JOHN G. KRUCHKO * # ±
JAY R. FRIES * +
PAUL M. LUSKY *
STEVEN W. RAY + #
KATHLEEN A. TALTY *
EDWARD LEE ISLER + #
SUSAN TAHERNIA * # +
JOAN E. BOOK * ±
JASON M. BRANCIFORTE #

Admitted * MD + VA # DC ± PA

KRUCHKO & FRIES
COUNSELORS AT LAW

Suite 202
7929 Westpark Drive
McLean, Virginia 22102

Telephone: (703) 734-0554
Telecopier: (703) 734-0876

Suite 305
600 Washington Avenue
Baltimore, Maryland 21204
---
(410) 321-7310

Suite 900
601 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
---
(202) 347-6550

MONITORING YOUR EMPLOYEES: HOW MUCH CAN YOU DO AND WHAT SHOULD YOU DO WHEN YOU UNCOVER WRONGDOING?

Steven W. Ray, Esq.
Kruchko & Fries

This outline is intended to provide a general overview and is not to be construed as legal advice with respect to specific factual situations

MONITORING YOUR EMPLOYEES: HOW MUCH CAN YOU DO AND WHAT SHOULD YOU DO WHEN YOU UNCOVER WRONGDOING?

Steven W. Ray, Esq.
Kruchko & Fries
7929 Westpark Drive
Suite 202
McLean, Virginia 22102

Employers have long been involved in monitoring the workplace performance of their employees. Technological changes in the last twenty years, however, have significantly enhanced an employer's ability to engage in such monitoring. Employers are capable of monitoring an employee's telephone calls, electronic mail, computer keystrokes, time spent on the telephone, and even time spent in the restroom. These changes in technology have given rise to an increase in the tension between an employer's right to monitor employees to maintain security and employee productivity and the rights of employees to privacy, even in the workplace. This outline summarizes the relevant legal landscape and offers some suggestions to employers seeking to implement an employee monitoring program.

I. MONITORING TELEPHONE COMMUNICATIONS

A. Federal Statutory Law

Title III of the Omnibus Crime Control and Safe Street Act of 1968 (hereinafter "Title III") prohibits any person from intercepting, using or disclosing any wire, oral or electronic communication. 18 U.S.C. § 2511(1). The statute defines "wire communication" to mean any communication by the aid of wire, cable, or other like connection, 18 U.S.C. § 2510(1); "oral communication" to mean any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception, 18 U.S.C. § 2510(2); and "electronic communication" to mean any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system. 18 U.S.C. § 2510(12). "Intercept" is defined by the statute to mean "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). Such a device is "any device or apparatus which can be used to intercept a wire, oral or electronic communication."

Violation of Title III may result in serious consequences for an employer. The statute provides that any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the statute may in a civil action recover statutory damages of $100 a day for each day of violation or $10,000, and punitive damages, if appropriate. 18 U.S.C. § 2520. In addition, a person violating the statute may be subject to a criminal fine or imprisonment or both. 18 U.S.C. § 2511(1), § 2511(4).

Title III, however, contains two critical exceptions that are relevant to employers who monitor employee telephone communications. The first of these, commonly referred to as the "business extension exception," requires both that the instrument used to intercept the call be

furnished by a communications provider and that the instrument be used in the ordinary course of the employer's business. Specifically, Congress excepted from the definitions of electronic, mechanical, or other device "any telephone or telegraph instrument, equipment or facility, or any component thereof furnished to the subscriber or user by a provider of wire or electronic communications in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business." 18 U.S.C. § 2510(5)(a). Unfortunately, little legislative history exists to explain Congress' intent in enacting this exception.

The second of these exceptions is the "consent exception." Title III states that "it shall not be unlawful . . . for a person . . . 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 . . . ." 18 U.S.C. § 2511(2)(d). Therefore, the "consent exception" applies as long as just one of the parties to the communication agrees to the interception.

These two exceptions to Title III have been applied, with varying success, in a handful of cases involving employer monitoring or interception of employee telephone communications. The court's decisions in those cases, which have not been entirely consistent, have established some of the parameters that must be observed by an employer seeking to invoke the exceptions.

Where the employee was employed in a complex area involving the employer's quality control, the employer's interception of his telephone conversations were excepted from Title III, particularly where the employer had provided its employees with a separate phone for personal calls and had informed the employees of its practice of monitoring calls. See Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392 (W.D. Okla. 1978).

An employer also did not violate Title III when it listened in on an employee's telephone conversation with a competitor with whom the employee had a close friendship. The parties agreed that the call was a business, not a personal, call, and the court found that the monitoring was in the ordinary course of the employee's business in that it was limited in purpose and time and "was not part of a general practice of surreptitious monitoring." Briggs v. American Filter Co., 630 F.2d 414 (5th Cir. 1980).

Where the conversation clearly is a personal call, however, the employer will have great difficulty in showing that the monitoring of the call occurred in the ordinary course of business. In Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983), the court held that:

> [A] personal 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 the call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.

The court also rejected the employer's argument that the employee impliedly consented to the interception because she knew of the employee's monitoring policy. The court held that "[c]onsent under Title III is not to be cavalierly implied," and concluded that the employee had consented to the monitoring of her business calls, but not her personal calls.

A similar conclusion was reached recently by another federal appellate court where an employer suspected his employee of theft and monitored her calls. The employer did not find evidence that she had committed the theft in question, but discovered that she had violated another company rule by selling goods at cost to a man with whom she was having an affair. Despite the fact that the employer learned about the infraction by listening to the employee's calls, the court held that the interception was not in the ordinary course of business because it was the interception of a personal call. Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992).

The clearest conclusion to be drawn from these cases is that an employer, under Title III, is obligated to cease listening as soon as it determines that the call is personal, regardless of the contents of the conversation.

B. State Statutory Law

In addition to federal wiretapping laws, almost every state has enacted statutes addressing the interception of telephone communication. Many of these state statutes are patterned after Title III, and include both the business extension exception and the consent exception. See, e.g., Va. Code Ann. § 19.2-61 et seq. Others have sought to expand the protections afforded under Title III[1] by enacting state laws that, among other things, require the consent of all parties to the communication before the consent defense can be asserted. Some of the state statutes are criminal statutes only, and offer no express civil private right of action, although in many of those states private plaintiffs may assert a common law privacy action based on the state policy embodied in the state statute.

For example, under Florida's wiretapping statute, Fla. Stat. Ann. § 934.01 et seq., all parties to a communication must consent to its interception or disclosure in order for the consent defense to be utilized. Royal Health Care Services, Inc. v. Jefferson Pilot Life Ins. Co., 924 F.2d 215, 218 (11th Cir. 1991). California's wiretapping statute also requires the consent of all parties to the communication before an interception is excepted from the statute's proscriptions. See Cal. Penal Code § 632

Consequently, an employer engaging in the monitoring of employee telephone communications must carefully consider, in addition to Title III, the state wiretapping statutes applicable to the employer's places of business.

C. State Common Law Claims

In addition to, or perhaps in lieu of, any state statutory private cause of action that an employee might have for interception of a telephone communication, an employee may also bring a common law action against an employer for invasion of privacy. Generally, most of these common

---

1 States are permitted to expand the protections of Title III and proscribe wiretapping more restrictively, but any state purporting to legalize an action outlawed by Title III would be preempted by that statute.

law privacy actions are based on either the theory that the employer negligently or intentionally breached a duty owed to the employee that is established in the state wiretapping statute, or, more commonly, on the premise that the employer has intruded upon the "seclusion" of the employee. Establishing the latter usually requires the individual asserting the privacy claim to show that the defendant committed an intentional intrusion, which a reasonable person would find objectionable or offensive, into the plaintiff's privacy or seclusion.

For example, in Pemberton v. Bethlehem Steel Corp., 66 Md. App. 133, 502 A.2d 1101, cert. denied, 508 A.2d 488 (1986), the court considered an invasion of privacy claim asserted by a union agent who claimed that an employer who employed some of the union's members had him placed under surveillance and thus intruded into his seclusion. The court held that the "gist of the offense is the intrusion into a private place or the invasion of a seclusion that the plaintiff has thrown about his person or affairs. There is no liability for observing him in public places, 'since he is not then in seclusion.'" Even if the employer's surveillance constituted an intrusion, the court further held, the surveillance would only be actionable if the intrusion would be highly offensive to a reasonable person. Thus, it is likely that whether an employer has engaged in a common law invasion of privacy by monitoring employee telephone communications will depend largely upon the employee's ability to show that his communication took place under circumstances that a court would find to be private and in a manner that a reasonable person would consider offensive.

To show that an intrusion was into a private place, a plaintiff alleging this type of common law claim probably must show that he had a reasonable expectation of privacy in the intercepted communication. For example, in Simmons v. Southwestern Bell telephone Co., 452 F. Supp. 392 (W.D. Okl. 1978), where an employee alleged a Fourth Amendment privacy right, the court held that, even had the plaintiff shown that his employer was a state actor so as to implicate the Constitution, he could not establish a reasonable expectation of privacy since the employer had a clearly established and communicated practice of monitoring employee telephone calls for service quality checks. See also Faulkner v. Maryland, 317 Md. 441, 564 A.2d 785 (1989) (holding that employee could not have had reasonable expectation of privacy in a locker because employer had expressly reserved right to inspect lockers).

II. MONITORING EMPLOYEE ELECTRONIC MAIL AND VOICE MAIL

A. Electronic Mail (E-mail)

As networked personal computers have proliferated throughout the business environment in the last ten years, there has been a concomitant expansion in the number of employees who now access some type of electronic mail ("E-mail") system as part of their daily routine. As originally enacted, Title III applied only to wire and oral communications and thus offered no protection to E-mail messages. In 1986, however, the protections of Title III were extended to "electronic communications" by the passage of the Electronic Communications Privacy Act ("ECPA"). One of the principal purposes behind the amendment of Title III was to offer non-aural communications, including E-mail, the same protection as was accorded wire/telephone communications. To achieve this goal, "electronic communication" was broadly defined to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or

foreign commerce." 18 U.S.C. § 2510(12). The legislative history of the ECPA is clear that electronic mail ("E-mail") was intended to be covered as an electronic communication.

By including electronic communication in the same provision as wire or oral communication, however, Congress made the monitoring of electronic communications subject to the same exceptions as had been afforded interception of wire or oral communications. Thus, an employer who chooses to monitor its employee's E-mail messages for business reasons most likely would be protected under the business extension exception. For example, just as employers are permitted to monitor telephone communication to ensure that employees are not spending too much company time engaged in personal calls, see, e.g., Deal, 980 F.2d at 1158, it would appear that an employer also would have a similar business purpose in monitoring E-mail messages to ensure that employees are not spending too much time exchanging personal messages. Moreover, by advising employees of its intent to periodically monitor E-mails, employers can assert that employees have given implied consent to such monitoring.

Furthermore, the provisions of the ECPA include an additional exception that employers seeking to monitor E-mail should be able to utilize as a defense to such monitoring. Under the ECPA, the provider of electronic communications can access stored communication without running afoul of the Act. Because, in the context of the corporate environment, the employer is the system provider, the employer arguably can access and review stored E-mail messages without violating the ECPA. There appear to be no reported decisions at this time regarding an employer's right to monitor employee E-mail, but several such cases appear to be pending in California, and it is inevitable that other cases will arise in the near future. In the meantime, as long as employers can meet either the requirements that courts have developed for the business extension exception or the consent exception, or can take advantage of the stored communications exception, monitoring of employee E-mail is probably permissible if conducted in a reasonable manner (i.e., no excessive reading of personal E-mail) and if the results of the monitoring are not improperly disclosed.

B. Voice Mail

As with E-mail, in the last ten years, "voice mail" has become prevalent in the business environment, allowing callers the option of leaving a message in an employee's "voice mailbox." The proliferation of voice mail raises additional questions about an employer's right to monitor employee communications in the workplace. Although there appear to be no reported decisions involving an employer's surreptitious interception of an employee's voice mail, at least one case is pending in New York that may address whether voice mail is entitled to the same, less, or greater protection than live telephone communications under either Title III, state statutes, or state common law privacy rights. The result in that case, or in others to follow, likely will be that voice mail is afforded, at a minimum, the same protection as live conversation, and arguably greater protection.

First, although it is unclear that voice mail is covered by Title III, most courts likely will consider voice mail messages to be either wire or electronic communications. If this is the case, then an employer will have to rely upon either the business extension exception or the consent exception in Title III. Second, employees may be able to bring an action under a more restrictive state statute or under a common law right of privacy. The employee may be able to establish the

latter based on a showing of a reasonable expectation of privacy. Unlike live conversations, most voice mailboxes may be accessed only through a password or numerical code. As a result, an employee may have a greater expectation of privacy in a voice mailbox than when engaging in live conversation. Consequently, employers should exercise extreme care in accessing employee voice mailboxes.

III. SUBJECTING EMPLOYEES TO POLYGRAPH EXAMINATIONS

A relatively routine method of detecting employee theft or misappropriation would be the use of a polygraph or lie detector test, particularly in those industries, such as the communications industry, where the employee's misappropriation might not become palpable until long after the offense, if at all. Unfortunately for employers, federal and state statutes prohibit random polygraph examinations, and their use, even in furtherance of a specific investigation, must be carefully administered.

A. Federal Law

The federal Employee Polygraph Protection Act of 1988 prohibits employers from requiring employees or applicants for employment to submit to a lie detector test except in very limited circumstances. 29 U.S.C. § 2002(1). Employers also are prohibited from discriminating against, disciplining, or discharging an employee who refuses to take a polygraph. 29 U.S.C. § 2002(3). Violations of the Act can result in the imposition of civil penalties of not more than $10,000 as well as the institution of private actions for equitable relief including reinstatement, promotion, or the payment of lost wages. 29 U.S.C. § 2005.

The Polygraph Act includes several exceptions to its proscriptions, however. The most important of these to private employers is the limited exemption for "ongoing investigations." Utilization of that exemption requires the employer satisfy a number of conditions. Specifically, the employer may require an employee take a polygraph if:

- The test is administered in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage;
- The employee had access to the property that is the subject of the investigation;
- The employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation; and
- The employer executes a statement, provided to the examinee before the tests, that --
    - sets forth with particularity with specific incident or activity being investigated and the basis for testing particular employees;
    - is signed by a person (other than a polygraph

examiner) authorized to legally bind the employer;

- is retained by the employer for at least three years; and
- contains at a minimum --

  -- an identification of a specific economic loss or injury to the business of the employer;

  -- a statement indicating that the employee had an access to the property that is a subject of the investigation; and

  -- a statement describing the basis of the employer's reasonable suspicion that the employer was involved in the incident or activity under investigation.

29 U.S.C. § 2006(d). In addition, the Polygraph Act states that an employer may not take action against an employee based on the results of the polygraph unless the employer has additional supporting evidence of the employee's involvement in the alleged offense. 29 U.S.C. § 2007.

The regulations to the Polygraph Act further define ongoing investigation as requiring the investigation of a specific incident or activity. Thus, the regulations explain an employer would not be permitted to subject an employee to a polygraph in an effort to determine whether any theft has, in fact, occurred. Furthermore, the regulations prohibit the use of a polygraph where the employer generally suspects that theft is occurring because of a high-loss of inventory, unless the employer is investigating a specific loss of a specific inventory and has a reasonable suspicion that a particular employee was involved. 29 C.F.R. § 801.12(b). A "reasonable suspicion" is an observable basis in fact, such as information from a co-worker or an employee's behavior or demeanor which indicates a particular employee's involvement, and mere access or opportunity does not give rise to a reasonable suspicion. 29 C.F.R. § 801.12(f).

The impact of the Polygraph Act is the virtual elimination of the polygraph or lie detector, which is broadly defined under the Act, as a means of preliminary investigation of employee misconduct. Only after the employer has developed a reasonable suspicion and has satisfied the requirements for administering a polygraph under the Act may the employee actually be subjected to a polygraph. The employer was held to have such a reasonable suspicion in In re Scrivener Oil Co., 7 I.E.R. Cas. 962 (1992), where the subject employee was working alone when at the time that the employer developed a large cash shortage. Because the employer complied with the notice requirements of the Polygraph Act, the employee's polygraph was not actionable under the Act. The employer was less fortunate in In re Rapid Robert's Inc., 7 I.E.R. Cas. 946, where the employer failed to satisfy the Act's requirements, even though it had reasonable suspicion to suspect the employee of theft, because it did not provide the employee with sufficient advance notice of the examination.

B. State Laws

Most states also have enacted laws prohibiting employers from subjecting employees to polygraph examinations, some of which are more restrictive than the federal Polygraph Act and provide greater potential remedies to the aggrieved employee. For example, in the District of

Columbia, employers are completely prohibited from subjecting employees to polygraph examinations. D.C. Code Ann. § 36-802. No "ongoing investigation" exemption exists under that statute, and violation of the D.C. law "shall be an unwarranted invasion of privacy in the District of Columbia, and shall be compensable by damages for tortious injury." In addition to an amount of damages to be "established by the court," the employer who violates that act may also be liable for attorney's fees and guilty of a misdemeanor. D.C. Code Ann. § 36-803.

Consequently, employers should take care to satisfy the requirements of the applicable state polygraph statute as well as the federal Polygraph Act before administering a polygraph to an employee, even as part of an ongoing investigation.

IV. WORKPLACE SEARCHES AND VIDEO SURVEILLANCE

Despite the number of statutes that have been enacted, at both the federal and state level, prohibiting or restricting an employer's ability to monitor telephone or electronic communications or to subject employees to polygraphs, employers are left relatively unfettered with regard to perhaps the most intrusive forms of employee monitoring, the physical search and video surveillance of a workplace.

A. Workplace Searches

1. Office and Desk Searches

Almost all of the developments in the area of workplace searches have involved public employees who have asserted Constitutional Fourth Amendment rights against being subjected to an unreasonable search and seizure. Because the employee's manager or supervisor generally is considered to be a government actor, such protections are deemed to apply. Prior to 1987, the application of the Fourth Amendment protections in the workplace of a public employer was somewhat inconsistent as courts wrestled with the extent to which a public employee may have a reasonable expectation of privacy in various aspect of the employee's work environment, such as the employee's desk, locker, and even briefcase.

The United States Supreme Court finally considered the issue in O'Connor v. Ortega, 107 S. Ct. 1492 (1987). The Court stated, first, that the workplace includes hallways, cafeteria, offices, desks, and file cabinets, even if an employee places personal items in those places. The Court also noted that "[n]ot everything that passes through the confines of a business address can be considered part of the workplace context, however." Specifically, the Court found that public employees may maintain their expectation of privacy in some items, such as suitcases or purses, even where they are brought into the workplace. The Court thus rejected the argument of the Solicitor General that a public employee can never have a reasonable expectation of privacy in the workplace, finding instead that each employee's expectation of privacy must be assessed in the context of the employment relationship.

> Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be

> reduced by virtue of actual office practices and procedures, or by legitimate regulation.

Emphasis added under the facts of that case, the Court held that an employee who had been subjected to his employer's search had a reasonable expectation of privacy in his desk and file cabinet, because he had maintained the same office for 17 years and did not share it with anyone. The Court then held that whether the employer had violated this expectation of privacy where its search was motivated by investigation of work related misconduct depended upon the reasonableness of the search. The case was remanded to the lower courts for this determination.

Although the O'Connor decision does not have direct application for private employers, its holding undoubtedly will provide guidance to courts that are faced in the future with determining the extent to which private employers may engage in workplace searches. See, e.g., Okura & Co. v. Careau Group, 783 F. Supp. 482, 505-06 (C.D. Cal. 1991)(court rejected invasion of privacy claims filed by corporate board members because it found, citing O'Connor, that the board members did not have a reasonable expectation of privacy in their offices vis-à-vis the CEO of the corporation who conducted the office searches).

Even though Fourth Amendment protections do not extend to private employees as regards their private employers, courts can also be expected to apply the Fourth Amendment analysis to searches by private employers. Employers thus can best protect themselves by communicating to employees the employer's right to conduct reasonable workplace searches of desks and file cabinets, thus reducing the employees' expectation of privacy in those areas. In addition, employers can reduce their exposure to invasion of privacy claims by limiting their searches to occasions where they have a reasonable suspicion of employee wrongdoing. See, e.g., Faulkner v. Maryland, 317 Md. 441, 564 A.2d 785 (1989) (private employer's search of employee's locker with police attending, even if constituting state action, was reasonable in light of employer's well founded belief that drugs and alcohol were being stored in employee lockers and in light of the employer's express reservation of the right to search employee lockers).

2. Physical Searches

Physical searches of an employee's person are almost unheard of in the context of private employers, but it is clear that any such search likely would constitute an invasion of privacy. In Bodewig v. K-Mart, Inc., 54 Ore. App. 480, 635 P.2d 657 (1981), a female employee accused by a female customer of stealing $20 was required to enter a dressing room and, in the presence of a female supervisor and the customer, disrobe down to her underwear. The Court held that the employee stated tort claims for outrageous conduct and infliction of emotional distress arising out of the search.

B. Video Surveillance

There have been surprisingly few reported decisions on the issue of whether an employer's video surveillance constitutes an invasion of employee privacy. In one case, Marrs v. Marriott Corp., 830 F. Supp. 274 (D. Md. 1992), a security supervisor who suspected that someone was looking through the locked drawers of his desk received permission from the employer to install a

hidden video camera in the office. The video camera taped a night security guard picking the desk drawer with a paper clip. After the guard was terminated, he sued, claiming, among other things, that the hidden videotaping was an intrusion upon his seclusion and thus an invasion of his privacy. Not unexpectedly, the court held that the employee had no reasonable expectation of privacy in an open office that all of the security guards could access.

A similar result was reached on slightly different grounds In Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 4 I.E.R. Cas. 1107 (Mich. Ct. App. 1989). There, an employee was injured after suffering a fall in his workplace. When the employee claimed a work-related disability, his employer hired a private investigative firm to determine whether and to what extent the employee was really injured. The investigative firm observed the employee in public, unbeknownst to the employee, and through the open windows of the employee's home, using both the naked eye and a powerful camera lens. The employee, when he learned of the surveillance, asserted a claim for invasion of privacy. The court held, first, that observation of the employee through an open window with the naked eye would not be considered as intrusive, but that whether the use of the camera lens was intrusive was a jury question. The court then concluded, however, that it was irrelevant whether the use of the lens was intrusive because the intrusion was not into matters that the plaintiff had a right to keep private, given the employer's interest in ensuring that the employee was not engaging in fraud by claiming disability.

Employers may engage in videotaping of the workplace because the employee does not have a reasonable expectation of privacy there, particularly if the employer discloses the presence of the cameras, and because the events that take place in the work environment are of legitimate interest to the employer. Of course, the employer should exercise good judgment and refrain from placing video cameras in places such as employee restrooms where a court almost certainly would conclude that the employees have a reasonable expectation of privacy.

V. PROPOSED LEGISLATION

In the last Congress, Senator Paul Simon (D-Ill.) proposed new legislation, entitled the Privacy for Consumer and Workers Act ("PCWA"), which would require that all electronic monitoring by employers be relevant to the employee's work performance and that employees, customers and the public be given notice of such monitoring.

Under the PCWA, as proposed, the term "electronic monitoring" would mean the "collection, storage, analysis or reporting of information concerning an employee's activities by means of a computer, electronic observation and supervision, telephone service observation, telephone call accounting, or other form of visual, auditory, or computer based technology which is conducted by any method other than direct observation by another person including the following methods: transfer of signs, signals, writing, images, sounds, data, or intelligence of nay nature which are transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system." The bill would permit an employee to have access to data collected about the employee's work performance and would limit disclosure and use of such data by the employer.

Although the bill would permit electronic monitoring, no employer would be permitted to

engage in such monitoring in bathrooms, locker rooms or dressing rooms, unless the employer has a reasonable suspicion that an employee is engaged in conduct which violates civil or criminal law. Moreover, lawful electronic monitoring would be restricted to a periodic or random basis and could only be done under the following conditions: (1) for new employees, random or periodic monitoring could occur for up to 60 days; (2) for employees with more than 60 days of tenure but less than 5 years, periodic or random monitoring would be limited to not more than two hours in any week and employees must be given notice of the monitoring at least 24 hours but not more than 72 hours before the monitoring begins; and (3) for employees with more than 5 years tenure, no electronic monitoring would be permitted unless the employer has a reasonable suspicion that the employee is engaged in conduct which violates criminal or civil law or constitutes willful gross misconduct, and this misconduct would adversely affect the employer's interest or the interest of such employer's employees.

An employer who engages in electronic monitoring would be required to post a notice from the Secretary of Labor which would inform employees about their rights under the PCWA. In addition, the employer would be required to provide each employee who would be electronically monitored with prior written notice about the monitoring. The employer's written notice would contain two parts, one part outlining the nature, scope and use of the monitoring[2] and the other part explaining where the employer is not required to give prior notice about monitoring.[3]

In addition, employers would be required to provide general notice about electronic monitoring to prospective employees and to give written notice to any prospective employee to whom an employment offer is made. Customers and the public would also be entitled to notification of electronic monitoring if the activity would encompass customers or members of the public.

The PCWA failed to make it out of Senate Labor Committee in the last Congress, although the Committee did take several days of testimony regarding the legislation. A representative from Senator Simon's office stated that reintroduction of the bill in the new Republican-controlled Congress is presently under consideration and, as of February 1995, no decision had been made regarding the bill's future. Because of the impact that legislation such as the PCWA would have on employer monitoring of employees, and because much of the testimony previously taken by the Committee was from representatives of employee interest or individual rights groups, such as the

---

2 The notice must include the following: (1) the form of electronic monitoring to be used; (2) the personal data to be collected; (3) the hours and days per week that electronic monitoring will occur; (4) the use to be made of personal data collected; (5) interpretation of printouts of statistics or other records of information collected through electronic monitoring if the interpretation affects the employees; (6) existing production standards and work performance expectations; and (7) methods for determining production standards and work performance expectations based on electronic monitoring statistics if the methods affect the employees.

3 The exception to notice requirement applies where an employer has a reasonable suspicion that the employee is engaged in conduct which (1) violates criminal or civil law or constitutes willful gross misconduct, and (2) adversely affects the employer's interest or the interest of such employer's employees.

Communications Workers of America and the ACLU (although some employers, such as MCI, also were represented), employers, particularly those in the communications industry, should carefully monitor such legislation in the future.

VI. GUIDELINES FOR MONITORING EMPLOYEES

Employers should establish some guidelines for employee monitoring and have such guidelines reviewed by counsel to ensure compliance with relevant federal and state laws. Because the law may differ slightly from state to state, it is difficult, if not impossible, to draft a uniform policy, but the following are some guidelines that employers should consider in implementing employee monitoring.

A. Determine the Monitoring Necessary for Protection of Business Interests

In many respects, whether defending against a statutory wiretapping claim or a breach of privacy allegation, the linchpin of an employer's defense is its ability to show that the employee monitoring was related to and justified by business necessity. Employers therefore should consider the nature of their business and outline those areas where employee monitoring would be justified. For example, an employer that utilizes telemarketing or consumer service personnel may need to monitor calls to ensure that appropriate customer relations are being observed.

Employers who have reasonable cause to suspect that illegal activities are taking place on the premises may also institute monitoring to eradicate any such activities in the interest of the business. If the illegal activity is an offense against the employer, such as theft or misappropriation of company property, then obviously business interests are implicated. Even if the activity is not against the employer directly, for example, the selling of illegal drugs in the employee locker room, then the employer may engage in reasonable monitoring because it is within an employer's business interests to ensure that crimes are not being perpetrated on the employer's property.

B. Consider the Impact of Applicable Laws

As noted above, state laws differ as to those activities that are considered permissible. For example, some states prohibit polygraph examinations of employees and some state constitutions specifically offer protection of privacy interests and may thus more easily give rise to a common law invasion of privacy claim. Consequently, employers should determine which state law governs their employees and design their employee monitoring system in accordance with that law. For employers with operations in different states, this may require the employer to maintain monitoring techniques that differ depending on the location of the facility where the employees are employed.

C. Communicate the Monitoring Policy to Employees

In addition to establishing the business necessity of monitoring, employers can best protect themselves from wiretapping or invasion of privacy claims by obtaining employee consent to monitoring, even if that consent is simply implied from the fact that the employer made its monitoring practices well known to its employees. Some employers may hesitate to communicate its intent to monitor on the basis that monitoring creates low employee morale and causes friction between employees and management. Although this will always be true to some extent, employers can limit the negative impact of employee monitoring by being straightforward with employees and by explaining that such monitoring is for the protection of the employee as well as the employer. In the end, employers should not sacrifice the need to obtain implied employee consent out of fear that communication of the monitoring policy will damage employer-employee relations.

An employer can communicate its monitoring policy in a number of ways:

- *Employee handbook or manual*. Notify the employees in the handbook that the employer engages in monitoring for business reasons, explain the nature of the monitoring, and state that the employee is presumed to have knowledge that his telephone conversations, E-mail, etc. may be monitored.

- *Other written communication.* Interoffice memoranda or handouts to employees can reiterate the policy contained in the handbook, and annual distribution of such handouts will negate the claim of the employee who asserts that he has not read the employee manual since he commenced employment and that the policy was not in the manual at that time.

- *Posting.* Post the monitoring policy on employee bulletin boards or in employee lounge areas.

- *Signed agreements.* Employers may want to include a communication about employee monitoring in other agreements that the employee is required to sign, such as a confidentiality agreement or a non-compete agreement. The employee's signature will provide the employer with express consent to monitor, provided the monitoring that takes place comports with the monitoring described in the agreement.

- *Employee meetings.* In order to defuse employee anxiety about monitoring and to communicate the policy, the employer may hold meetings with employees where the monitoring is explained and where employees can ask questions. Recording attendance at such meetings is advisable in the event that the employer later seeks to assert the employee's presence at the meeting as evidencing implied consent.

D. Establish Reasonable Limits on Monitoring

An employer's monitoring policy and practices should be tailored to protect its business interests, and should not be overbroad either in design or in implementation. Courts have tended to view unlimited or unfettered monitoring practices with disfavor. Thus, for example,

employers generally should not monitor "personal" communications or undertake overly intrusive surveillance measures, such as the placement of video cameras in restrooms or by the entrances to restrooms, in locker rooms, or in employee lounges.

E. Train Managers and Supervisors to Observe Acceptable Limits

In addition to designing reasonable limits on monitoring, employers should take measures to ensure that the limits are honored by the managers or supervisors with access to the information gathered in the monitoring. If an employee learns that a manager entertained himself by reading the employee's E-mail, the employer may face an unnecessary invasion of privacy claim.

F. Maintain Procedures for Use and Disclosure of Monitoring Results

Employers should also design and implement the means by which the results of employee monitoring will be used and disclosed. For example, if the employer randomly tapes telephone conversations between employees and customers, the employer should have procedures in place that specify the individual responsible for screening those tapes, the secure location where the tapes will be maintained, and the period for which the tapes will be stored before being erased.

VII. ACTIONS UPON DISCOVERING WRONGDOING

One of an employer's worst nightmares is to discover that an employee has been engaging in theft, embezzlement, fraud, or some other offense against the company. Unfortunately, such events do occur, and an employer must be prepared to respond when an employee offense is uncovered. Appropriate employer response is important not only so that the employee may be prosecuted for his actions, but also so that the employer may determine, to the greatest degree possible, the full nature and extent of the damage caused to the company by the employee's actions. Although every situation will necessarily vary according to its facts, the following is a suggested checklist of steps the employer should consider taking when it first receives notice of possible wrongdoing by an employee.

A. Act Quickly But Prudently.

Obviously if a crime is being committed against the employer, a rapid response is necessary. Failure to act may result in further harm to the company or in the loss of valuable evidence that is needed to prove the wrongdoing. At the same time, however, employers must balance the need to act quickly with prudence. An employer that acts imprudently or rashly may find that it has taken action against an innocent employee and perhaps has exposed itself to numerous claims by the accused employee, including claims for defamation and intentional infliction of emotional distress. The employee also likely will be sued for discrimination if the employee is a member of a protected class. Employers thus must balance speed with prudence.

B. Notify In-house Counsel and/or Outside Legal Counsel

The legal ramifications of employee malfeasance are significant, both for the employer and the

employee. Counsel should be contacted immediately when criminal activity is suspected.

C. Confirm, to the Extent Possible, the Misconduct

Employers will serve themselves well by taking the necessary time to gather sufficient facts and to preserve evidence before acting against an employee. What may seem to be an egregious criminal offense at first glance may turn out to nothing more than a slight infraction of company policies. Confirmation of the misconduct is also important because the employer will need to produce evidence of the wrongdoing if, in fact, criminal misconduct is involved. Gathering and preserving evidence is critical in the early stages of an investigation.

D. Keep Information on a "Need-to-Know" Basis

The investigation and confirmation of the wrongdoing should be conducted using a minimal number of personnel. If employees learn that an investigation is underway, the employer may be further damaged in a couple of respects. First, the employee who is suspected of engaging in the wrongdoing may get wind of the investigation and destroy valuable or necessary evidence of the wrongdoing. As a result the employer may be unable to prove the crime occurred, or may be unable to assess the severity of the criminal activity. Second, by allowing word of an investigation to seep out, the employer may subject itself to a defamation claim when the other employees learn that a co-worker is being investigated, especially if it turns out that he is innocent of any activity rising to the level of criminal conduct. Employers thus should take precautions to maintain the confidentiality of the investigation.

E. Apply Company Policies in a Consistent and Nondiscriminatory Manner

Before acting on an employee's misconduct, be sure that the company is applying its policies in a manner that is consistent with past practice. For example, if an employee has been caught giving a family member access to free long distance service, an action that unquestionably both violates company policy and the law, the employer must also consider how it has treated previous violators, if any have existed. If the accused employee is a member of a protected class (minority, disabled, older worker, etc.), and is treated more harshly than others in the past, the employer likely has exposed itself to civil liability, even if the employee actually engaged in the misconduct. If, for example, a company has a well established history of merely reprimanding white males who are caught giving family members access to long distance service, and then discharges a black employee who has engaged in the same conduct, the employer will not fare particularly well in the ensuing discrimination action. Employers should apply company policy and practice consistently.

F. Depending on the Offense, Contact Law Enforcement Authorities

For obvious reasons, as soon as evidence of criminal activity is confirmed, law enforcement authorities should contacted.

G. Confront the Employee

Before the employee is summarily terminated and charged with criminal offenses, the employer should (perhaps in the presence of law enforcement officials or in-house security personnel, depending once again on the seriousness of the conduct) confront the employee. At least two witnesses should be present. This will provide the employee with an opportunity to explain the misconduct and present a defense of his actions. If it later turns out that the employee is not guilty of the alleged misconduct, and if the employer failed to give the employee some semblance of due process, an employer might have difficulty presenting its defense in the ensuing civil action for wrongful discharge. For this same reason, confrontation of the employee should take place away from the employee's regular worksite so that the employee, should the charges prove to be false, will not be unduly humiliated in front of co-workers. Such humiliation will undoubtedly give rise to claims for defamation and intentional infliction of emotional distress.