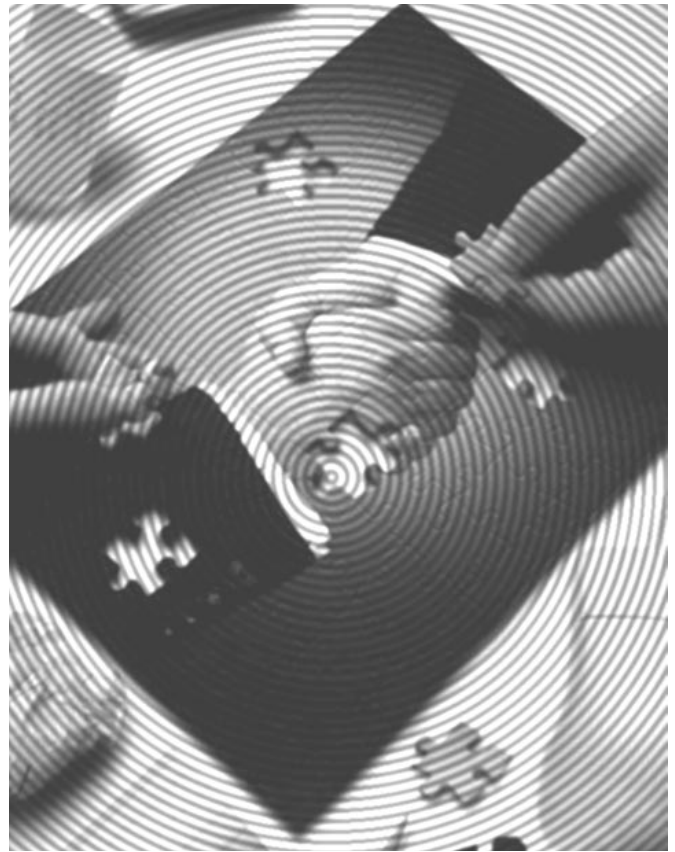


Workplace Privacy: Balancing Employer- Employee Rights and Obligations in the New Millennium (Part II)

by Mark A. Fahleson

*Editorial Note: This is the concluding section
of Mr. Fahleson's article appearing in the
March, 2002 issue of "The Nebraska Lawyer."*



"Lie Detector"

Monitoring and Investigating Employee Conduct

Polygraphs

Employee Polygraph Protection Act of 1988

Signed into law by President Ronald Reagan in June 1988, the federal Employee Polygraph Protection Act ("EPPA"), 29 U.S.C. §§ 200-209, severely limits an employer's ability to lawfully use "lie detectors." While the EPPA does contain exemptions for public employers, certain private employers and for ongoing investigations, the EPPA's onerous requirements have all but ended the use of lie detector examinations in employment.

Coverage

The EPPA covers "employer[s] engaged in or affecting commerce or in the production of good for commerce."⁴² The term "employer" is broadly defined to include "any person acting directly or indirectly in the interest of an employer in relation to an employee or prospective employee."⁴³ "Commerce" is broadly defined as well, having the same meaning as it does for purposes of the Fair Labor Standards Act of 1938, i.e., "trade, commerce, transportation, transmission, or communication among the several States or between any State and any place outside thereof."⁴⁴

Mark A. Fahleson is a partner with Rembolt Ludtke & Berger LLP in Lincoln, Nebraska, where he practices management-side workplace law. He currently serves on the Executive Committee of the Labor Relations and Employment Law Section of the Nebraska State Bar Association.

This article is adapted from a presentation made by the author at the 101st annual meeting of the Nebraska State Bar Association in October 2001.

The EPPA restricts the use of "lie detectors," which is broadly defined to include "a polygraph, deceptograph, voice stress analyzer, psychological stress evaluator, or any other similar device . . . that is used, or the results of which are used, for the purpose of rendering a diagnostic opinion regarding the honesty or dishonesty of an individual."⁴⁵

Prohibitions

Among other things, the EPPA prohibits employers from:

- directly or indirectly, requiring, requesting, suggesting or causing any employee or prospective employee to take or submit to any lie detector test;
- using, accepting, referring to, or inquiring concerning the results of any lie detector test of any employee or prospective employee;
- discharging, disciplining, discriminating against, or denying employment or promotion to, or threatening to take any such actions against any employee or prospective employee:
 - who refuses, declines, or fails to take or submit to any lie detector test;
 - on the basis of the results of any lie detector test; or
 - because she filed any complaint or instituted any proceeding under or related to the EPPA, has or will testify in such a proceeding, or has exercised any right protected by the EPPA.

Exemptions

The EPPA exempts from its coverage public employers, national defense and security contractors, FBI contractors, security guard firms, and drug manufacturers and distributors.⁴⁶

The EPPA also contains a limited exemption for employers engaged in an ongoing investigation involving economic loss or injury to the employer's business.⁴⁷ The loss must be to the employer, not to its employees or some third-party.⁴⁸

The "ongoing investigation" exemption is only available if:

- the employee being subject to the lie detector test 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.
- "Reasonable suspicion" has been liberally construed to include such things as an employee's expressed intention to quit⁴⁹; and
- the employer executes a statement, provided to the employee before the lie detector test, that:
 - sets forth the incident/activity being investigated and the basis for testing the employee;
 - is signed by a person (other than polygraph examiner) that can legally bind the employer;
 - is retained by the employer for at least 3 years;
 - and contains, at a minimum:
 - identification of the specific economic loss/injury to the employer;
 - a statement indicating that the employee had access to the property that is the subject of the investigation; and
 - a statement describing the employer's reasonable suspicion that the employee was involved.

Examinee Rights

The exemptions set forth above do not apply unless an examinee is provided with certain rights with respect to the test. Specifically:

- All Phases of Test: Throughout all phases of the lie detector test:
- the examinee shall be permitted to terminate the test at any time;
- the examinee cannot be asked questions in a manner designed to degrade, or needlessly intrude on, the examinee;
- the examinee cannot be asked any question concerning:
 - religious beliefs or affiliations;
 - beliefs or opinions regarding racial matters;
 - political beliefs or affiliations;
 - any matter relating to sexual behavior; or beliefs, affiliations, opinions, or lawful activities regarding unions or labor organizations; and

The term "employer" is broadly defined to include "any person acting directly or indirectly in the interest of an employer in relation to an employee or prospective employee."

- the examiner cannot conduct the test if there is sufficient written evidence by a physician that the examinee is suffering from a medical or psychological condition or undergoing treatment that might cause abnormal responses during the actual testing phase.
- The examiner must:
 - have a valid and current license granted by licensing and regulatory authorities in the state in which the test is to be conducted, if so required by the state;
 - maintain a minimum of a \$50,000 bond or an equivalent amount of professional liability coverage;



- maintain all opinions, reports, charts, written questions, lists, and other records relating to the test for three (3) years after the test; and
- not conduct and complete more than five (5) polygraph tests on a calendar day on which the test is given, and shall not conduct any such test for less than a 90-minute duration.
- Pretest phase: During the pretest phase, the prospective examinee must:
- be provided with reasonable written notice of the date, time, and location of the test, and of her right to obtain and consult with legal counsel or an employee representative before each phase of the test;
- be informed in writing of the nature and characteristics of the tests and of the instruments involved;
- be informed, in writing:
 - contains a two-way mirror, a camera, or any other device through which the test can be observed;
 - whether any other device, including any device for recording or monitoring the test, will be used;
 - that the employer or the examinee may (with mutual knowledge) make a recording of the test.
- read and sign a written notice informing the examinee:
 - that the examinee cannot be required to take the test as a condition of employment;
 - that any statement made during the test may constitute additional supporting evidence for the purposes of an adverse employment action;
 - of the limitations imposed by this provision of the EPPA; of the legal rights and remedies available to the examinee if the polygraph test is not conducted in accordance with the EPPA;
 - of the legal rights and remedies of the employer under the EPPA; and

- be provided an opportunity to review all questions to be asked during the test and be informed of the right to terminate the test at any time.
- Actual testing phase: During the actual testing phase, the examiner cannot ask the examinee any question that was not presented to the examinee in writing for review prior to the test.
- Post-test phase: Before taking any adverse employment action, the employer shall: further interview the examinee on the basis of the results of the test; and provide the examinee with: a written copy of any opinion or conclusion rendered as a result of the test; and a copy of the questions asked during the test along with the corresponding charted responses.



Nebraska Licensing of Truth and Deception Examiners Act

Adopted in 1980 before the adoption of the federal EPPA, the Licensing of Truth and Deception Examiners Act, NEB. REV. STAT. §§81-1901 to - 1936, sought to restrict, but not prohibit, use of truth and deception examinations in employment. Specifically, the Nebraska Act bars most employers from: (a) requiring employees or prospective employees to submit to a truth and deception examination as a condition of employment; or (b) using the results of a truth and deception examination as the basis for an employment decision.⁵⁰ Exempted from this prohibition is employment involving public law enforcement. However, the Nebraska Act permits

employers to use such examinations provided:

- the applicant/employee is not preselected for the examination in a discriminatory manner;
- the applicant/employee is given written and oral notice that the examination is voluntary and may be discontinued at any time;
- the applicant/employee signs a form acknowledging that the examination is being taken voluntarily;
- the employer asks the applicant/employee only job-related questions and does not ask any questions regarding the applicant's sexual practices; labor union, political or religious affiliations, or marital relationships;
- if the examination is of a current employee, the examination is being conducted with respect to a specific investigation;
- if the employee is terminated, the results of the test are not the sole determinant⁵¹; and
- the employer keeps a record of all of the questions asked and the responses for one (1) year.

Violations of the Nebraska Act by an employer or prospective employer constitute Class II misdemeanors. Violations of the Nebraska Act may also provide a source of public policy that may serve as the basis for a claim of wrongful termination.⁵²

Presumably, the Nebraska Act is preempted by the federal EPPA to the extent the Nebraska Act provides less protection to employees than does its Nebraska counterpart.⁵³

Constitutional Protections

Use of polygraphs in employment may violate the constitutional right to privacy.⁵⁴ However, where polygraph results will not be used in a criminal proceeding, public employees have no Fifth Amendment protections.⁵⁵

Civil Rights

Employers that use polygraphs in a discriminatory fashion may run afoul of federal and state civil rights statutes. For example, actionable discrimination may exist where an employer hires a white applicant over a black applicant, despite the fact that both failed an employer-administered polygraph.⁵⁶

Common Law

Use of polygraphs in employment may also give rise to a variety of common law claims, including claims of intentional/negligent infliction of emotional distress⁵⁷, invasion of privacy⁵⁸, and wrongful termination/public policy exception to employment at will.⁵⁹

Telephone Monitoring

Federal Wiretapping Act

Generally

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§2510-2520, ("Wiretapping Act") prohibits the intentional interception of a wire or electronic communications or the intentional disclosure of the contents of the interception. Specifically, the Wiretapping Act, among other things:

- Imposes criminal liability on any person who, without judicial authorization intentionally intercepts, endeavors to intercept, or procures another person to intercept any wire, oral or electronic communication.⁶⁰ "A telephone conversation is a wire conversation."⁶¹
- Creates a civil cause of action entitling any person "whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the Wiretapping Act]" to "recover from the person or entity which engaged in that violation such relief as may be appropriate."⁶² Appropriate relief for violations of the Wiretapping Act can include actual damages, punitive damages, attorneys' fees and costs. Where no actual damages exist, a plaintiff can recover liquidated statutory damages of \$100 for each violation or \$10,000, whichever

is greater.⁶³

- Sets forth specific exemptions, including:
 - Consent Exemption: A violation of the Wiretapping Act does not occur where one of the parties to the communication has given prior consent to the interception. However, this consent exemption does not apply where the communication is intercepted for the purpose of committing a criminal or tortious act in violation of the U.S. Constitution or any federal or state law. Generally, a party's consent can be express or implied.⁶⁴ However, mere knowledge of the capability to monitor alone cannot be considered implied consent.⁶⁵
 - Business Extension Exemption: The Wiretapping Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."⁶⁶ The Act expressly exempts from its definition of "electronic, mechanical, or other device" certain types of equipment furnished and used in the ordinary course of business. Specifically, this exemption covers "any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of business."⁶⁷ This exemption contains two essential elements: (a) either the telephone company or the subscriber furnished the intercepting telephone or telegraph instrument, equipment, facility or component; and (b) the equipment was used in the ordinary course of business.
- May or may not cover listening to stored voicemail messages.⁶⁸

Representative Cases



- *Arias v. Mutual Cen. Alarm Servs.*, 202 F.3d 553 (2nd Cir. 2000). Defendant employer operated central station alarm service that monitored burglar and fire alarms for its customers and notified police and fire/rescue departments when alarms were activated. The defendant installed and maintained Dictaphone telephone recording system that was attached in the telephone company's junction box. The system recorded all incoming and outgoing calls. The plaintiffs — employees of the defendant — had no actual knowledge of and did not consent to the recording. On one occasion, employees complained that they heard "beeps" during their telephone conversations and were told by the defendant's chairman that their telephone conversations were not being recorded, despite the fact they were. After the plaintiffs learned the defendant continually recorded its employees' telephone conversations at work, they brought a claim under the Wiretapping Act. On appeal, the court affirmed the trial court's granting of judgment in favor of the defendant, rejecting the plaintiff's claim that "the surreptitious, 24-hour recording of all telephone conversations, regardless of the personal, private and privileged nature of some of the conversations, is not in the ordinary course of business."⁶⁹ Because such recording was standard practice in the central station alarm industry and was recommended or mandated by various regulatory bodies, it was in the "ordinary course of its business" and, thus, the business extension exception applied.
- *Desilets v. Wal-Mart Stores, Inc.*, 171 F.3d 711 (1st Cir. 1999). Store management secretly recorded conversations of night-shift employees on voice-activated tape recorders. Plaintiffs were awarded liquidated damages, attorneys' fees and costs. On appeal, court awarded plaintiff's liquidated damages based on number of days on which violations occurred, rather than number of violations.

- *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992). Defendants owned and operated a liquor store in Arkansas, which was adjacent to their trailer home. The store and the trailer home shared the same telephone line. The plaintiff was an employee and was suspected of being involved in a burglary of the store. In response, the defendants purchased a recording device from Radio Shack and

Employer monitoring of employee telephone calls can give rise to a number of common law claims, the most common of which is invasion of privacy.

installed it on the phone in the trailer house. The recorder would automatically record all conversations with no indication to the parties that the call was being taped. Over nearly 2 months, the defendants taped 22 hours of calls, on which the plaintiff, among other things, engaged in "sexually provocative" conversations with a man with whom she participated in a "partner-swapping arrangement" and was having an extramarital affair with. The plaintiff also revealed that she had sold her paramour a keg of beer at cost, a violation of liquor store policy for which the plaintiff was fired. The court rejected the defendants' use of the consent and business extension exemptions. First, the court held that although actual consent may be implied, the defendants did not inform the plaintiff that they would be monitoring her calls and set up the recording system so that participants could not tell that their call was being recorded. Second, the court held that the business extension exemption was unavailable because the intercepting equipment *i.e.*, the recording device as opposed to the telephone itself, was not provided by a telephone company. Moreover, the interception was not in the ordinary course of business because the defendants "recorded twenty-two hours of calls, and . . . listened to all

of them without regard to their relation to [the defendants'] business interests."⁷⁰

- *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983). Plaintiff was a sales representative; much of plaintiff's work was done by telephone. The employer had an established, published policy informing employees that solicitation calls are monitored to review and improve sales techniques. Employees were permitted to make personal telephone calls on company phones and were told that personal calls would not be monitored except to the extent to determine whether a particular call was of a business or personal nature. During her lunch hour, plaintiff received a telephone call in her office from a friend, during which the plaintiff revealed that she was interviewing with another employer, such call being monitored by her employer. The plaintiff was subsequently summoned to a meeting with her supervisor, where she was questioned about her job interview. The court reversed summary judgment for the employer. The consent exemption, which does not turn on the business nature of the call, did not apply because the plaintiff did not consent to a policy of general monitoring. The business extension, which applies without regard to the consent of either party, did not apply once the employer learned it was a personal, not a business, call. At that point the employer was obligated to cease its monitoring. Simply put, "a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents."⁷¹

Common Law

Employer monitoring of employee telephone calls can give rise to a number of common law claims, the most common of which is invasion of privacy.

Invasion of Privacy

Cases

Cases from other jurisdictions construing the right to privacy as it applies to the

monitoring of telephone conversations include the following:

- *Amati v. City of Woodstock*, 829 F.Supp. 998 (N.D. Ill. 1993). The City's police department maintained a telephone system that automatically recorded all telephone conversations on every line but one, which was reserved for private use. This policy was communicated to police department employees. However, at some point the police chief requested and received permission from the City manager to surreptitiously wiretap the "private" line. This wiretap remained in place for over a year, until discovered by the employees. The Plaintiff police department employees brought suit against the City and police chief alleging, among other things, tortious invasion of privacy based upon the City's intrusion upon their seclusion. The district court rejected the Defendants' motion to dismiss, holding that "[t]he placing of a recording device in an area where one has a reasonable expectation of privacy is both intrusive and disruptive. In plain language, it ruins the privacy."⁷²
- *Jackson v. Nationwide Credit, Inc.*, 426 S.E.2d 630 (Ct. App. Ga. 1992). The plaintiffs were employed by defendant Nationwide to collect delinquent student loans. After the plaintiffs separated from employment with Nationwide, some voluntarily and some involuntarily, Nationwide filed suit against the plaintiffs seeking to enjoin their use of Nationwide's trade secrets and to enforce a noncompetition covenant. The plaintiffs filed, among other things, a counterclaim for invasion of privacy arising out of Nationwide's monitoring of their telephone conversations at work. The court affirmed the trial court's granting of summary judgment to Nationwide on this claim.

Specifically, the appellate court held that it could not "that it is an unreasonable intrusion into [plaintiffs'] seclusion, solitude or private affairs for Nationwide to monitor its telephones as it routinely did. All employees were advised that the telephones were for business only and that the telephones would be monitored. Therefore, using a speaker telephone to monitor [plaintiffs'] telephone calls while at work, in the context of this case, does not constitute an unreasonable intrusion into their private affairs."⁷³

- *Oliver v. Pacific N.W. Bell Tele. Co.*, 632 P.2d 1295 (Or. App. 1981). Plaintiff was employed by codefendant North Pacific Lumber Company as a lumber trader. After separating from his employment with North Pacific, North Pacific filed suit seeking to enforce a noncompetition agreement against plaintiff. The court refused to enforce the covenant, in part because North Pacific had unclean hands in that it had improperly monitored employee telephone calls. Plaintiff subsequently filed suit against North Pacific for, among other things, invasion of privacy. On appeal, the court recognized an

invasion of privacy claim for improper interception and monitoring of employee telephone conversations. However, because the plaintiff had no evidence that his calls were actually monitored but, rather, only produced evidence that the calls of other employees had been monitored, North Pacific was entitled to summary judgment.

- *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973). The plaintiff discovered that a telephone company employee had attached a wire tap to his telephone that transmitted the plaintiff's telephone conversations over a standard FM radio. After the wiretap was discovered and removed, the telephone company employee reattached the wire tap. The plaintiff complained to the telephone company and the employee was terminated. Plaintiff successfully brought an invasion of privacy action against the telephone company employee.

Computer Monitoring

Employer monitoring of employee use of computers and e-mail is a relatively new development, in part because over the past twenty years computer use has leapt



in status from luxury to necessity. Many companies today heavily rely upon computers in nearly every aspect of business. It is commonplace to roam the halls of business and professional offices all over the world and find most employees hovered behind computer monitors.

What most of the hovering employees do not realize is that each strike of their keyboard and click of their mouse is accessible to their employers. A recent survey of one thousand large companies revealed that 45% monitor their employees' e-mail, computer files, and phone calls, and almost two-thirds use some type of electronic monitoring.⁷⁴

There are a number of reasons that employers are interested in monitoring the computer activities of their employees. Employers have a significant interest in avoiding potential litigation arising from harassing or discriminatory e-mails floating around office computer networks. Potential trade secrets leaks along with opportunistic behavior create an interest in monitoring employee computer use. Probably the most obvious reason for employee monitoring is productivity levels. With the distraction of Internet access, it is a wonder that any work gets done anymore. In a recent Wall Street Journal article, an Internet retailer reported that 65 % of orders are placed during work hours, and Internet traffic actually drops on the weekends. The only conclusion that can be drawn is that employees do their Internet shopping while their employers believe they are diligently at work. Another survey of three companies revealed that the companies collectively spent "the equivalent of 350 eight-hour workdays accessing the Penthouse Magazine website in a single month."⁷⁵

Consequently, a strong case can be made that employers have a legitimate business justification for monitoring computer and e-mail use by their employees. But, like employer monitoring of employee telephone calls, an employer's right to monitoring is not without limits.

Federal Electronic Communications Privacy Act

Generally

Adopted in 1986, the Electronic Communications Privacy Act ("ECPA")

amended the original federal Wiretapping Act to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and technological technologies." S. REP. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. Among other things, the ECPA added "electronic communication" to the Wiretapping Act's protection of "wire" and "oral" communications, as well as to the definition of "intercept." Courts have treated e-mail somewhat differently than phone messages since the adoption of the ECPA. This is due to the explicit distinction between intercepting communications and accessing stored communications.

As discussed above, the Wiretapping Act provides civil and criminal relief against "any person who — (a) intentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."⁷⁶ Interception, as it relates to e-mail, occurs when the message is acquired after it has been sent by the sender, but before it is received by the recipient.⁷⁷ Therefore, under the Wiretapping Act as amended by the ECPA, a plaintiff has a valid claim when an employer acquires an e-mail sent by an employee before the recipient of the e-mail receives it.

One portion of the ECPA is the Stored Wire and Electronic Communications Act, 18 U.S.C. § 2701 *et seq.* ("Stored Communications Act") which provides, among other things, protection against unauthorized "access" to "electronic communication while it is in electronic storage."⁷⁸ Electronic storage refers to "intermediate storage" and "back-up protection storage," both of which are created during the transmission of a sent e-mail. In short, the ECPA's Stored Communication Act provides a cause of action against employers who access e-mails from storage during the period of time between the sending of the e-mail and the receipt of the e-mail by the recipient.

Moreover, where e-mail is concerned, protection of an employee's privacy is limited under the "service provider exception" of the ECPA which states:

It shall not be unlawful under this chapter for . . . [an] officer, employee, or agent of a provider of wire or elec-

tronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.⁷⁹

Some have argued that employers who provide their own networks and e-mail systems would qualify as a "provider." While employers who use public e-mail networks like Compu-serve or MCI Mail may not be providers, they are sometimes considered "agents."⁸⁰

Representative Cases

○ *Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623 (E.D. Pa. 2001). Plaintiff Richard Fraser began working as an agent for Nationwide Insurance in 1986. At the time, he signed an agent's agreement under which he would be an independent contractor and would represent Nationwide in the sale and service of insurance. Each party had the right to cancel the agreement at any time. In 1990, Fraser leased computer hardware and software from Nationwide for business purposes. The lease agreement specifically stated the computer system was the property of Nationwide. Whenever someone logged onto the computer, a notice appeared on the screen informing the user that the system, including e-mail, could be monitored to protect against unauthorized use.

In June 1996, Fraser and other Nationwide agents formed a chapter of the Nationwide Insurance Independent Contractors Association, an organization aimed at defending the status of exclusive career agents as independent contractors, the court said. The organization also sought to prevent the company from engaging in allegedly illegal business practices. Fraser participated in lobbying efforts, and filed a complaint with the state reporting alleged illegal business practices, the court said. In 1998, Nationwide was implementing new business practices that Fraser and other agents opposed.

Association members asked Fraser to prepare a letter to Nationwide's competitors to solicit interest in acquiring the policyholders of the approximately two hundred NIICA members in Pennsylvania. The agents did not actually intend to leave Nationwide, but merely wanted to use the letter as leverage. The letter ultimately was sent to just one

competitor. Nationwide secured a copy of the letter, but did not know if it been sent to any competitors, the court recounted. In August 1998, the company's director of electronic communications searched Nationwide's electronic file server for e-mails indicating whether or not the letter had been sent. The director found an e-mail Fraser had sent to a co-worker indicating the letter had been sent to at least one competitor. The e-mail was retrieved from the co-worker's file of already received and discarded messages stored on the server. In September 1998, Nationwide canceled Fraser's Agent Agreement. Fraser appealed to Nationwide's internal review board, which upheld the termination.

Fraser sued, alleging Nationwide unlawfully intercepted his e-mail communication when it retrieved the message from its electronic storage sites in violation of the Wiretapping Act and its protection against unauthorized "interception" of electronic communication. The trial court held that Nationwide did not "intercept" the communication since it retrieved the e-mail after it had been already sent and received. According to the court, retrieval of a message from storage while it is in the course of transmission is 'interception' under the statute, while retrieval of a message from storage after transmission is complete is not. Fraser also maintained that Nationwide unlawfully accessed his e-mail from storage, in violation of the federal Stored Communications Acts, which prohibits unauthorized "access" to an electronic communication while it is on "electronic storage" during the

course of transmission. The act defines "electronic storage" as temporary storage incidental to the electronic transfer of the message or storage by an electronic communications server for purposes of backup protection. On this claim, the court held that the Stored Communications Act would protect a message in "intermediate storage," or the storage that occurs after the message is sent, but before it is received by the recipient, the court said. However, "retrieval of a message from post-

[T]he Nebraska Act contains an extremely broad exemption for employer interception . . .

transmission storage is not covered by the Stored Communications Act. The Act provides protection only for messages while they are in the course of transmission." Thus, the trial court found that Nationwide's conduct was not prohibited under either the federal wiretap act or the Stored Communications Act because Nationwide did not intercept or access the messages sent by Fraser during their transmission.

- *Konop v. Hawaiian Airlines Inc.*, 236 F.3d 1035, opinion withdrawn, 262 F.3d 972 (9th Cir. 2001). The plaintiff, an employee of Hawaiian Airlines, maintained an Internet website where he posted bulletins critical of his employer, its officers and the pilot's union. The plaintiff controlled access to his website by requiring visitors to log in with a user name and password, which he provided to his fellow employees, but not members of management. Employee's using the website had to register and consent to an agreement not to disclose the site's contents. A company vice-president convinced an employee to let him use the employee's name to access the website because he was concerned about untruthful allegations on the

site. The vice-president did just that, clicking on the button accepting the terms and conditions and forwarding the information he found to company management and the union. The employee filed suit alleging numerous tort and labor claims and violation of the federal wiretap act and Stored Communications Act. The Ninth Circuit held that the contents of an employee's secured website were electronic communications protected under the Wiretapping Act and that Hawaiian Airlines violated the Act when it accessed the employee's website without permission and under false pretenses. On August 28, 2001, this opinion was withdrawn by the Ninth Circuit with no accompanying explanation other than "[a] subsequent opinion will be filed at a later date. Judge Reinhardt dissents from the withdrawal of the opinion."⁸¹

- *Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041 (N.D. Ill. 1998). Defendant UOP hired plaintiff Andersen Consulting to perform a computer systems integration project. During the project, Andersen employees had access to and used UOP's internal e-mail system. UOP's e-mail system was entirely internal and was not connected to the Internet. After UOP became dissatisfied with Andersen's performance, it terminated the project and sued Andersen alleging breach of contract, negligence and fraud. While the case was pending, UOP and its law firm divulged the contents of Andersen's e-mail messages on UOP's e-mail system to the Wall Street Journal, which subsequently published an article entitled, "E-Mail Trail Could Haunt Consultant in Court." Andersen then brought suit against UOP and its law firm, alleging violation of the ECPA. The district court granted UOP's motion to dismiss, holding that UOP did not provide "electronic communication service to the public" and therefore was not covered by the ECPA.

○ *McVeigh v. Cohen*, 983 F.Supp. 215 (D.D.C. 1998). McVeigh was a highly decorated member of the U.S. Navy serving aboard the nuclear submarine U.S.S. Chicago. A civilian volunteer received an e-mail through American Online ("AOL") regarding the toy-drive she was coordinating for the children of U.S.S. Chicago crew members. Because the e-mail contained only an e-mail address, the civilian searched the AOL member profile directory to discover that the sender of the e-mail worked in the military, listed his marital status as "gay," and identified his interests as including "collecting pics of other young studs" and "boy watching." The civilian volunteer forwarded the e-mail to her husband, who was an officer on the U.S.S. Chicago. Navy JAG commenced an investigation to discover if the author of the e-mail and member profile was McVeigh. JAG investigators spoke to an AOL representative, who confirmed that McVeigh was the holder of that e-mail account. Because McVeigh's statement of homosexuality violated the Navy's "Don't Ask, Don't Tell," policy, McVeigh was terminated. However, the district court granted McVeigh a preliminary injunction barring his discharge, in part because the Navy likely violated the ECPA by obtaining the information from AOL without a search warrant or valid subpoena.

○ *Bohach v. Reno*, 932 F. Supp. 1232 (D. Nev. 1996). The City of Reno's police department retrieved messages stored on the their computer paging system in an internal affairs investigation of the plaintiff-employee. In rejecting the plaintiff's ECPA claim, the court held the city was exempt as a "service provider" under the ECPA because it provided the terminals, computer, and software necessary for the users to send and receive electronic communications. *Id.* at 1236. Because the City was the provider of the "service," neither it nor its employees could be liable under the ECPA.

Nebraska Act

In 1969, Nebraska adopted its version of

the Wiretapping Act. Like the federal Wiretapping Act, the Nebraska Intercepted Communications Act, NEB.REV.STAT. §§ 86-701 to -712, has been amended to cover electronic communications. However, unlike the federal ECPA, the Nebraska Act contains an



extremely broad exemption for employer interception, disclosure or use of communications. Specifically, the Nebraska Act provides that it is not unlawful for any employer on its business premises to:

intercept, disclose, or use that communication in the normal course of his, her or its employment while engaged in any activity which is a necessary incident to the rendition of his, her or its service or to the protection of the rights or property of the carrier or provider of such communication services.⁸²

However, the Nebraska Act does bar an employer's use of random monitoring unless:

- the random monitoring is done for mechanical, service quality, or performance control checks; and
- reasonable notice of the policy of random monitoring is provided to the employer's employees.

Like the federal Wiretapping Act and ECPA, the Nebraska Act does not apply where one of the parties to the communication consents to interception of the communication provided the communication is not being intercepted for a criminal or tortious purpose.

Constitutional Protections

Generally

Like other forms of employer surveillance discussed herein, an employer's monitoring of employee computer use or e-mail may be subject to the protections of the Fourth Amendment and its state counterparts. However, because a finding of state action is necessary, these constitutional protections generally extend only to public employees.⁸⁴

Cases

○ *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000). Criminal case. Simons was employed by a division of the CIA as an electronic engineer. The CIA provided Simons with an office and a computer with Internet access. The CIA instituted a policy limiting employee use of Internet and notifying employees that the CIA could "audit, inspect, and/or monitor" employee use of the Internet. The CIA discovered, after searching the "firewall" database, that Simons' computer had an unusually large number of hits using the word "sex." CIA management subsequently examined Simons' computer and discovered that Simons' had downloaded over 1,000 pornographic files from the Internet, some of which pictured minors. Simons was terminated by the CIA and convicted of violating various federal child pornography statutes. In appealing his criminal convictions, Simons challenged the warrantless search of his computer database. The Fourth Circuit held that although Simons had an expectation of privacy in his office (which he did not share with anyone), he was subject to a valid warrantless search of his office computer. The appellate court held that the government's interest in investigating work-related misconduct outweighed any reasonable expectation of privacy Simons had in his computer files.

○ *Bohach v. Reno*, 932 F. Supp. 1232 (D. Nev. 1996). The City of Reno's police department retrieved messages stored on the their computer paging system in an internal affairs investi-

gation of the plaintiff-employee. The court rejected Bohach's constitutional claim and held that even if the officers had a subjective expectation of privacy, they couldn't have had an objective expectation of privacy. The court reasoned (1) the messages Bohach had sent were "essentially e-mail," (2) the officers knew they were logged onto a network, and (3) the messages sent were prohibited by the department's anti-discrimination policy.⁸⁵

- *Star Pub. Co. v. Pima County Attorney's Office*, 891 P.2d 899 (Ariz.App. 1994). As part of its investigation of improprieties in a county office, Plaintiff newspaper requested copies of e-mail communications of county employees, which was refused by the Defendant County. In order the production of the e-mails and awarding the Plaintiff newspaper attorneys' fees, the Arizona appellate court noted in dicta that it "doubt[ed] that public employees have any legitimate expectation of privacy in personal documents that they have chosen to lodge in public computer files"⁸⁶

Common Law Claims

Invasion of Privacy

Generally

As with telephone monitoring, courts have recognized claims for tortious invasion of privacy where an employer has intentionally intruded upon the solitude or seclusion of an employee or her private affairs or concerns, provided the intrusion would be highly offensive to a reasonable person. However, as the case below demonstrates, courts tend to find employees have a reduced expectation of privacy in their use of employer-provided computers and e-mail and grant employers greater latitude with respect to their ability to monitor such.

Cases

- *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996). Defendant Pillsbury maintained an e-mail system that was used to promote internal communications. Pillsbury repeatedly assured its employees that

all e-mail communications would remain confidential and privileged, could not be intercepted and used by the Pillsbury against the employees as ground for discipline or termination. On his home computer, Plaintiff Smyth received certain e-mails from his supervisor, to which he responded by "making comments about Pillsbury sales staff, including a threat to; kill the backstabbing bastards" and a reference to a planned holiday party as the "Jim Jones Koolaid affair." Pillsbury intercepted the e-mails and terminated Smyth, who subsequently brought suit for wrongful discharge and invasion of privacy. The trial court granted Pillsbury's Rule 12(b)(6) motion to dismiss, finding that: (i) Smyth did not have a reasonable expectation of privacy in his e-mail messages because he voluntarily sent them over Pillsbury's computer system, notwithstanding any assurances made by Pillsbury; and (ii) even if Smyth had a reasonable expectation of privacy, that expectation was outweighed by Pillsbury's legitimate interest in preventing inappropriate, unprofessional or illegal communications over its e-mail system.

Defamation

- *Meloff v. New York Life Ins. Co.*, 240 F.3d 138 (2d Cir. 2001). After 27 years as an employee of New York Life Insurance Company, plaintiff Phyllis Meloff was fired for billing seven months of personal commuting expenses to her company credit card and failing to reimburse the company. Her supervisor sent an e-mail to seven company managers outlining Meloff's discharge for using the credit card "in a way in which the company was defrauded." The e-mail was subsequently transmitted by one manager to four additional managers, one of whom forwarded the message to five more employees. Additional employees learned of the memo through word-of-mouth. Meloff sued New York Life for sex discrimination, retaliation and defamation. Meloff's discrimination claim was dismissed before trial and the jury rejected her retaliation claim. However, the jury sided with Meloff on her claim of defamation, awarding her \$250,000 in

compensatory damages and \$1 million in punitive damages. The trial judge overturned the jury verdict. On appeal, the Second Circuit awarded Meloff a new trial, finding that a jury, rather than a trial judge, was better prepared to evaluate whether the average person would find the company's comments about Meloff to be defamatory. The company argued there was no defamation because it had a qualified privilege to discuss the incident with other management personnel and the e-mails were designed to notify only top staff of the termination. To that privilege, Meloff had to prove the statement was false and that the company abused its discretion. The court said a reasonable jury could have found actual malice in New York Life's circulation of the e-mail accusing Meloff of fraud. The court noted that when Meloff spoke with her supervisor about the credit card bill and presented the supervisor with a reimbursement check the supervisor responded "mildly" and said that the charges were "no problem." In addition, Meloff had paid for personal charges before on her credit card and had even been given a reimbursement form by company representatives. Yet, Meloff was terminated a week after explaining the situation to her supervisor and an e-mail was sent implying she had defrauded the company.

Audio/Video Monitoring

Statutory Restrictions

- *Dorris v. Absher*, 179 F.3d 420 (6th Cir. 1999). Defendant was employed as director of the local Rabies Control Center, whose office consisted of one large room that was shared by all employees. On two occasions, the defendant placed a tape recorder on the top shelf of a cabinet in the large room and secretly recorded the conversations of the employees. The conversations were of a highly personal nature and included harsh criticism of the defendant. The defendant director subsequently played the recordings for friends and relatives. Based on the information contained in the recordings, the defendant

terminated two of the employees. The employees brought suit alleging, among other things, violation of the Wiretapping Act. Because the court found that the surreptitious tape recording constituted an "interception" of an "oral communication" and the employees had an expectation of privacy that was both subjectively and objectively reasonable, judgment against the defendant director under the Wiretapping Act was affirmed.

Common Law

Courts in other jurisdictions have recognized cause of action for invasion of privacy with respect to the improper use of audio and video recording devices.⁸⁷

Searches

Long before employer's began inquiring into such "high tech" areas as employee e-mail use and their genetic makeup, employers routinely conducted physical searches of employees and their property for legitimate work-related purposes such as investigations of workplace theft. Obviously, an employer's physical search of an individual's person or personal effects gives rise to same types of issues and claims raised above. Some illustrative cases are as follows:

- *O'Connor v. Ortega*, 480 U.S. 709 (1987). Dr. Magno Ortega, a physician and psychiatrist, was an employee of a state hospital and had primary responsibility for training physicians in the psychiatric residency program. Hospital officials became concerned about possible improprieties in Ortega's management of the program, particularly with respect to his acquisition of a computer and charges against him concerning sexual harassment and inappropriate disciplinary action against a resident. While he was on administrative leave pending investigation of the charges, hospital officials, allegedly in order to inventory and secure state property, searched Ortega's office and seized personal items from his desk and file cabinets that were subsequently used in administrative proceedings to support Ortega's discharge. No

formal inventory of the property in the office was ever made, and all the other papers in the office were merely placed in boxes for storage. Ortega filed an action against hospital officials under Section 1983



alleging that the search of his office violated the Fourth Amendment. The Supreme Court held that Ortega had a reasonable expectation of privacy in at least the desk and file cabinets in his office (a five justice majority found a reasonable expectation of privacy in the entire office) and that the search was subject to the Fourth Amendment. However, this reasonable expectation "may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."

- *K-Mart Corp. Store No. 7441 v. Trotti*, 677 S.W.2d 632 (Ct. App. Tex. 1984). Plaintiff Billi Trotti was employed in K-Mart's hosiery department, where employees were provided with lockers for the storage of personal effects during working hours. Lockers were not assigned and employees could, on request, receive locks for the lockers from K-Mart or purchase and use their own locks on the lockers. However, employees using their own locks were not required to provide K-Mart management with either a combination or duplicate key. Pursuant to this practice, Trotti used one of the lockers and brought her own combination

lock. On one particular day, Trotti placed her purse in her locker and locked it. When she returned to her locker during her afternoon break, she discovered the lock hanging open and her purse in disarray, although nothing was missing. K-Mart management had searched the lockers looking for a missing watch and price-marking guns. It was unclear whether K-Mart had a policy regarding searching of the lockers and their contents or whether this policy was communicated to the employees. The court held that Trotti had a reasonable expectation of privacy in the employer-provided locker and its contents because she purchased and used her own lock on the locker with the employer's knowledge.

- *Vernars v. Young*, 539 F.2d 966 (3d Cir. 1976). Plaintiff was a shareholder, officer, director and employee of Young Galvanizing. In challenging his termination, the plaintiff alleged one of the defendants opened and read without plaintiff's consent mail which was delivered to the defendant corporation's office but was addressed to plaintiff and marked "personal." The Third Circuit held that plaintiff stated a cause of action: "Just as private individuals have a right to expect that their telephonic communications will not be monitored, they also have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons."

Off-Duty Conduct

Most jurisdictions uphold an employer's right to investigate the off-duty conduct of its employees. However, depending upon the conduct involved and its relationship to the employer's valid interests and employee's duties, courts are sometimes reluctant to grant employers carte blanche authority to use the fruits of their off-duty investigations in affecting the terms and conditions of an employee's employment.


Cases

- *Grusendorf v. City of Oklahoma City*, 816 F.2d 539 (10th Cir. 1987) (upholding regulation barring on—

and off-duty smoking by firefighter trainees).

- *Rulon-Miller v. International Bus. Machine Corp.*, 208 Cal.Rptr. 524 (1984)(plaintiff was terminated by IBM after she was ordered to stop dating an employee of a competitor or be fired; the court affirmed \$300,000 jury verdict on wrongful discharge and intentional infliction of emotional distress claim).

Statutes

In recent years, a growing number of jurisdictions have attempted to prohibit employers from discriminating against employees for engaging in “any lawful activity” off the premises of the employer during nonwork hours that does not conflict with the employer’s essential business interests.⁸⁸ Although supporters of these statutes often argue that the primary purpose behind their legislation is to prohibit workplace discrimination against employee tobacco use, critics have argued that the use of “any lawful activity” is a back door effort to grant sexual orientation protected status. It is for this reason that recent legislative enactments have been narrowed to only protect smokers. 

Endnotes available upon request. Please contact Kathryn Bellman or Pamela Moore at the NSBA office. (402) 475-7091 or (800) 927-0117. E-Mail: kbellman@nebar.com or pmoore@nebar.com