

**PRIVACY IN THE WORKPLACE:
SOURCES OF LAW AND
ILLUSTRATIVE CASES**

Prepared for
American Bar Association
Section of Labor and Employment Law
2007 Annual CLE Conference

Philadelphia, Pennsylvania
November 7-10, 2007

T. J. Conley
Leonard, Street and Deinard
150 South Fifth Street, Suite 2300
Minneapolis, Minnesota 55402
(612) 335-1634
tjc@leonard.com

I. SOURCES OF LAW

A. Constitutional:

1. **Fourth Amendment.** The Fourth Amendment does not prescribe all searches and seizures, but does require reasonableness. *O'Connor v. Ortega*, 480 U.S. 709 (1987).
2. **State Constitutions.** “A number of state constitutions have an explicit guarantee of privacy, but California is the only state granting constitutional privacy rights to private sector workers.” Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Work Place*, 54 Fla. L. Rev. 289, 294 (2002).

B. Federal Law:

1. **Electronic Communications Privacy Act of 1986 (“ECPA”),** 18 U.S.C. §§ 2510-2522 (c/k/a “Federal Wiretap Act”).
 - a. Provides a civil cause of action against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a).
 - b. There are two exceptions to the general prohibition against interception: consent and the ordinary course of business exception.
 - c. The ordinary course of business exception will apply where the interception concerns the operation of the business, or the employer has a legitimate business interest justifying the interception.
2. **Stored Communications Act,** 18 U.S.C. §§ 2701-2711. (Title II of the ECPA). The SCA provides that a person or entity providing an electronic communication service to the public shall not knowingly divulge the contents of a communication in electronic storage. 18 U.S.C. § 2702.
3. **National Relations Labor Act,** 29 U.S.C., §§ 151 – 169. Even non-union employees in the private sector may find protection under the NRLA when they act in concerted fashion. *See, e.g., E.I. duPont de Nemours & Co.*, 311 NLRB 893 (1993) (Company policy prohibiting distribution of union literature via e-mail, while permitting other non-work uses of the same resource, was an unfair labor practice); *Guard Publ’g Co.*, NLRB No. 36-

CA-8743-1 (oral argument 3/27/07) (use of company e-mail to communicate about union issues).

4. **Health Insurance Portability and Accountability Act of 1996 (HIPPA)**, 42 U.S.C. §§ 201 et seq.; 45 CFR 164.
5. **Fair Credit Reporting Act**, 15 U.S.C. §§ 1681 et seq.

C. State Law:

1. Various state statutes analogous to the ECPA provide employees with protection with regard to stored wire and electronic communications. *See Adams, Scheuing, and Feeley, E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly*, 67 Def. Couns. J. 32, 40 (2000).
2. Some state laws provide broader coverage than the ECPA. *See, e.g.* New York Penal Law Sec. 250.25 (person is guilty of tampering with private communications when, knowing that he does not have the consent of the sender or receiver, he opens and reads sealed private communication); 1998 Conn. Pub. Acts § 142 (b)(1) (requires employers who engage in any type of electronic monitoring to give prior notice to all employees who may be affected); Massachusetts' Unlawful Interception of Wire Communication, G.L.C. 272, 99; Brown, *Policies for Corporate Internet and E-Mail Use*, 564 PLI/Pat 637 (1999).

D. Common Law of Privacy. *See* Restatement (Second) of Torts, § 652

1. **Intrusion into seclusion:** Intrusion into seclusion claims are rarely successful against employers in the context of intercepting email due to the difficulty of proving a reasonable expectation of privacy. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Work Place*, 54 Fla. L. Rev. 289, 302-304 (2002). *See also* Martin and Anderson, *Workplace Claims: Wrongful Termination, Collateral Torts, Privacy, Restrictions on Right to Compete, Reference Checks, and Investigations*, 662 PLI/Lit 1095, 1136 (2001); Adams, Scheuing and Feeley, *E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly*, 67 Def. Couns. J. 32, 41-46 (2000).
2. **Public disclosure of private facts:** Invasion of privacy actions based on employer disclosures of private facts are generally unsuccessful. *See e.g., Chimare v. T.D. Waterhouse Inv. Servs., inc.*, 280 F.Supp.2d 208 (S.D. N.Y. 2003); Annotations to Restatement (Second) of Torts § 652D. However, such actions are viable under certain circumstances. *See, e.g., Beaumont v. Brown*, 257 N.W.2d 522, 534 (Mich. 1977).

E. Contractual: Collective Bargaining Agreements may affect an employer's right to conduct surveillance:

1. In *National Steel Corp. v. NLRB*, 324 F. 3d 928 (7th Cir. 2003), several unions filed charges against National Steel to require that it bargain over the company's use of hidden cameras. On appeal, the Seventh Circuit, relying on *Ford Motor Co. v. NLRB*, 441 U.S. 488 (1979), held that the company had an obligation to submit the matter to collective bargaining because it was germane to the work environment and not a managerial decision at the core of entrepreneurial control.
2. See, *BMW v. Athena Neurosciences, Inc.*, 2001 W.L. 788738 (N.D. Ia. 2001) (Entering negotiated order prohibiting railroad from conducting genetic testing on union employees).

II. ILLUSTRATIVE CASES

A. E-Mail Monitoring

1. **Timing of Interception:** Employers will not violate the ECPA so long as they are monitoring only post-receipt e-mails. To violate the ECPA, the acquisition must occur during the transmission, not after the e-mail is received. Accessing stored, opened e-mail after receipt is not considered "intercepting" under the ECPA. See Kevin Chapman, *I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts*, 5 N.C. J. L. & TECH 121 (2003); *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 W.L. 974676 (D. Mass. 2002); *Eagle v. Investment Services Corp.*, 146 F.Supp.2d 105 (D. Mass. 2001); *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa 1996).
2. **Reasonable Expectation of Privacy:** In *Thygeson v. U.S. Bancorp*, 2004 WL 2066746 (D. Or. 2004), the Court held that US Bancorp's access of Thygeson's "personal" folder on the company's computer did not constitute an invasion of privacy. The court found that Thygeson could not have had a reasonable expectation of privacy in the e-mails that he sent and received using his U.S. Bancorp office e-mail, even though he saved them in a folder labeled personal, because they were not password-protected.

The court additionally found that Thygeson did not have a reasonable expectation of privacy in the internet websites that he accessed from his computer, even though "in contrast to an e-mail system provided by an employer, most employees have a higher expectation of privacy when

accessing personal internet e-mail accounts, such as Netscape or Hotmail accounts, even when doing so while at work.” *Thygeson*, 2004 WL 2066746, * 21.

3. *But see Fischer v. Mt. Olive Lutheran Church*, 207 F.Supp.2d 914, 924-25 (W.D. Wis. 2002) (denying summary judgment to coworkers and supervisor who accessed employee’s personal e-mail account by guessing his password because such actions may violate both federal Stored Communications Act and Wisconsin wiretap act).
4. *But see Haynes v. Office of the Attorney General Phil Kline*, 298 F.Supp.2d 1154, 1162 (D. Kan 2003). (Former employee had reasonable expectation of privacy, despite warnings to the contrary, because employees were allowed to use their work computers for private communications; employees were told how to create public and private files; employees were advised that intentional access to another users email without permission was prohibited; employees were given passwords to prevent others from gaining access to their computers, and there is no evidence that the employer ever monitored or viewed private files, documents or emails of any employee in the past).
5. **Employer’s Duty:** Where a company has the technical capacity and legal ability to monitor its employees’ email and internet connections, the employer may have a duty to act upon learning that an employee is viewing child pornography on his workplace computer by terminating the employee and/or informing law enforce. *Doe v. XYV Corp.*, 887 A.2d 1156 (N.J. App. 2005).
6. In *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), the Court held that even though an employee had a reasonable expectation of privacy in his workplace computer, his employer’s reservation of control over it gave the employer authority to consent to a search conducted by the FBI looking for child pornography.

B. Home Computer:

1. In *TBG Ins. Services Corp. v. Superior Ct. (Robert Zieminski)*, 117 Cal. Rptr. 2nd 155 (Ct. App. 2002), the plaintiff, a former executive, used a company computer at home. Company policy forbade the use of the home computer for other than business purposes, and also forbade its use for obscene or other inappropriate purposes.

After the executive was discharged for inappropriate computer use and sued for wrongful discharge, the company demanded that he turn over the

home computer during discovery. The former executive refused to comply, arguing that to do so would represent an invasion of his privacy, as well as that of his wife's and children's. The court nonetheless ordered the computer to be turned over, subject to a protective order covering private transactions, because the employee had provided express consent to the company's policy which reserved the right to monitor that computer and deprived him of any expectation of privacy.

2. *Northwest Airlines, Inc. v. Local 2000, No. 00-08*, (D. Minn. 2000) (employees' home computers may be analyzed by third party to analyze whether data is discoverable for claim of illegal work stoppage).
3. *T. B. G. Insurance Services Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155 (Cal. Ct. App. 2002) (No violation of privacy claim under California Constitution where employer brought motion to compel production of computer employee had used for work at home as a defense in former employee's wrongful termination action.)
4. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) (unauthorized access by supervisor to employee's website could violate Stored Communications Act).

C. Telephone Monitoring

1. Third party retrieval and recording of a voicemail message was "interception" subject to the Wiretap Act, and not covered by the Stored Communications Act." "When the Fifth Circuit observed that the WireTap Act is famous (if not infamous) for its lack of clarity,' it might have put the matter too mildly.'" *U.S. v. Smith*, 155 F.3d 1051, 1054 (5th Cir. 1998) (internal citations omitted).
2. *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992) (Employer who surreptitiously wiretapped and tape recorded employee conversations violated wiretap statute because employee did not consent to tape recording and business use of telephone extension exception did not apply.)
3. *Briggs v. American Air Filter Co, Inc.* 455 F. Supp. 179 (N.D. Ga. 1978), *aff'd* 630 F.2d 414 (5th Cir. 1978) (Where manager had reason to believe that employee was disclosing confidential business information, manager's use of the extension phone was in the ordinary course of employer's business and was therefore exempt from provision prohibiting the interception of wire communications.)

4. *James v. Newspaper Agency Corp.* 591 F.2d 579 (10th Cir. 1979)
(Employer came within exception where installation of monitoring device was based on concern over abusive language by irate customers and need for better training and supervision to employees dealing with public, and installation was not done surreptitiously).
5. *Arias v. Mutual Central Alarm Service, Inc.*, 202 F.3d 553 (2nd Cir. 2000)
(Covert interception of employee telephone calls fell within ordinary course of business exception to federal wiretap statutes since legitimate business reasons supported both the recording of all incoming and outgoing calls and the lack of notice to employees; employer was repository of sensitive security information, accurate recording of calls could assist the employer, its customers, and police and fire departments, and recording was standard industry practice recommended by underwriters and trade associations.)
6. *EPPS v. St. Mary's Hospital of Athens, Inc.*, 802 F.2d. 412 (11th Cir. 1986)
(Interception of employee telephone call fell within telephone extension exception to civil liability.)
7. *But see Williams v. Poulos*, 11 F.3d 271 (1st Cir. 1993) (Employers' interception of employee's telephone calls did not come within consent exception to federal wiretapping laws; although intercepted corporate officer was told that employee calls would be monitored, officer was not told of manner in which monitoring was conducted or that he himself would be monitored.)
8. Some jurisdictions have recognized that the improper interception of employees' phone calls may constitute a tortious invasion of privacy. *See Ali v. Douglas Cable Communications*, 929 F. Supp. 1362 (D. Kan.1996) and cases from Georgia, Louisiana, Oregon, and Alabama cited therein.

D. Videotape/Audiotape Monitoring

1. *Audenreid v. Circuit City Stores, Inc.*, 97 F. Supp. 2d. 660 (E.D. Pa. 2000)
(hidden video camera in plaintiff's office not an interception under federal or state law because it did not capture audio).
2. *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997) (Videotaping of employees in open and undifferentiated work area not objectionable under Fourth Amendment because employees lacked objectively reasonable expectation of privacy); *Brannen v. Board of Ed.*, 761 N.E. 2d. 84 (Ohio 2001) (same).

3. *Cramer v. Consolidated Freightways, Inc.*, 255 F.3d 683 (9th Cir. 2001) (Court rejected defendant's claim that state law privacy claim should be pre-empted under Section 301 of the Labor Management Relations Act where employer had concealed video cameras and audio listening devices behind two-way mirrors in restrooms, ostensibly to detect and prevent drug use by truck drivers.)

E. Drug Testing

1. *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989) (suspicionless drug-testing of employees applying for promotion to sensitive positions reasonable under Fourth Amendment).
2. *Booker v. City of St. Louis*, 309 F.3d 424 (8th Cir. 2002) (affirming summary judgment against municipal correction officer who was dismissed after failing drug test).
3. *Carroll v. City of Westminster*, 233 F.3d 208 (4th Cir. 2000) (Fourth Amendment not violated when physician conducted drug urinalysis without police officer's knowledge during routine office visit).
4. *Aubrey v. School Board of Lafayette Parish*, 148 F.3d 559 (5th Cir. 1998) (school board's need to conduct suspicionless searches outweighed privacy interests of safety sensitive employees).
5. *Wilcher v. City of Wilmington*, 139 F.3d 366 (3rd Cir. 1998) (finding that drug-testing method was reasonable under the Fourth Amendment did not preclude finding that it was an invasion of privacy under Delaware law).
6. *But see Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611 (3d Cir. 1992) (Pennsylvania common law regarding tortious invasion of privacy may give rise to wrongful discharge action relating to urinalysis or to personal property searches.)
7. Many states have their own drug testing statutes. *See, e.g.*, Minn. Stat. §§ 181.950-957.

F. Medical and Psychological Examinations

1. **Business Necessity:** Medical examinations to determine fitness to return to work must meet the requirement of job-relatedness and business necessity. *See e.g. Beveridge v. Northwest Airlines*, 259 F.Supp.2d 838 (D. Minn. 2003).

2. The Second Circuit has recently offered standards to guide the inquiry as to whether the examination was required for business necessity:

An employer cannot simply demonstrate that an inquiry is convenient or beneficial to its business. Instead, the employer must first show that the asserted “business necessity” is vital to the business. For example, business necessities may include ensuring that the workplace is safe and secure or cutting down on egregious absenteeism. The employer must also show that the examination or inquiry genuinely serves the asserted business necessity and that the request is no broader or more intrusive than necessary. The employer need not show that the examination or inquiry is the only way of achieving a business necessity, but the examination or inquiry must be a reasonably effective method of achieving the employer’s goal.

Conroy v. New York Dept. of Correctional Services, 333 F.3d 888, 897-98 (2nd Cir. 2003).

3. **Non-Disabled Plaintiff:** A non-disabled applicant may be protected by the ADA’s regulation of medical examinations. *O’Neal v. City of Albany*, 293 F.3d 998 (7th Cir. 2002); *Green v. Joy Cone Co.*, 278 F.Supp.2d 526 (W.D. Pa 2003) (person need not be a “qualified individual with a disability” in order to seek injunctive relief for a violation of the ADA’s prohibitions on pre-hire medical inquiries).
4. **Conditional Offer:** While the ADA permits an employer to require an applicant to submit to a medical examination after a conditional offer of employment has been made, the medical examination is premature if the offer is also contingent upon other matters, such as satisfaction of a background check. *Leonel v. American Airlines, Inc.*, 400 F.3d 702 (9th Cir. 2005).
5. **Psychological Testing:** Requiring applicants or employees to submit to psychological screening such as the Minnesota Multiphasic Personality Inventory (MMPI) may implicate the provisions regarding medical testing under the Americans With Disabilities Act. *See Karraker v. Rent-A-Center, Inc.*, 411 F.3d 831 (7th Cir. 2005). However, the ADA does allow for post-hire testing when such testing is “job related and consistent with business necessity.” *See e.g. Conrad v. Board of Johnson County Commissions*, 237 F.Supp.2d 1204 (D. Kan. 2002).

6. **FMLA:** The Family Medical Leave Act also entitles employers to require a medical certification from employees. *See* 29 C.F.R. §§ 825.305-825.308.
 - a. Employers may request clarification of the certificate supplied by the employee. *Sorrell v. Rinker Materials Corp.*, 395 F.3d 332 (6th Cir. 2004); *Wheeler v. Pioneer Dev. Serv., Inc.*, 349 F.Supp.2d 158 (D. Minn. 2004).
 - b. Employers may also challenge the adequacy of the information provided. *Kauffman v. Federal Express Corp.*, 426 F.3d 880 (7th Cir. 2005); *Brumbalough v. Camelot Care Centers, Inc.*, 427 F.3d 996 (6th Cir. 2005). *See also* *Cooper v. Fulton County*, 458 F.3d 1282 (11th Cir. 2006) (upholding regulation that employee has 15 days to submit medical certification); *Killian v. Yorozu Automotive Tennessee, Inc.*, 454 F.3d 549 (6th Cir. 2006) (same).
7. **Accountability:** An employer may require employees on sick leave, including FMLA leave, to report into a hotline whenever they leave their houses; “there is no right in the FMLA to be ‘left alone’”. *Callison v. City of Philadelphia*, 430 F.3d 117 (3rd Cir. 2005).

G. Genetic Testing

1. *Norman-Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F.3d 1260 (9th Cir. 1998) (constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information, raising serious questions about nonconsensual testing for certain conditions).
2. Forty-six states have enacted some form of genetics legislation. Suter, *The Allure and Peril of Genetics Exceptionalism: Do We Need Special Genetics Legislation*, 79 Wash. U. L.Q. 669, 691 (2001). Twenty-seven states prohibit employers from requiring employees to submit to genetic testing or restrict the use of such test results. Finkin, *Privacy in Employment Law* (2d Ed. Supp., 2007) at 14.