claims was proper. The Court, however, refused to dismiss the privacy claim, based on the alleged “non-consensual” aspect of the testing.

Second, the ADA could affect employers who use genetic testing to discriminate against employees and applicants with a disability. The term "disability" includes a physical or mental "impairment" limiting a major life activity, a record of such impairment, or being regarded as having such an impairment. 42 U.S.C. § 12102(2). While the issue is far from settled, the EEOC's Compliance Manual states that:

"This part of the definition of 'disability' applies to individuals who are subjected to discrimination on the basis of genetic information relating to illness, disease, or other disorders. Covered entities that discriminate against individuals on the basis of such genetic information are regarding the individuals as having impairments that substantially limit a major life activity. Those individuals, therefore, are covered by the third part of the definition of 'disability'".

EEOC Directive 915.002 (March 15, 1995).

Employers should carefully determine their need to conduct genetic screening or monitoring of their employees. If necessary, however, employers should ensure that they conduct these tests according to accepted medical practices, adequately inform employees regarding the need for the tests, and protect employee privacy regarding the results of the tests. In addition, employers should consider whether any actions, as a result of such tests, have an adverse impact on a protected class of individuals. Finally, employers should consult their state laws to determine whether employees have any additional protections regarding genetic testing or monitoring.