FEDERAL, STATE AND COMMON LAW PRIVACY ISSUES IN THE COMPUTER AGE

34TH ANNUAL INSTITUTE ON EMPLOYMENT LAW

Michael J. Leech

Biographical Information

Program Title: 34th Annual Institute on Employment Law

Name: Michael J. Leech

Position or Title: Principal

Firm or Place of Business: Talk Sense Mediation

Address: 101 North Wacker Drive, Suite 2010,
Chicago, IL 60606
Phone: (312) 250-8123
Fax: (312) 250-8129
E-Mail: mleech@talk-sense.com

Primary Areas of Practice: Employment Law, Mediation & Business Litigation

Law School: University of Virginia

Work History:

Chapman & Cutler (1976-1978)

Hinshaw & Culbertson (1978-present)

Membership in Associations, Committees: Founding Member, ABA Labor Section Committee on Employee Rights & Responsibilities; Founding Member, National Employment Lawyers Association; Fellow, American College of Labor & Employment Lawyers; Liaison for College of Labor & Employment Lawyers to American Law Institute's Restatement of Employment Law project.

Table of Contents

Introduction

This paper provides guidance on the privacy issues spawned by the expended use of technology in the workplace at the beginning of the Twenty-First Century. Reference is made to provisions of the US Constitution, federal statutes, state statutes, and common law causes of action.

E-mail & The National Labor Relations Act

E-mail is an essential part of today's workplace. What was once communicated in telephone conversations that could not be captured in anything other than the fallible and unreliable human memory is now preserved *in toto*, virtually indefinitely. E-mail provides an opportunity to monitor employee communications to a degree never before possible. This has made e-mail a valuable source of information for employer investigations: only the most cautious employee fails to leave a trail in the e-mail records.

Many people believe that deleting an e-mail message makes it disappear forever. Not so. Information systems protocols typically call for daily or at least weekly "backing up" of the entire contents of a system, which means that messages not immediately deleted can be recovered from backup computer tapes. Other mechanisms on the computer hard drive or on the server provide opportunities to recover even messages deleted immediately. Computer systems administrators can retrieve e-mail messages from personal e-mail accounts that have been accessed at work.

It is now commonplace for employee communications about workplace conditions and events to take place via e-mail. It is also common for the NLRB to determine that such communications reflect or constitute "protected, concerted activity" that Section 7 of the Act protects even in non-union facilities. For instance, the decision in *Timekeeping Systems, Inc.,* 323 NLRB 244, 154 LRRM 1233 (1997) focused on a sarcastic e-mail message from a software engineer to other employees about a newly-announced vacation policy that led to the employee's termination. The Board concluded that the sending of the e-mail message itself was concerted activity and that the employee was thus protected from discriminatory discharge based on his exercise of the right to send the e-mail message. See also *Electronic Data Systems Corp.,* 331 NLRB 343, 164 LRRM 1211 (2000)(e-mail message was not protected concerned activity only because it solicited employees to engage in a partial work slowdown unprotected by Section 7); *Daimler Chrysler,* 344 N.L.R.B. No. 154 (2005)(upholding

discipline for sending e-mail message encouraging aggressive use of "pool car" provision of collective bargaining agreement because it amounted to advocacy for a prohibited work slowdown).

Employer efforts to adopt rules governing the use of e-mail messages to discuss or carry on union organizing or other activities analogous to no-solicitation rules have not met with favor because they have not been consistently enforced. In *Media General Operations, Inc.*, 2002 WL 1267989 (ALJ Ruling, 2002), the right of an employer to prohibit personal use of e-mail was acknowledged, but the policy failed because both employees and managers at the company routinely used e-mail and computer messages for a variety of personal reasons. Thus, prohibiting the use of e-mail for union activity discriminated in violation of Section 8(a)(1) of the Act.

California Newspapers Partnership, 2002 WL 31940725 (ALJ Ruling, 2002) determined that a communications policy prohibiting use of e-mail for non-business reasons, including union-related business, was invalid because the employer never enforced the policy with respect to other non-business uses of e-mail. In addition, the ALJ determined that the communications policy was a mandatory subject of bargaining, and that neither the management rights clause nor the Zipper clause in the collective bargaining agreement permitted the employer to adopt the policy without union agreement or bargaining to impasse. In that case, the employee and union advocated even broader limitations of employer e-mail policies. They argued that prohibiting employees to circulate union material by e-mail is impermissible generally, perhaps seeking to expand *Excelsior Underwear* to create a right of access to employees by e-mail. The ALJ refused to consider the arguments because they were not supported by the General Counsel. The General Counsel had told the ALJ that it was relying on established law, while indicating that consideration was being given to advocacy of wider theories in other cases.

In *The Guard Publishing Co*., 2002 WL 336963 (ALJ Ruling, 2002), the ALJ relied on the failure to apply the "business-only" requirement to personal concerns of employees to conclude that

the policy was discriminatory and a violation of Section 8(a)(3). This made the employer's proposal to include the policy in the collective bargaining agreement illegal and its refusal to withdraw the proposal a violation of Section 8(a)(5).

The decision in *Prudential Ins. Co of America,* 2002 WL 31493320 (ALJ Ruling, 2002) found the employer's "business-only/no union advocacy" e-mail rule invalid on somewhat different grounds. In that case, it was not the use of e-mail for personal purposes, but the *employer's* use of e-mail and other computer resources to fight the union organizing campaign, that led to the decision that the prohibition was improper. The ALJ in that case, which involved employees scattered through the country not working on company premises, concluded that the prohibition was sufficiently material to invalidate the closely contested election results and require a new election.

Technology Issues in Harassment, Discrimination, Retaliation and Wrongful Termination Cases

Desktop and laptop computers are essential pieces of equipment in the Twenty-First Century workplace. In most instances, the computers are networked through a central server and provide internet access. While the internet provides access to a wealth of useful information employees may need to perform their jobs effectively, it also provides access to other websites, including those which enable workers to access, display and publish pornography to their co-workers. This has led many employers to implement filtering software to ensure that the internet is used for business purposes only. Employers who did not have this technology face an increased exposure to liability for sexual harassment. As with other electronic information, computer systems archiving is so comprehensive that a record of internet sites visited by each computer connected to the server will typically be maintained on backup computer tapes for an extended period of time.

Hostile Work Environment: Liability

Internet pornography has formed the basis for claims of hostile work environment in many cases. In *Luttrell v. O'Connor Chevrolet, Inc.,* 89 FEP Cases 161, 2001 WL 1263990 (N.D. Ill. 2002)(Kocoras, J.), the plaintiff testified that a co-worker repeatedly invited her to participate in an Internet pornography website and repeatedly exposed her to pornography downloaded from the company computers. This formed a part of the evidence the court found that a jury could determine was "severe and pervasive" harassment actionable under Title VII. The court in *Coniglio v. City of Berwyn,* 1999 WL 1212190 (N.D. Ill. 1999) found displays of internet pornography to be sufficient to state a claim for hostile work environment, citing *Galloway v. General Motors Services Parts Operation,*78 F.3d 1164, 1167 (7th Cir. 1996). *Accord, Estes v. Georgetown University,* 231 F.Supp.2d 279, 90 FEP Cases 698, (D. D.C. 2002).

Hostile Work Environment: Defense

In *DuFresne v. J.D. Fields and Co., Inc.,* 85 FEP Cases 25, 2001 WL 30671 (E.D. La. 2001), a plaintiff-employee bringing a sexual harassment claim had viewed internet sex scenes on her work computer and once attached an image to an e-mail to a manager at his home. The court ruled that this was probative and admissible on the issues of hostile work environment and damages.

Discriminatory Enforcement of Computer Policies

In a sex discrimination case, *Sherrod v. AIG Healthcare Management Services, Inc.,* 2000 WL 140746 (N.D. Tex. 2000), a woman who was found to have had downloaded sexual images from the internet and lost her job as a result. She claimed that the employer's actions were discriminatory based on sex. She argued that the employer did not take similar action against a male employee who she asserted had sent her at least one of the images. The employer escaped liability because she had not complained to anyone about this and management did not know about that incident. In addition, the employer showed that it had previously

fired an employee for downloading pornographic material from the internet.

It was the ignorance of the employer in *Sherrod* that enabled it to win summary judgment. An employer who monitors the websites visited by its employees to ascertain whether unauthorized activity is underway but does not enforce prohibitions on improper activity consistently risks liability for discrimination.

Employer Responsibility For Technological Retaliation

The employer in *Blakey v. Continental Airlines, Inc*., 164 NJ 38, 751 A.2d 538 (2000), maintained a website through a computer internet service provider, CompuServe, which also operated a separate, linked "employees-only" forum in conjunction with the website. Management was not welcome on the forum site, but when plaintiff initiated legal action against the company claiming discrimination, her co-workers unloaded criticism and ridicule on her in the forum. She complained to management about the allegedly false and defamatory comments being posted in retaliation for her legal action, and the court concluded that the employer had a duty to stop this form of co-worker harassment. The employer's responsibility for the comments was based on the court's conclusion that the forum website was an integral part of the workplace.

Retaliation

In *Hunnford v. McEnaney,* 249 F.3d 1142, 17 IER Cases 1121 (9th Cir. 2001), the court held that where a public employer terminated an employer who reported his concerns about downloading of pornographic material from the internet on department computers, liability for retaliation (for exercise of First Amendment rights) could be imposed.

Discovery Issues

In *Giardina v. Lockheed Martin Corp.,* 2003 WL 1338826 (E.D. La. 2003), the employee was permitted discovery of non-work-related sites visited by employees in a specific work area for a

period of months. In that case, the employee was permitted to take the discovery because she claimed that downloaded pornography was left for her to view on company computers in retaliation for her complaints about sexual harassment. In a case where widespread sexual harassment is alleged, an employee could presumably obtain such internet site visit records, which normally are automatically retained in computer backup storage tapes, as a means of proving how widespread the practice is.

In *TGB Ins. Services Co. v. Superior Court,* 96 Cal.App.4th 443, 117 Cal.Rptr. 155, 18 IER Cases 545 (2002), the employer defended a wrongful termination lawsuit by citing the employee's documented accessing of pornographic sites at work. The employee asserted that the sites "popped up" on his screen without his having tried to access them. But the employer had also issued the employee a laptop computer for use at home, and sought to inspect it to determine whether he used it to access pornographic sites. The employee resisted the request, citing personal information he maintained on the home computer (such as personal financial information), although the employer's policy with respect to both the office computer and the laptop computer stated that both were issued for business use only. The court concluded that access to any personal information could be the subject of a protective order, and ordered the plaintiff to provide the laptop.

Laws Creating Privacy Rights of Employees Using Technology Tools In The Workplace

Employers gather information on employees most frequently for purposes of detecting violations of employer policy and interests and taking action against offending employees. Avoiding liability to third parties or other employees is another reason for information-gathering activities, and assisting law enforcement to identify and prosecute violations of criminal law is yet another. While privacy, and its cousin anonymity, protect personal dignity, they also operate as indirect restraints on the otherwise virtually unrestrained power of employers to punish at-will employees.

Outlined below are some of the legal restraints designed to protect personal privacy that may be applied to employer information gathering activities. Those that have application to only one type of activity are described in the discussion of the area in which they are most frequently applied. Those introduced here are the laws that apply to a number of different forms of information-gathering.

Common Law Invasion of Privacy Torts

The Restatement, Second, of Torts §652, identifies four distinct invasion of privacy torts, (1) intrusion upon the seclusion of another; (2) appropriation of name or likeness of another; (3) publicity given to private facts; and (4) publicity placing a person in a false light. *Lovgren v. Citizens First National Bank of Princeton,* 126 Ill.2d 411, 534 N.E.2d 987, 128 Ill.Dec. 542 (1989). Of these four torts, intrusion upon seclusion is most frequently implicated in employment cases. For instance, in *Karraker v. Rent-A-Center, Inc.,*411 F.3d 831 (7th Cir. 2005) (MMPI personality test was a "medical examination" under the ADA which could not be used to make promotional decisions) denied a claim for public disclosure of private facts based on circulation of disclosure of the results of a personality test because the test results were viewed by people involved in dealing with the test and otherwise kept in a locked file cabinet. Only a few employment cases have presented problems in the other areas. Thus, the discussion here will focus on intrusion upon seclusion.

Illinois has adopted the last three of these causes of action, but remains somewhat ambivalent about the first, "intrusion upon seclusion." *Id.* There is a longstanding conflict among the appellate districts on the subject. Recent appellate decisions refusing to recognize the tort have focused on the facts of the particular case and concluded that the requirements of the tort would not have been met if it was recognized. The more egregious situations have prompted recognition of the tort in two districts where it was not previously recognized (First and Second Districts). The First, Second, Third and Fifth Districts now recognize the tort. The Fourth District has left open the question of whether it will reverse its current position rejecting the tort if faced with the proper case.

The core of this tort is the offensive prying into the private domain of another. Examples cited with approval include the following: invading someone's home; an illegal search of a shopping bag at a store; eavesdropping by wiretapping; peering into windows of a private home; and persistent and unwanted telephone calls. Where the harm results more from the act of making information public than from the intrusive collection of information, the tort of "publication of private facts" is more properly applied, *Id.*

With this tort, and with statutory standards cited in this section, the concept of a "reasonable expectation of privacy" is essential. This principle is founded on law arising under the Fourth Amendment's search and seizure restraints on governmental action, which apply to public employees but which are most frequently litigated in criminal prosecution suppression hearings. The same concept has been adopted by courts construing federal statutes protecting privacy interests. Often the legality of a search or monitoring of employee activity turns on whether the area which has been searched or monitored is one in which the employee has a "reasonable expectation of privacy."

The elements of the tort of intrusion upon seclusion were outlined in the much-cited decision of the Third District Appellate Court in *Melvin v. Burling,* 141 Ill.App.3d 786, 95 Ill.Dec. 919, 490 N.E.2d 1011 (3d Dist. 1986): (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is offensive or objectionable to a reasonable person; (3) the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish or suffering. The "reasonable expectation of privacy" standard approximates the combination of the second and third elements.

Fourth Amendment Limits On Public Employers

The Fourth Amendment to the U.S. Constitution protects the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures" and such activities are not to be performed by the federal government without "probable cause," and in certain instances, until issuance of a warrant by a "neutral and detached magistrate." These restrictions are applied to the States through the Fourteenth

Amendment due process clause under the “selective incorporation” doctrine. In the employment context, the Fourth Amendment applies to the actions of the federal, State and local government towards public employees. It does not restrain private employers unless their actions can properly be considered “State action.”

O'Connor v. Ortega , 480 U.S. 709 (1987) recognized at least the possibility of employee privacy interests in employee desks and file cabinets, in the context of a public employee claim for unreasonable search and seizure under the Fourth Amendment. But the opinion also acknowledged that actual office practices could mean that the employee had no "reasonable expectation of privacy" necessary to secure Constitutional protection. The Court called for balancing employee expectations of privacy against the government employer's need for supervision, control and efficient operation of the workplace.

Wiretap Act, Stored Communications Act and Electronic Communications Privacy Act

The Wiretap Act, 18 U.S.C. §§2510-2522, was amended by the Electronic Communications Privacy Act of 1986 (ECPA). Previously, the statute applied to oral and wire communications. The ECPA extended the statute to data and electronic communications as well and created the Stored Communications Act, 18 U.S.C. §§2701-2711, dealing with access to stored wire and electronic communications and transactional records. The simple-sounding prohibitions of these statutes mask some complicated issues, and the intersection between them is a complex, often convoluted area of the law. Both statutes contain extensive provisions dealing with the powers of and limitations on law enforcement and other governmental agencies in this arena.

The Wiretap Act applies to “any aural transfer” made using wire, cable or other like connections operated by a person engaged in providing such facilities for transmission of interstate or foreign communications or communications, or affecting interstate commerce, 18 U.S.C. §2510(1). It applies to any oral communication uttered by a person exhibiting a reasonable expectation that the communication is not subject to interception,

18 U.S.C. §2510(2). It now also applies, by virtue of ECPA, to electronic communications transmitted by a wire, radio, electromagnetic, photoelectric or photooptical system affecting interstate commerce. 18 U.S.C. §2310(12). The central prohibition of the Wiretap Act is on the "interception" of a wire, oral or electronic communication and on the knowing disclosure or use of such an intercepted communication, 18 U.S.C. §2511(1). Also prohibited are intentional disclosure or use of such intercepted communications, 18 U.S.C. §§2511(c), 2511 (d), 2511(e).

Interception, disclosure and use are permitted under a number of circumstances described in the statute. Switchboard operators and operators of communication service providers may do so where necessarily incident to providing service or protecting their rights or property, 18 U.S.C. §2511(2)(a)(i). Persons acting under color of law may do so where they are parties to the communication or have the consent of a party to the communication, 18 U.S.C. §2511(2)(c). Persons who are parties to a communication may intercept a communication where their purpose is not criminal or tortuous under federal or State law, 18 U.S.C. §2511(2)(d). Pen registers and trap or trace devices are permitted by the statute, 18 U.S.C. §2511(2)(h)(i).

The Stored Communications Act makes it unlawful to obtain, alter or prevent access to a wire or electronic communication in electronic storage by accessing an electronic communications service facility without authority to do so or in a way that exceeds authorization given, 18 U.S.C. §2701(a). These prohibitions do not apply to conduct authorized by the service provider or user, 18 U.S.C. §2501(c).

Both statutes impose criminal liability, and both also create a civil remedy. The Wiretap Act permits a person whose communication has been intercepted, disclosed or intentionally used in violation of the Act to sue for declaratory relief, injunctive relief, damages, plus reasonable attorneys' fees, 18 U.S.C. §2520. Recoverable damages consist of either actual damages and any profits made by the violator as a result of the violation or the greater of $100 per

day for each day of violation or $10,000, *Id.* Service providers, subscribers or others aggrieved by a violation of the Stored Communications Act may also sue for declaratory relief, injunctive relief, damages and reasonable attorneys' fees. Recoverable damages consist of actual damages and any profits made by the violator as a result of the violation , but in no case less than $1,000, *Id.* In addition, the Stored Communications Act authorizes awards of punitive damages (not available under the Wiretap Act), *Id.* Interrelated and time-compacted violations do not result in multiplication of the statutory damages, however, and the District Court has discretion to refuse to allow such damages at all, *Dorris v. Abscher,* 179 F.3d 420, 427-430 (6th Cir. 1999).

Illinois Personnel Records Review Act

The Illinois Personnel Records Review Act, 820 ICLS §40/1 *et seq*. creates the following employee rights: (1) the right to review employee personnel records during employment and for up to one year thereafter upon seven (and in some cases fourteen) days' notice, 820 ICLS §40/2; (2) the right to obtain copies of those records, 820 ICLS §40/3; (3) the right to exclude in judicial and quasi-judicial proceedings any personnel record "information" that has been intentionally withheld after a request, 820 ICLS §40/4; (4) the right to have a statement explaining the employee's position included in the records and in releases of those records to a third party, 820 ICLS §40/6; (5) the right to expunge personnel records containing false information where they have been knowingly placed in the records, 820 ICLS §40/6; (7) limitations on the right of an employer to gather and record information concerning certain non-employment activities, 820 ICLS §40/9; (8) a right to have disciplinary records more than four years old deleted from disclosures to third parties, 820 ICLS §40/8; and (9) a right to written notice of the disclosure of any disciplinary record to a third party, to be given at or before the time the disclosure is made, 820 ICLS §40/7. This panoply of rights is so extensive that any one of them is a potential trap for the unwary or careless employer.

The prohibition on employer gathering of information on certain non-employment activities has never been the subject of a reported decision. The provision prohibits an employer from gathering or keeping records on "an employee's associations, political activities, publications, communications or nonemployment activities" without written employer consent, 820 ILCS §40/9. It does not apply to (a) activities on the employer's premises or during the employee's working hours that interfere with the performance of the employee's duties; (b) activities, whenever and wherever occurring, which constitute criminal conduct or may reasonably be expected to harm the employer's property, operations or business; and (c) activities which could by the employee's action harm the employer's business. 820 ILCS §40/9.

Duty to Exhaust Administrative Remedies. The remedy provision of the statute, 820 ICLS §40/12, requires that before the employee may initiate suit on an alleged violation, he or she must first file a complaint with the Illinois Department of Labor. Under the statute, the Department is called upon to "attempt to resolve the complaint by conference, conciliation, or persuasion." The statute provides that only where this has failed and the Department has not filed suit may the employee may file an action in Circuit Court. *see Park v. City of Chicago,* 297 F.3d 606, 89 FEP Cases 698 (7th Cir. 2002)(not deciding issue but affirming District Court's decision to that effect on another ground). There are no decisions addressing whether the employee may go to court with a complaint where the Department concludes that there has been no violation; the language of the statute is not clear. On the one hand, a finding of a violation is explicitly a prerequisite for a suit by the Department, and not for the employee. On the other hand, the exhaustion provision calls for the efforts by conference, conciliation or persuasion to have "failed."

Searches, Surveillance, Monitoring, Eavesdropping and Accessing of Technology Tools Used By Employees

In a number of the areas described below, one or more of the statutes described above may come into play, along with others mentioned below. Covered here are the privacy issues associated with surveillance of employees, monitoring and recording employee telephone use, accessing employee e-mail, searches of employee offices, and searches of employee computers.

Employee Telephone Calls

Employers who listen in on employee telephone calls must consider both the federal and State laws dealing with such conduct, as well as the common law invasion of privacy tort.

Federal Wiretap Act

Listening in on or recording an employee telephone call constitutes an interception of an oral communication or wire communication under the Wiretap Act—wiretaps were the original target of the statute. Employers may listen in on and record employee telephone conversations if they have secured employee consent (express or implied) or if they come within the "extension telephone exemption."

Wiretap Act Elements. "Intercept" is defined in the statute as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). Overhearing a telephone communication is not an "interception," *United States v. McLoed,*493 F.2d 1186 (7th Cir. 1974)(no interception where government agent overheard conversations because agent did not use any electronic, mechanical or other device to hear the communication); *see Wesley College v. Pitts,* 974 F.Supp. 375, 13 IER Cases 355 (D. Del. 1997)(glimpsing at e-mail on computer screen was not an "interception").

Voice Mail Messages. Listening to a stored voice-mail recording does not normally constitute an "interception." First, the person making a voice mail recording effectively consents to being

recorded by leaving the recorded message, *Payne v. Norwest Corp.,* 911 F.Supp. 1299, 79 FEP Cases 1293 (D. Mont. 1995) *aff'd* 113 F.3d 1079 (9th Cir. 1997). Second, as discussed below with respect to e-mail messages, an "interception" under the Wiretap Act can occur only with respect to a communication that is "in transit," e.*g., Wesley College v. Pitts,* 974 F.Supp. 375, 13 IER Cases 355 (D. Del. 1997)(collecting cases). Only the more limited restrictions of the Communications Storage Act apply to communications after they have been completed. Questions can arise with respect to voice mail recordings, however, when they are forwarded to persons other than the intended recipient, calling into question the scope of the consent, and where the eavesdropper listens to the message before the intended recipient does, during which time the communication has not been completed.

Consent Defense. The consent defense is established by 18 U.S.C. §2511(2)(d): "It shall not be unlawful under this chapter for a person not acting under color of law 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 tortuous act in violation of the Constitution or laws of the United States or of any State." The consent may be express or implied, clearing the way for monitoring and recording programs that are disclosed to employees and for which they sign consents or which operate with posted notices.

The courts are not expansive in recognizing consent beyond what has been expressly given. In *Watkins v. L.M. Berry & Co.,* 704 F.2d 577 (11th Cir. 1983), the court observed that such consent is not to be "cavalierly implied," citing case law holding that knowledge of the capability of monitoring alone is not a sufficient basis on which to imply consent. The court held that a consent could be limited. In *Watkins*, the employer had a system set up for monitoring sales people's calls to enable review to improve sales techniques. The supervisor listened in to a telephone call that turned out to be a personal call between the plaintiff and a friend in which they discussed a job interview plaintiff had been on recently. The court noted that the policy, to which the employee

impliedly consented, indicated that personal calls would not be monitored, and as soon as the personal nature of a call became clear, it would not be monitored.

Deal v. Spears, 780 F.Supp. 618, 7 IER Cases 191 (W.D. Ark. 1991) *aff'd* 980 F.2d 1153, 8 IER Cases 105 (8th Cir. 1992) held that recording from the employer's extension telephone on the same line was not consented to. A threat to put in a pay telephone or monitor employee telephone calls could not support a consent defense because the employer monitored and recorded the telephone calls principally in the hope that the employee would make an admission of complicity in a theft—a hope inconsistent with the idea that the employee knew of and therefore consented to the monitoring.

"Not For Criminal or Tortuous Purpose" Requirement. Where consent has been given, such as when one party to the communication is recording the conversation, the consent provision still requires that the interception be for a lawful purpose. A number of state statutes go beyond the federal law requirement of consent by one party to a communication to recording of the communication. The court in *Payne v. Norwest Corp.,* 911 F.Supp. 1299, 79 FEP Cases 1293 (D. Mont. 1995) *aff'd* 113 F.3d 1079, 79 FEP Cases 1303 (10th Cir. 1997) explained that this does not mean that the extension telephone exemption is not available without two-party consent. The court explained that the exemption is lost where the *purpose* is criminal or tortuous under State law, not when the same *act* is tortuous under State law.

In *Thomas v. Pearl,* 998 F.2d 447 (7th Cir. 1993), the recording was made by a party to the telephone conversation, so one-party consent was not an issue. The plaintiff claimed that the recording was an invasion of privacy under Illinois law. The gist of the plaintiff's concern was not with the recording of the conversation, the court concluded that the intrusion upon seclusion tort could not defeat the consent defense. The subject matter on which publication was made was a matter of public interest, so the tort of publication of private facts could not apply, either. Thus, the consent defense was found to be sufficient.

Extension Telephone/Ordinary Course of Business Exemption. The "extension telephone" exemption is contained in the definition of the "electronic, mechanical or other device," use of which is required to run afoul of the Wiretap Act. The statute provides that it does not include telephone equipment furnished by a telephone service provider in the ordinary course of its business or furnished by the subscriber or user for connection to the telephone facilities *and* used by the subscriber or user in the ordinary course of its business. 18 U.S.C. §2510(5)(a). This provision of the statute also extends the exemption to equipment used by the telephone service provider in the ordinary course of its business and to equipment used by a law enforcement officer in the ordinary course of his duties.

Consent Not Required For Extension Telephone/Ordinary Course of Business Exemption. The court in *Briggs v. American Air Filter Co.,* 630 F.2d 414 (5th Cir. 1980) concluded that the extension telephone exemption must be applicable to at least certain situations in which the employer has not notified the employee of the monitoring or recording of telephone calls. Otherwise, the court reasoned, the exception would be redundant of the consent defense. Thus, while consent may be given by employees to recording of both business and personal telephone calls, the business extension exception operates without regard to consent, *Watkins v. L.M. Berry & Co.,* 704 F.2d 577 (11th Cir. 1983).

Equipment Used Must Be Telephone Equipment. Equipment that has been installed specially for the purpose of monitoring or recording calls may not qualify for this exemption. In *Williams v. Poulos,* 11 F.3d 271 (1st Cir. 1993), the court concluded that the monitoring and recording system (which relied on attaching alligator clips to a designated extension line) could not be considered to be a "telephone or telegraph instrument, equipment or facility, or a component thereof." This was something different, the court found, from a telephone extension, a console installed by a telephone company, or a monitoring device installed by a telephone company. On the other hand, in *Epps v. St. Mary's Hospital of Athens, Inc.,* 802 F.2d 412 (11th Cir. 1986), the court emphasized that a recording device hooked up to an EMS dispatch console, which automatically recorded all incoming calls and

which could record outgoing calls when a button was depressed, was not the "intercepting device." The dispatch console (telephone equipment) was the intercepting device, not the recorder. But this observation in *Epps* was later disapproved of by the court in *Deal v. Spears,* 980 F.2d 1153, 8 IER Cases 105 (8th Cir. 1992).

Ordinary Course of Business Requirement. Determining when monitoring is "in the ordinary course of business" not has not been a simple matter. A classic case of what is ordinary course of business was *James v. Newspaper Agency Corp.* 591 F.2d 579, 18 FEP Cases 1547 (10th Cir. 1979), where the employer's program was for training purposes and to protect employees from abusive callers and employees were notified of it and did not protest.

The overlap between a "reasonable expectation of privacy" in telephone calls and the "ordinary course of business" was discussed by the court in *Briggs v. American Air Filter Co.,* 630 F.2d 414 (5th Cir. 1980): "If the common experience in this country is that under certain circumstances, communications made on office telephones are not listened to by employers or their agents, it could not be said that an act of listening-in to such a conversation is 'in the ordinary course of business.'"

Personal-Business Conversation Distinction. In *Briggs*, the court focused on what it saw as the compelling reasons for the supervisor to listen in on the conversation. The employee had a friend who worked for a competitor and the supervisor was concerned that he was disclosing the company's confidential information to his friend. Although there was no policy justifying the eavesdropping the supervisor did, the court concluded that if there was any case in which listening to an employee's telephone call without his consent would be justified from a business standpoint, this was it. Thus, "when an employee's supervisor has particular suspicions about confidential information being disclosed to a business competitor, has warned the employee not to disclose such information, has reason to believe that the employee is continuing to disclose such information, and knows that a particular phone call is with an agent of a competitor, it is within

the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed." The three factors cited by the court in support of its conclusion were (1) the employee conceded that the discussion was a business call, not a personal call; (2) the listening-in was for a limited purpose and time; and (3) there was no general practice of surreptitious monitoring of employee telephone calls.

In *Watkins v. L.M. Berry & Co.,* 704 F.2d 577 (11th Cir. 1983), the court focused on the fact that the call was of a personal nature to conclude that listening to it was not "in the ordinary course of business." The intercepted call was between plaintiff and a friend, and in the call they discussed a job interview plaintiff had with a prospective new employer. While the subject was certainly a matter of interest to her present employer, the court observed, the employer had no "legal interest" in the call because she was an at-will employee. The employer might just as well have an interest in whether the plaintiff had "nice" friends, said the court—the subject of the call was not in the ordinary course of "business" for the employer.

The court in *Epps v. v. St. Mary's Hospital of Athens, Inc.,* 802 F.2d 412 (11th Cir. 1986) followed the *Watkins* personal/business distinction, finding in that case that the recording was proper because it concerned a matter within the legal interest of the employer. In *Epps,* the EMS recording system recorded all incoming calls, but only recorded outgoing calls when a button was depressed. The plaintiff was on an outgoing telephone call discussing supervisors and making "scurrilous" comments about them when another employee who had been listening to the call went to the next room and began recording the call. The court found that this was no personal call, in that it occurred during business hours over a business telephone. "Certainly the potential contamination of a working environment is a matter in which the employer has a legal interest," said the court.

Continued Listening To Personal Conversation Prohibited. The court in *Watkins* also said that an employer may listen to a

conversation only long enough to determine whether it is personal, and when it is, must stop monitoring or recording or it goes beyond the scope of the exemption. Similarly, the court in *Fisher v. Mt. Olive Lutheran Church, Inc.,* 207 F.Supp.2d 914 (W.D. Wis. 2002) held that there were jury questions where church staff listened in on a cordless extension telephone counseling session conducted by its youth minister with a caller who discussed homosexual experiences. The evidence about what the plaintiff said was in dispute, but his end of the conversation was being conducted from a private office with the door was closed. After hearing a sexually graphic conversion on the extension telephone, church staff continued listening after the personal nature of the conversation was clear. The court questioned whether there was a sound business reason for church staff to have continued listening in, regardless of the contents, and concluded that trial on the question was required.

Deal v. Spears, 780 F.Supp. 618, 7 IER Cases 191 (W.D. Ark. 1991) *aff'd* 980 F.2d 1153, 8 IER Cases 105 (8th Cir. 1992) held that recording of some twenty-two hours of mostly personal conversations from the employer's extension telephone went well beyond the boundaries of the ordinary course of business.

Illinois Electronic Eavesdropping Act

The Illinois eavesdropping statute, 720 ILCS §5/14-1 *et seq.,* covers listening in on and recording oral conversations as well as intercepting, retaining or transcribing electronic communications. The prohibition is on operating an eavesdropping device, which is "any device capable of being used to hear or record oral conversation or intercept, retain or transcribe electronic communications…" 720 ILCS §5/14-1. The essential offense prohibited by the statute is "…using an eavesdropping device for the purpose of hearing or recording all or any part of a conversation" or intercepting, retaining or transcribing electronic communications without the consent of *all* the parties to the conversation or communication, 720 ILCS §5/14/2(a)(1).

The statute contains many exemptions, a number of which regulate conduct by police officers, and several of which could be important in the employer-employee context:

Recording or listening to consumer "hotlines" by manufacturers or retailers of food and drug products is permitted, but recordings must be destroyed or turned over to law enforcement after 24 hours, 720 ILCS §5/14-3(f).

Recording a conversation by a party to the conversation who has a reasonable suspicion that another party to the conversation is about to commit or has committed a criminal offense against the individual or a family member for purposes of obtaining evidence of the crime, 720 ILCS §5/14-3(i).

Telephone monitoring by an entity engaged in marketing or opinion research or by an entity engaged in telephone solicitation, to record or listen to employee conversations when the purpose is service quality control, education or training, or internal research related to the business and with the consent of at least one of the participants in the conversation, 720 ILCS §5/14-3(j). No such recording may be furnished to law enforcement or used in any inquiry, investigation, administrative proceeding or judicial proceeding or divulged to a third party. *Id.* Upon determining that a conversation monitored or recorded does not relate to the applicable business subject, the recording or listening must be terminated and the recording destroyed as soon as possible. *Id.* Notice to employees, including prominent signage in the workplace is required, *Id.* Affected employees must be provided access to personal telephone lines. *Id.*

Violations of the statute may be redressed by civil suit as well as criminal prosecution. Injunctive relief, compensatory damages and punitive damages may be awarded, 720 ILCS §5/14-6. However, under 720 ILCS §5/5-4(a), corporate civil liability for conduct violating the statute, which is felonious, may be imposed only where it has been authorized, requested, demanded or performed by the board of directors or a "high managerial agent"

of the employer, *Morris v. Ameritech Illinois,* 337 Ill.App.3d 40, 271 Ill.Dec. 411, 785 N.E.2d 62 (1st Dist. 2003)(finding employee failed to make requisite showing of corporate direction for alleged breach of rights under the statute).

The "two party consent" requirement appears to significantly expand the scope of privacy protection provided by the federal statute, but this can be misleading. The Illinois cases are crystal clear that "eavesdropping" does *not* include situations in which the recording of a telephone call or other conversation is made by a party to the communication, *People v. Herrington,* 163 Ill.2d 507, 206 Ill.Dec. 705, 645 N.E.2d 957 (1995); *People v. Beardsley,* 115 Ill.2d 47, 104 Ill.Dec. 789, 503 N.E.2d 346 (1983); *Thomas v. Pearl,* 998 F.2d 447 (7th Cir. 1993); *People v. Rodriguez,* 289 Ill.App.3d 223, 223 Ill.Dec. 807, 680 N.E.2d 757 (2d Dist. 1997); *People v. Bennett,* 120 Ill.App.3d 144, 75 Ill.Dec. 544, 457 N.E.2d 986 (5th Dist. 1983). **NOTE: Amendments to the statute have since been held by the Illinois Supreme Court to modify by implication the definition of "eavesdropping" to include recording by parties to the conversation, invalidating this contstruction.**

The reasoning behind this construction is that the person making the communication does not seek to keep the communication secret from the person to whom it is directed, and so there is no invasion of a privacy interest in a recording made by a party to the communication. The information could be just as easily conveyed by the recipient without a recording. "Eavesdropping," which appears in the title of the statute, normally refers to someone *outside* the communication surreptitiously listened to and/or recorded the communication. In such cases, the outsider may do so only with the consent of both parties to the communication. **NOTE: Amendments to the statute have since been held by the Illinois Supreme Court to modify by implication the definition of "eavesdropping" to include recording by parties to the conversation, invalidating this contstruction.**

However, where a third party standing next to a participant in the conversation is able to hear both ends of a telephone conversation

by listening in the earpiece of the telephone with the party to the conversation, this is not eavesdropping because no eavesdropping device has been used, *People v. Giannopoulos,* 20 Ill.App.3d 338, 314 N.E.2d 237 (1st Dist. 1974). When the unaided human ear can hear what has been said on the telephone, the statute does not apply. Similarly, hearing a telephone conversation through a switchboard does not constitute eavesdropping, *People v. Bennett,* 120 Ill.App.3d 144, 75 Ill.Dec. 544, 457 N.E.2d 986 (5th Dist. 1983), nor is listening on an extension, unless the extension's mouthpiece has been disabled, which turns the extension telephone into a listening device, *People v. Gervasi,* 89 Ill.2d 522, 61 Ill.Dec. 515, 434 N.E.2d 1112 (1982).

Common Law Invasion of Privacy

The recitation of types of conduct that can constitute invasion of privacy in *Lovgren v. Citizens First National Bank of Princeton,* 126 Ill.2d 411, 128 Ill.Dec. 542, 534 N.E.2d 987 (1989) includes "eavesdropping by wiretapping." This provides no insight into what forms of wiretapping might be considered an intrusion upon seclusion, but suggests that in certain cases listening in on or recording telephone conversations would be actionable under the tort. The courts could decide that the statute (perhaps together with any additional protection provided by the federal statute) defines what constitutes an intrusion upon seclusion.

In *Thomas v. Pearl,* 998 F.2d 447 (7th Cir. 1993), the court concluded that where the gist of the harm complained of is not the intrusiveness of the conduct, intrusion upon seclusion would not apply. In that case, the court concluded that since the telephone recorded conversations themselves were not intrusive (the plaintiff spoke to the defendant voluntarily), the harm flowed from the publication of the conversations , and thus intrusion upon seclusion would not apply. Since the subject of the conversation that was publicized, recruiting abuses by a public university in attempting to sign a high school athlete (the plaintiff), was a matter of public interest, the publication of private facts invasion of privacy cause of action did not apply either.

Two cases have addressed the intrusion upon seclusion tort in the context of telephone surveillance in employee investigations conducted by telephone companies with respect to their own employees. In *Schmidt v. Ameritech Illinois,* 329 Ill.App.3d 1020, 263 Ill.Dec. 543, 768 N.E.2d 303 (1st Dist. 2002), an employee of the telephone company was investigated by management when he falsely denied having gone on a vacation trip while on disability leave. The investigation extended to a review of his personal telephone records as well as the telephone records of his wife's employer, confirming the employer's information that the employee had indeed taken the vacation trip. The defense argued that the first element of the tort was not satisfied because the review of telephone records was "authorized" on a number of grounds: the right of an employer to investigate its employee; the right of an employer to review its own records; and the right recognized by federal telecommunications law of a telephone service provider to protect its rights or property. Of the three, the court found the last to be the most compelling, citing the Wiretap Act's exemption for telephone service providers, 18 U.S.C. §2511(2)(a)(i): "It shall not be unlawful under this chapter for…an officer, employee or agent of a wire to electronic communication services, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication…while engaged in any activity which is a necessary incident to…the protection of the rights or property of the provider of that service…" The court found that in conducting its investigation, the telephone company was protecting its "rights and property," which included its monetary resources.

The court went on to conclude that the plaintiff had failed to satisfy the damage element of intrusion upon seclusion because the injury which caused his anguish and suffering was not the prying into his telephone records, but the termination of his employment. The court noted that the employee would have been terminated based on information secured by the employer prior to the investigation into telephone records. In addition, the court was not convinced that the injury complained of by the plaintiffs, being upset, depressed, and crying, was sufficient to establish mental anguish or suffering. Under Illinois law, the court said, medical

care, inability to sleep or work, or loss of reputation and integrity in the community must be shown to prove mental anguish.

In *Morris v. Ameritech Illinois,* 337 Ill.App.3d 40, 271 Ill.Dec. 411, 785 N.E.2d 62 (1st Dist. 2003), the court followed *Schmidt* in dismissing a claim based on review of telephone records. The court also dismissed a claim for eavesdropping on a telephone conversation against the telephone company because, it held, the vicarious liability applicable to the eavesdropping statute pre-empted the common law *respondeat superior* liability standards in an invasion of privacy tort claim based on eavesdropping.

Reviewing the elements of the tort of intrusion upon seclusion to the eavesdropping setting suggests some additional issues likely to arise when a telephone eavesdropping claim is made under the intrusion upon seclusion tort. The act of eavesdropping itself, when done by someone not a party to the communication that is being monitored or recorded, represents an "unauthorized intrusion or prying." Under this element, a court might (or might not) conclude that to be unauthorized, monitoring or recording must be in violation of the Illinois statutory standards, and perhaps also the federal standards.

Turning to the second element, the court might conclude that only conversations that concern intensely personal matters, or that do not concern business matters, are properly protected by the tort. Otherwise, the intrusion would not be "offensive or objectionable to a reasonable person." Alternatively, a court could conclude that the very act of listening in or recording a conversation by someone who is not a party to it is offensive and objectionable. The same problem is raised by the third element, which requires that the matter upon which the intrusion occurs be "private": this might require that the subject of the communication be private, or the exclusive nature of telephone calls might make the conversation "private" regardless of the subject.

Surveillance of Employees

One recent decision upholds The NLRB's determination that an employer's installation of numerous hidden cameras to monitor employee conduct on the job is a mandatory subject of bargaining under the National Labor Relations Act, *National Steel Corp. v. N.L.R.B.,* 324 F.3d 928 (7th Cir. 2003)(employer required to bargain with the union over the installation of cameras). This position was first articulated by the Board in *Colgate-Palmolive Co.,* 323 NLRB 515 (1997). However, this does not mean that invasion of privacy claims in union workplaces are invariably pre-empted by §301 of the LMRA. *Compare Matter of Amoco Petroleum Additives Co.,* 964 F.2d 706 (7th Cir.1992)(claim based on placing investigative camera at entrance to women's locker room pre-empted) *with Schmidt v. Ameritech Corp.,* 115 F.3d 501 (7th Cir. 1997)(claim for monitoring residential telephone calls not pre-empted)*; Keehr v. Consolidated Freightways of Delaware, Inc.,* 825 F.2d 133 (7th Cir.1987)(claim based on remarks about sexual activities of employee's wife not pre-empted).

Brewers and Malters, Local Union No. 6 v. N.L.R.B., --- F.3d ---, 2005 WL 1560399 (D.C. Cir. 2005) approved a board ruling finding that the installation of concealed cameras on the brewery roof, which was used for both work purposes and as an information break area, constituted unilateral action concerning a mandatory subject of bargaining. In that case, management argued that the legitimate security purposes of the system installed made bargaining unworkable, but the court agreed with the board that the union and company could bargain over the general requirements for the use of such devices. The court overturned the board's decision to deny relief to the individual employees because they were videotaped while engaged in conduct amounting to just cause for discharge. The court concluded that a cease-and-desist order did not satisfy the board's "complete relief" standard.

Many of these cases arise under the tort of invasion of privacy. They may be instructive with respect to principles that will govern when this tort is applied to less traditional forms of employee monitoring, as well as the scope of an employee's "reasonable expectation of privacy."

In *Johnson v. K-Mart Corp.,* 311 Ill.App.3d 573, 243 Ill.Dec. 591, 723 N.E.2d 1192 (1st Dist. 2000), the court found that intrusion upon seclusion was possible in connection with an undercover investigation of employees conducted for the employer by a private investigator. The employer had retained an investigator to become an employee in order to investigate theft, vandalism, sabotage, which had been experienced at the facility, and possible sale and use of drugs by employees. The investigator, who was hired as a janitor, made regular written reports concerning the employees. These reports, in addition to addressing the subjects of the investigation, also dealt with personal aspects of the employees' lives such as family matters, romantic interests/sex lives, future employment plans, complaints about the employer, and various personal matters (medical information, personal activities).

The court found that this could constitute intrusion upon seclusion. While the information the investigator obtained was all volunteered by the workers, it was obtained by deception, and not just at work but also at social functions of the employees. This raised a question about whether the intrusion was authorized. The employer continued to receive reports on personal matters without instructing the investigator to confine his reports to the matters under investigation. The court found this to be an offensive and objectionable intrusion concerning private matters.

The court went on to find that the same events presented a jury question on whether the employees had an actionable claim for publication of private facts. The court concluded that a "public" under this tort could be a limited one, if it was a "public" with which the plaintiff has a special relationship. The court found that the employer could represent such a "public."

On the other end of the spectrum, the investigators won summary judgment in *Hall v. InPhoto Surveillance Co.,* 271 Ill.App.3d 852, 208 Ill.Dec. 251, 649 N.E.2d 83 (4th Dist. 1995). There, the plaintiff was expected to file a malpractice claim because alleged errors in a first operation required a second operation. The investigators positioned themselves on public property with a

video camera, although it did not function, at a point that provided an unobstructed view of the bedroom of her rural home. There were no curtains on the windows. No videotape was actually taken, there was no trespass on plaintiff's property, and the undisputed evidence contradicted the allegations of the complaint that the investigators entered Plaintiff's property and took photographs through a bedroom window. Under these circumstances, without deciding whether the tort would be recognized, the court concluded that summary judgment on the claim for intrusion upon seclusion was proper. It quoted the trial judge's comments, including his observation that "An individual who seeks to recover damages for personal injuries should not be surprised that some investigation of her claim will be undertaken."

In *Benitz v. KFC National Management Co.,* 305 Ill.App.3d 1027, 714 N.E.2d 1002, 239 Ill.Dec. 705 (2d Dist. 1999), the court had no difficulty in finding intrusion upon seclusion where the plaintiffs' co-workers poked holes in the ceiling of the women's bathroom, viewed plaintiffs disrobing and using the restroom facilities, took pictures and discussed their private body parts.

In *Schiller v. Mitchell,* 357 Ill.App.3d 435, 828 N.E.2d 323, 293 Ill.Dec. 353 (2d Dist. 2005), the court found no intrusion on seclusion where the defendants installed a videotape camera that was pointed at the plaintiffs' garage, driveway, side-door area and backyard as part of an ongoing neighborhood feud between the two. The court pointed out that a passerby on the sidewalk or tree trimmer could see what the camera filmed, albeit from a different angle, holding that a camera pointed at a publicly visible location was not an intrusion on seclusion.

Employee surveillance activity using electronic tools can also run afoul of the Wiretap Act. In *Dorris v. Abscher,* 179 F.3d 420, 425 (6th Cir. 1999) the court found a violation when a supervisor placed a hidden tape recorder in a common employee office and transcribed conversations among them in which they criticized him. The court found that employees had an objectively and subjectively reasonable expectation of privacy in their small, isolated common office area. "[T]he frank nature of the

employees' conversations makes it obvious that they had a subjective expectation of privacy," said the court.

In *Bowyer v. Hi-Lad, Inc.,* 216 W.Va. 634, 609 S.E.2d 895 (2004), the court upheld a $500,000 judgment against an employer for its undisclosed use of an extensive video and audio monitoring system in the public areas of the hotel in violation of a state eavesdropping statute similar to the Illinois eavesdropping statute. The court found that although the camera and hidden microphones were placed in public spaces, the eavesdropping was nevertheless in violation of a reasonable expectation of privacy.

Employee Office Searches

With these cases, the governing legal principles are those established by the tort of intrusion upon seclusion and the Fourth Amendment protections of public employees, which are triggered by a finding that an individual has a reasonable expectation of privacy in an office.

Fourth Amendment Public Employee Protection

As noted above, *O'Connor v. Ortega ,* 480 U.S. 709 (1987) recognized at least the possibility of employee privacy interests in employee desks and file cabinets. The opinion also acknowledged that actual office practices could mean that the employee had no "reasonable expectation of privacy" necessary to secure Constitutional protection. In *Sheppard v. Beerman*, 18 F.3d 147 (2d Cir. 1994)(search of law clerk's office, desk and file cabinets), the court relied on the "open" context of the office—in that case the office of a court clerk in a judge's chambers—to conclude that there was no reasonable expectation of privacy. This meant that the search did not violate Fourth Amendment standards.

The court in the criminal case of *United States v. Simons,* 206 F.3d 392 (4th Cir. 2000) found that where the employee had an office he did not share, he had a reasonable expectation of privacy. However, this is only the first step of the analysis with respect to a

public employee Fourth Amendment question. Citing *O'Connor,* the court in *Simons* found that a warrantless search was proper when the employer conducts a search as part of an investigation of work-related misconduct so long as the search is reasonable at its inception (i.e., founded on reasonable cause to suspect that the search will turn up evidence of work-related misconduct) and the search is limited to the objectives of the search and not excessively intrusive in light of the nature of the suspected misconduct. In that case, the office search was conducted to retrieve a hard drive on the employee's computer after a remote check of the hard drive had shown that it would contain evidence of downloaded child pornography. The court also held in *Simons* that the potential for criminal charges did not deprive the public employer of the right to conduct the search as a search for evidence of work-related misconduct.

Even where there is a reasonable expectation of privacy, a search may be justified. Where the search seeks proof of criminal activity, probable cause and where applicable, a search warrant , will be required. But where it is in pursuit of evidence of employee misconduct, as distinguished from a search for evidence of criminal activity, the search need only satisfy a broad "reasonableness" standard, even if such evidence turns up. In *Gossmeyer v. McDonald,* 128 F.3d 481 (7th Cir. 1997), the employee was a child protective officer and child pornography was found in her file cabinet. The court found the reasonableness standard applied despite the presence of other law enforcement officials at the search. The search was reasonable because, at its inception, although based on a corroborated anonymous tip, the tip from someone claiming to be a co-worker showed sufficient signs of reliability, such as specific identification of the location where the items could be found. The ultimate scope of the search did not exceed what was reasonably necessary.

Intrusion Upon Seclusion Tort

The U.S. District Court in *Hoth v. American States Insurance Co.,* 735 F.Supp. 290 (N.D. Ill. 1990) brushed aside assertions that an employer's search of an employee's desk could constitute intrusion upon seclusion. The company investigator who searched the plaintiff's desk, the court said, had authority to search the office,

file cabinet and desk, and he had not alleged anguish and suffering as a result of the search, only as a result of the termination of his employment.

One compelling argument the employer has in the case of any office search is that the property being searched *belongs to the employer*. It is indeed difficult to see how such a search could be found to be unauthorized unless the employer had published a policy restricting the scope of office searches or issued locks and keys, authorizing employees to retain personal items in certain spaces, such as employee lockers.

On the other hand, in a criminal case, *United States v. Anderson,* 154 F.3d 1225 (10th Cir. 1998), the court found that, *as against the government*, the officer of a private corporation had a reasonable expectation of privacy in his office. It further concluded that he could have such an expectation in other areas of the company's facilities where all of the relevant circumstances suggested that he had taken steps to ensure privacy in the space in question.

One case illustrating how intrusion upon seclusion could arise in the context of an office search is *Doe v. Kohn, Nast & Graf ,P.C.,* 862 F.Supp. 1310 (E.D. Pa. 1994). In that case, the HIV-positive plaintiff claimed, *inter alia,* that his office had been searched, personal medical documents obtained and information learned from them disseminated. The court noted that a search of an employee's workplace done in a manner that reveals matters unrelated to the workplace can represent an invasion of privacy. There was sufficient circumstantial evidence of the search to defeat summary judgment in that case.

In *Bryan v. KTIV Television,* 868 F.Supp. 1146, 67 FEP Cases 1602 (N.D. Iowa), the employee failed to prove intrusion upon seclusion based on an office search sufficiently to survive summary judgment. The employee in that case, although possessing some evidence that his desk had been searched, could not show who had conducted the search. As a result, he had no evidence tying management or any authorized agent of the

employer to the search. The court concluded that the employee did not, in any event, have a reasonable expectation that the employer would not search his desk or office area for employer-owned documents. The furniture belonged to the employer, and the employee acknowledged that he assumed that if we was on vacation other employees might go into his office to retrieve documents.

Computer and E-Mail Searches

The question is whether browsing through the e-mail messages an employee has sent and received at work represents an invasion of the employee's privacy rights. The answer is, generally not. Office telephone systems and equipment, like e-mail systems and office computers, are owned by the employer. Switchboards, like servers, provide an obvious opportunity for employers to eavesdrop on employees' communications. Nevertheless, the courts have not typically applied the privacy protections given to telephone calls to e-mail communications.

Constitutional Protections of Public Employees

The balancing test of *Ortega* has resulted generally in determinations that the government is entitled to search employee computers. In *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the court found no reasonable expectation of freedom from search of the CIA employee's computer for downloading of pornography where employer policy stated that it would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." *Accord, United States v. Thorn,* 375 F.3d 679 (8th Cir. 2004)(employer's published policy on lack of privacy in computer and reserving right to search precluded any reasonable expectation of privacy); *United States v. Angevine,* 281 F.3d 1130 (10th Cir. 2002)(no reasonable expectation of privacy where employer had posted warnings disclaiming right to privacy in

electronic information); *United States v. Bailey*, 2003 WL 21705226 (D. Neb. 2003)(collecting cases).

Judge Posner weighed in on this subject in *Muick v. Gkenayre Electronics,* 280 F.3d 741 (7th Cir. Feb. 6, 2002), concluding that while a public employer could create a reasonable expectation of privacy in employer-owned office equipment by furnishing locks for securing private papers, the employer's announcement that it reserved the right to inspect laptop computers provided to employees prevented there from being any reasonable expectation of privacy with respect to the contents of the laptop. Thus, the employer's stated intentions to employees are one crucial element of determining whether there are privacy rights.

In *Leventhal v. Knapek,* 266 F.3d 64 (2d Cir. 2001), the court did hold that an accountant had a reasonable expectation of privacy because of the secure surroundings of his computer and the lack of warnings of the possibility of search. The court concluded: "Leventhal occupied a private office with a door. He had exclusive use of the desk, filing cabinet, and computer in his office. Leventhal did not share use of his computer with other employees in the Accounting Bureau nor was there evidence that visitors or the public had access to his computer. We are aware that 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." Construing the evidence in favor of Plaintiff at the summary judgment stage, the court found that there could be a reasonable expectation of privacy because "we do not find that the DOT either had a general practice of routinely conducting searches of office computers or had placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer."

Similarly, in *United States v. Salina,* 283 F.3d 670 (5th Cir. 2002), the court found a reasonable expectation of privacy in the employee's computer where the employee had a locked private office, the employer had no written policy on computer monitoring use of the computer, which until the events leading to his

prosecution, was not networked. The computer was password protected by the employee and computer technicians of the employer had limited access to it. However, once again the public employer's right to conduct a reasonable search while investigating potential misconduct dispensed with any requirement for a search warrant, and the employer had reasonable cause to believe that it would find evidence of work-related misconduct by conducting the search.

Wiretap Act and Stored Communications Act

The Wiretap Act and Stored Communications Act limit both public and private employers, and both may have direct application to searches of employee e-mail messages.

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the court reviewed an award under both the Wiretap Act and the Stored Communications Act resulting from the government's actions following seizure pursuant to a search warrant of a company's computer. The plaintiff company maintained a bulletin board service on the computer which included e-mail service for 365 subscribers. The District Court found that government personnel had read and deleted private e-mail stored on the BBS. Parsing the arcane linguistic differences between the Wiretap Act and the Stored Communications Act (Electronic Computer Privacy Act), the court concluded that while recovery under the Stored Communications Act was proper, recovery under the Wiretap Act was not.

The e-mails, everyone conceded, were stored communications and recovery for their reading and deletion was proper under the Stored Communications Act. Under that Act, it was unlawful to "alter or prevent access to" any "electronic communication in electronic storage by accessing an electronic communications service facility without authority to do so."

The dispute was over whether the e-mails, which had been sent to the BBS and were waiting to be read should be treated as "electronic communications," that had been "intercepted" in violation of the Wiretap Act, as amended by the ECPA to cover electronic communications. The court found that electronic communications in electronic storage of a computer awaiting delivery are not "electronic communications" that can be "intercepted" while they are awaiting delivery. The e-mails sitting on the BBS computer were in temporary storage incidental to electronic transmission, fitting instead the definition of "electronic storage."

The significance of this arcane distinction for searches of employee e-mail messages was illustrated in *Frasier v. Nationwide Mutual Ins. Co.,* 135 F.Supp.2d 623 (E.D. Pa. 2001). In that case, the employee was an insurance agent and an activist in the agent's association. He called attention to business practices he believed to be illegal and reported them to State authorities. The result was a fine for the underwriter and an agreement to cease the practices. The underwriter was aware of the agent's communications with State authorities. Prompted by this, it issued a general memo warning about "inappropriate communications with State insurance departments, the media and State legislatures."

This battle swirled around changes in business policies that the underwriter had announced, and the agent had drafted a letter for the agent's association suggesting to a competitor of the underwriter that its agents might be willing to join them if the changes went forward. This was intended as a pressure tactic, but management learned about and obtained a copy of the letter. It then searched its e-mail server and found evidence in the agent's e-mail messages that he had sent the letter to at least one competitor. He was fired.

In the ensuing litigation, the agent accused the underwriter of violating the Wiretap Act prohibition on interception of electronic communications. The court concluded that this claim could not stand, because the e-mails that management had accessed had already been delivered. "Retrieval of a message from storage

while it is in the course of transmission is 'interception' under the Wiretap Act; retrieval of a message from storage after transmission is not 'interception' under the Act."

In this case, however, the court also found that there was no violation of the Stored Communications Act, either. The e-mail storage was neither "temporary, intermediate storage…incidental to electronic transmission," nor was it stored "'by an electronic communication service for purposes of backup protection of such communication." The decision suggests that storage for archival purposes or for other reasons unrelated to the communication process is not covered by the statute. It does not state whether this point, or the fact that the storage was no provided by an outside "electronic communication service" was dispositive. The court did not need to consider whether the underwriter had an absolute right to access and read an agent's e-mail messages simply because they were sent through its system, as 18 U.S.C. §2701(c) would suggest, *see Crowley v. CyberSource Corp.,* 166 F.Supp.2d 1263 (N./D. Cal. 2001)(online retailer was not provider because it purchased communications service)

Frasier and *Steve Johnson Games* hold that the Stored Communications Act applies only during the interval between the time when the author of the e-mail sends it and the time when the recipient actually reads it (which can be anything from moments to weeks). Only in that limited period is the message is a "stored communication" the privacy of which is protected in any way by either the Wiretap Act or the Stored Communications Act. Once the e-mail is read, there is no protection, unless perhaps the e-mail is remotely stored.

Frasier was followed and expanded upon by the court in *Borninski v. Williamson,* 2005 WL 1206872 (N.D. Tex. 2005), where the employee's hard drive was copied by security personnel and the hard drive contained e-mail messages that had evidently been received by the employee from a hotmail account. The messages demonstrated that a security certification given by the employee was not complete and accurate. The employee claimed that the employer must have accesses his outside account, since he never

received certain messages produced by the employer in discovery. The court held that this was not a sufficient on which to challenge the sworn statement of the employer's security officer explaining how the materials were obtained.

The court this found no evidence of an unlawful "interception" of an electronic communication. It concluded that materials downloaded to a server of personal computer were not "stored communications" for purposes of the Stored Communications Act. It also concluded that the employee's pre-employment consent was also sufficient to excuse a violation of the statute had one occurred.

In *U.S. v. Councilman,* 373 F.3d 197 (1st Cir. 2004), the court determined that even if the e-mail message was in temporary storage while in transit, the owner of the computer system (in this case, an internet service provider) was permitted to access the e-mail message and use its contents. The court observed that "It may well be that the protections of the Wiretap Act have been eviscerated as technology advances." The decision, which was vacated for hearing *en banc,* was criticized by Senator Leahy, one the authors of the legislation, as contrary to the legislative intent, 2 No. 4 Andrews Privacy Litig. Rep. 13 (2004).

The scope of protection provided for e-mail messages after the Electronic Computer Privacy Act is thus limited to situations like that in *Fischer v. Mt. Olive Lutheran Church, Inc.,* 207 F.3d 914 (W.D. Wis. 2002), where the employer accessed e-mail messages on the employee's hotmail account, correctly guessing his password to gain access, and retrieved personal messages in that manner. This represents extremely limited protection of employee e-mail privacy under the statutes.

Another circumstance in which a violation of the Stored Communications Act, but not the Wiretap Act, can occur as a result of disclosure of e-mail messages is illustrated by *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). In that case, the defendants issued subpoenas to a corporate adversary's Internet Service Provider ("ISP") seeking all e-mail messages. Noting that

there was no subject matter, individual employee or time limitation on the messages sought, the court concluded that the subpoena was invalid, and sanctions were imposed for its issuance. Pursuant to the subpoena, the ISP provided a sample of messages, which consisted of messages unrelated to the litigation, some of which were personal in nature. This all occurred without notice to the corporate party whose e-mail was subpoenaed. The Ninth Circuit concluded that the ISP's disclosure pursuant to a patently invalid subpoena, even if it gave notice of a right to contest validity, was not an "authorized" disclosure under the Stored Communications Act, and gave rise to a claim for damages. It did not, however, come within the Wiretap Act. It was sufficient to constitute a violation of the Computer Fraud & Abuse Act provisions, 18 U.S.C. §1030(a)(2)(C)(g) because it could represent loss of $5,000 or more.

Intrusion Upon Seclusion Tort

Reasonable Expectation of Privacy. No Illinois cases address whether or not an employee's e-mail messages or computer hard drive could represent an intrusion on seclusion. *Fischer,* a federal District Court decision construing Wisconsin law, recognized that a "private place" need not be a geographical place, citing the *Restatement's* recognition of privacy in medical records. Rather, the court concluded, privacy "encompasses a person's private belongings as long as the place these private belongings are intruded upon is one that a reasonable person would consider private." The court concluded that whether accessing the employee's personal e-mail account, by guessing his password, and then reading and printing out his e-mail messages, was highly offensive to a reasonable person, was a question for the jury.

The same does not hold, however, for employer-maintained e-mail systems. In *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 WL 974676 (D. Mass. 2002), citing *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996), the court agreed that even in the absence of a company e-mail policy, employees could not have a reasonable expectation of privacy in their work e-mail once it was communicated to a third person over a system used by the entire office. In *Kelleher v. City of Reading,* 2002 WL 1067442 (E.D. Pa. 2001), on the other hand, where the employee claimed to have

had a reasonable expectation of privacy in her e-mail, the court disagreed because the City had unequivocally reserved its right to inspect the e-mail messages of employees that Plaintiff claimed had been screened and read by defendants. But the court disagreed with *Smyth* and another decision categorically rejecting the possibility that there could be a reasonable expectation of privacy in e-mail messages, *Commonwealth v. Proetto,* 771 A.2d 123 (Pa. Super. 2001).

Implied Consent To Employer Monitoring. Although courts will not imply consent to telephone monitoring or recording under the Wiretap Act from mere knowledge that it is possible to access the communication, *Garrity* holds the exact opposite for e-mail messages in the intrusion upon seclusion context. Citing *McLaren v. Microsoft Corp.,* 1999 WL 339015 (Tex. Ct. App. 1999) with approval: "…any e-mail messages…were first transmitted over the network and were at some point accessible by a third party. Given these circumstances, we cannot conclude that plaintiff, even by created a personal password, manifested—and defendant recognized—a reasonable expectation of privacy in the contents of e-mail messages..." *Accord, Bohach v. City of Reno,* 932 F.Supp. 1232 (D. Nev. 1996) (knowledge by the employee that a voice message would pass through a computer and be stored there was enough for the court to imply consent); *Ali v. Douglas Cable Communications,* 929 F.Supp. 1362, 1380-1381 (D. Kan. 1996).

Monitoring Justified By Business Purposes or Legal Duty. *Garrity* also concludes that any reasonable expectation in privacy of e-mail messages would likely be trumped by the employer's business interests. In that case, the court expressed the view that protection of other employees from workplace harassment, mandated or at least encouraged by State and federal law, would authorize restriction of employee privacy rights.