

PRIVACY IN THE WORKPLACE

Gail E. Mautner, Nancy W. Anderson, Sarah E. Haushild
Lane Powell Spears Lubersky LLP

Special thanks to our summer associate, Mary Schug, for her legal research and assistance in assembling these materials.

I.

INTRODUCTION

"Privacy in the workplace" actually covers a broad range of topics. The traditional employer activities that raise issues of workplace privacy include: drug testing, workplace and employee searches, surveillance by tape recording or video, and monitoring off-duty conduct. The emergence of the Internet and e-mail has created a vast new area of possible privacy rights for employees. Employees' use of this new technology at work has blurred the lines between personal and professional life. Employers have an interest in promoting workplace efficiency and protecting themselves from liability associated with misuse of employer-owned Internet and e-mail resources. Advances in technology now make it possible to monitor closely employees' use of the Internet and e-mail. Consequently, employers must be informed as to what privacy rights such monitoring may implicate. A recent study by the American Management Association reported that 77.7 percent of employers responding used some form of electronic monitoring and/or surveillance to track employee activity. See American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings, at 1.

The traditional notions of employee privacy rights and the expansion and application of these rights to the Internet and e-mail are central to this presentation. First, the source of privacy rights in both the public and private sectors will be addressed. Second, the extent to which

employers may monitor on-duty employee conduct will be looked at in traditional situations as well as in the emerging areas of Internet and e-mail use. Third, the extent to which an employer may monitor and regulate employees' off-duty conduct will be examined. Although preemployment screening by employers implicates the privacy rights of potential employees, it is beyond the scope of this presentation.

II.

SOURCE OF PRIVACY RIGHTS

A. The Public Sector.

Privacy rights for public employees are found in the United States Constitution and are generally broader than privacy rights enjoyed by employees in the private sector. In order to invoke the protection of the privacy rights guaranteed by the United States Constitution, an individual must be affected by "state action." 42 U.S.C. § 1983; Lugar v. Edmonson Oil Co., 457 U.S. 922, 928-29 (1982). "State action" generally refers to action by employees of the federal or state government, or a subdivision or agency thereof. Privacy rights stem from different parts of the Bill of Rights. The First Amendment protects an employee's freedom of speech and association. The Fourth Amendment prohibits unreasonable searches and seizures. The Fifth Amendment ensures against self-incrimination and the Fourteenth Amendment guarantees due process and equal protection.

State constitutions may also provide a right to privacy. The Washington state constitution provides in Article I, Section 7: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." The Washington Supreme Court has declined to decide whether this provision allows a plaintiff to maintain a civil cause of action based on this right to privacy. See Reid v. Pierce County, 136 Wn.2d 195, 213-14, 961 P.2d 333 (1998)

(stating that plaintiffs may obtain adequate relief under the common law and that such actions are better addressed under the common law invasion of privacy than as a constitutional cause of action); see also John Doe v. Gonzaga Univ., 143 Wn.2d 687, 705, ____ P.3d ____ (2001) (citing Reid, supra, and analyzing plaintiff's invasion of privacy claim under common law right against invasion of privacy without relying on Washington State Constitution). The Oregon state constitution does not explicitly provide for a right of privacy. See Jane Does 1, 2, 3, 4, 5, 6, and 7 v. Oregon, 164 Or. App. 543, 562, 993 P.2d 822 (1999) (holding that neither Article I, Section 1, nor Article I, Section 33, taken together or separately, have ever been construed to provide a general right of privacy under the Oregon Constitution).

B. The Private Sector.

Because "state action" is required to state a claim for violation of the right of privacy found in the Constitution, the United States Constitution has limited applicability to the private workplace. Similarly, the Washington Constitution's right of privacy found in Article I, Section 7 has been construed at the Court of Appeals level as a restraint on government and not a restraint on private individuals. Roe v. Quality Transportation, 67 Wn. App. 604, 608, 838 P.2d 128 (1992) (holding that the Washington Constitution does not provide a right of action against a private employer when that employer terminates an employee for refusing to undergo a random drug test); see also State v. Lee, 135 Wn.2d 369, 397, 957 P.2d 741 (1998) (citing the holding in Quality Transportation, supra, with favor). As noted above, the Washington Supreme Court has declined to address whether the State Constitution provides such a private right of action. See Reid v. Pierce County, supra. However, there are other sources of rights available to employees in the private sector.

Many statutes govern the extent to which employers can intrude into an employee's life. While there are no federal or state statutory provisions that expressly protect privacy in general, there are federal and state statutes that provide for certain privacy interests in particular transactions or with regard to particular matters. Many federal and state statutes focus directly on workplace-specific privacy issues. Employers must also comply with more general laws protecting individual privacy. For example, federal wiretap legislation limits the nonconsensual tape recording of phone calls and various statutes preclude polygraph tests in the workplace.

1. Common Law Invasion of Privacy Torts. The common law invasion of privacy tort is comprised of four subcategories: intrusion upon seclusion; public disclosure of private facts; placing an individual in a "false light"; and right of publicity. See Restatement (Second) of Torts § 652A (1977). The first three are most relevant in the employment law context and will be discussed below.

Washington recognizes the common law general rule for invasion of privacy: "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his [sic] privacy, if the matter publicized is of the kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Reid v. Pierce County, supra, at 204-05 (citing Restatement (Second) of Torts § 652D (1977)). The Washington Supreme Court explicitly stated that the "common law right of privacy exists in this state and that individuals may bring a cause of action for invasion of that right." Id. at 206; accord, John Doe, supra, at 706. Oregon also recognizes this tort for invasion of privacy. See McLain v. Boise Cascade Corp., 271 Or. 549, 554, 533 P.3d 343 (Or. 1975) ("It is now well established in Oregon that damages may be recovered for a violation of privacy").

a. Intrusion Upon Seclusion. A private sector employee can make out an "intrusion upon seclusion" invasion of privacy claim by showing that an employer: (1) made an intentional intrusion, physical or otherwise; (2) upon the plaintiff's solitude or seclusion or private affairs or concerns; (3) which would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977). What constitutes "conduct highly offensive to a reasonable person" is not easily defined and must be determined on a case-by-case basis. The following cases illustrate that the "intrusion upon seclusion" tort will only be found in the most egregious situations.

Although not an employment law case, Mark v. King Broadcasting Co., 27 Wn. App. 344, 354-57, 618 P.2d 512 (1980), shows that Washington recognizes the tort of intrusion upon seclusion. The court noted that in order for the invasion of privacy from intentional intrusion upon seclusion to be actionable, the invasion must be of something that the general public would not be free to view. See id. at 356. In Mark, the court held that because a cameraman from the local television station recorded the plaintiff in his pharmacy from an outside window, in a reasonable manner from a public sidewalk, without using ruse or subterfuge, and did not record anything that a passerby could not have seen, the plaintiff could not recover for intrusion upon seclusion. Id. The court further stated that there was no reason to believe that the film alone would have offended a person of ordinary sensibilities. Id.

Two Oregon cases illustrate the possible outcomes in a cause of action for intrusion upon seclusion based on distinct fact patterns in the employment law setting. In McLain v. Boise Cascade Corp., 271 Or. 549, 554-57, 533 P.2d 343 (1975), an insurance company arranged for plaintiff's surveillance on his own property in connection with plaintiff's pending worker's compensation claim. Plaintiff's activities were filmed during daylight hours from a vantage point

where neighbors or pedestrians could have viewed plaintiff. The investigator's filming and trespassing on a narrow strip along the boundary of plaintiff's property were held not to violate plaintiff's right to privacy. Absent any evidence of intent to harm, harass, or annoy plaintiff, he was entitled to nominal damages only for the trespass. However, the court held that surveillance of an employee's private life or personal matters would be actionable if conducted in an unreasonable and obtrusive manner. Id. at 555-56.

In Leggett v. First Interstate Bank of Oregon, 86 Or. App. 523, 525-26, 739 P.2d 1083 (1987), defendant referred plaintiff to a psychologist because of problems plaintiff encountered at work with coemployees aggravating her phobia about insects and spiders. Plaintiff continued with the psychologist as a private patient after defendant paid for the initial sessions. Defendant's managers met with plaintiff's psychologist without plaintiff's consent and gathered information from the doctor regarding plaintiff's ability to continue with her employment. Plaintiff was terminated after the employer's meeting with her psychologist. Id. at 526. In analyzing whether the intrusion would be "highly offensive to a reasonable person" courts often look at competing interests and the reasonableness of the employee's expectation of privacy. In Leggett, the court acknowledged the employer's "legitimate interest in determining an employee's condition to the extent that it relates to employment," but found that the jury could reasonably have found "that the seriousness of the intrusion on the plaintiff's privacy outweighed the defendant's interest." Id. at 527-28.

Intrusion upon seclusion claims may arise in cases where an employer intercepts an employee's telephone conversation (see Oliver v. Pacific Northwest Bell, 53 Or. App. 604, 607-09, 643 P.2d 1295 (1981)), investigates off-duty conduct or examines an employee's personal belongings, automobile, or computer, even if such items are located on the employer's

premises. Anytime an employer looks or otherwise inquires into what is arguably an employee's personal affairs or property, the employer should be mindful of intrusion upon seclusion elements so as not to intrude where the employee has a reasonable expectation of privacy.

b. Public Disclosure of Private Facts. To establish an invasion of privacy claim based on "public disclosure of private facts," a plaintiff employee must show that the defendant: (1) disclosed private facts; (2) disclosed them to the public generally or to a large number of persons; and that (3) the disclosure was in the form of publicity of a highly objectionable kind. See Simpson v. Burrows, 90 F.Supp.2d 1108, 1125 (D. Or. 2000); see also Cowles Publishing Co. v. Washington State Patrol, 109 Wn.2d 712, 721, 748 P.2d 597 (1988) (for public disclosure of private facts claim, matter publicized must be (a) highly offensive to a reasonable person and (b) not of legitimate concern to the public); Restatement (Second) of Torts § 652D (1977).

There are many cases involving public disclosure of private facts. The Oregon Supreme Court has held that the facts disclosed must be "private," and not public facts. See Trout v. Umatilla Co. School Dist., 77 Or. App. 95, 99-101, 712 P.2d 814 (1984). In Trout, three schoolteachers had been disciplined following an alcohol-related automobile accident unrelated to their employment. The school district publicized statements about the accident and about the disciplinary proceedings. The court held that the party plaintiffs attended and the subsequent accident were public events, "not private affairs into which [the] district pried." Id. at 100. The court concluded that plaintiffs' anonymity was lost when they were involved in the public incident, the consequence of which was the disciplinary action by a public body. Id. at 100-01.

In Caspary v. Washington, 1997 WL 103688 (Wn. App. Div. 1. Mar. 10, 1997) (unreported opinion), the court refused to allow recovery on an invasion of privacy claim for

public disclosure of private facts. In Caspary, plaintiff was a corrections officer who was bitten by an inmate who later tested HIV-positive. Id. at *1. The court held that because the bite took place in plaintiff's public life as a corrections officer and not in the course of his private life and because there were witnesses to the bite, plaintiff could not recover. Id. at *10.

Employer liability over public disclosure of private facts can arise whenever the employer discloses employee information that is personal in nature. Consequently, information about an employee's sexual orientation, medical information, personal affiliations, and any other personal information should be kept confidential to avoid potential liability.

c. "False Light." Oregon and Washington have recognized the tort of "false light." The elements of the false light invasion of privacy theory are found in the Restatement (Second) of Torts § 652E (1977):

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of privacy, if:

- (a) the false light in which the other was placed would be highly offensive to a reasonable person; and
- (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

"False light" invasion of privacy claims are very similar to the tort of defamation and the two are often alleged together. Defamation is basically a written (libel) or oral (slander) publication of a false statement to a third party that tends to "diminish the esteem, respect, goodwill or confidence in which [the plaintiff] is held or to excite adverse, derogatory or unpleasant feelings or opinions against [him or her]." L&D of Oregon, Inc. v. American States Ins. Co., 171 Or. App. 17, 14 P.3d 617 (2000). Thus, the only real difference between the two torts is the

required size of the audience. Although the torts are often alleged together, if they arise out of the same occurrence, double recovery will not be allowed. See Brink v. Griffith, 65 Wn.2d 253, 258-59, 396 P.2d 793 (1964) (holding that although plaintiff could allege defamation and false light due to the circumstances surrounding his termination, he could recover only once).

Many terminated employees have filed claims for false light/defamation over the circumstances surrounding their termination. One particular problem area is references that have been given to prospective employers. Liability can arise when an employer provides to prospective employers information beyond the former employee's name, position held, and dates of employment. The reason for the termination and details about an employee's work performance or employment history are often candidates for potential liability under this kind of claim. This is because the truth of such matter is often in dispute and can be easily challenged by the employee. Defamation/false light suits are very difficult to defend, because, in many circumstances, the plaintiff need not prove any actual damages, and the falsity element is often a question of fact for the jury. Even where the statement in connection with termination is entirely accurate, proving the accuracy of the reference at trial can be costly and risky.

In view of the risks of false light/defamation claims, it is good practice to: (a) restrict the number of people who are authorized to give references concerning former employees; (b) give references only in writing, in response to written requests; and (c) limit the reference to confirmation of dates of employment, job title and compensation. An employer should consider giving additional information only if it has a comprehensive release from the former employee waiving claims for statements made in the reference. To ensure this practice is followed, all calls should be routed to one or more individuals who are trained in the appropriate manner in which to provide a written reference. If an employer is sued for statements made by a supervisor who

was not authorized, having a clear policy in place may provide a defense that any defamatory statements were not made in the course and scope of the supervisor's employment.

Because false light/defamation claims require disclosure to the public in general or publication to third parties, it is also important to ensure that the reasons for an employee's termination are only communicated to those with a "need to know." For example, in Benassi v. Georgia-Pacific, 62 Or. App. 698, 700-02, 662 P.2d 760 (1983), the employer, after terminating the employee, gathered its employees together and explained that the former employee had been terminated for a drinking problem. The employee brought suit for defamation, arguing that his ability to find a job after his termination had been damaged by the employer's public statements regarding the reasons for his discharge. A jury agreed and awarded \$350,000 in damages to the discharged employee. The Oregon Court of Appeals reversed, but clearly indicated that an employer risks a defamation claim by publishing the reasons for discipline to individuals who do not have a reason to know. Id. at 703-10.

III.

MONITORING AND INVESTIGATING ON-DUTY CONDUCT OF EMPLOYEES

Employers' interests in ensuring a responsible and safe workplace are often at odds with an employee's expectation of privacy. An employer is certainly entitled to investigate suspected employee misconduct; however, the investigation will most often be judged by whether it was done in a "reasonable" manner. Employer practices that may infringe on an employee's reasonable expectation of privacy include drug tests, audio and visual surveillance, searches, and interrogations. Recently, it has been suggested that unfettered monitoring of employee internet and e-mail, without notice or a limit in scope, may lead to a violation of an employee's right to

privacy. See Associated Press, Judges Protest Computer Monitoring, Group Claims the Practice Is Illegal, at www.msnbc.com/news/611195.asp (Aug. 8, 2001). Employers must be aware of these potential conflicts in order not to subject themselves to liability for violating an employee's right to privacy.

A. Drug Testing.

1. Public Employers. Public employers are generally limited to testing employees for drugs only if they have a "reasonable suspicion." The Fourth Amendment protects employees from unreasonable search and seizure and applies to public employers or private employers acting as instruments or agents of the government. Furthermore, the Fourth Amendment applies to private sector employees when drug testing is required or authorized by Federal regulations. See Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989). Public employers will generally be permitted to perform drug testing on a particular individual after a "reasonable suspicion" has developed for that individual and random testing when the drug testing serves a "compelling societal interest." See Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665-66 (1989).

2. Private Employers. Private employers are usually not subject to constitutional restraints in terms of drug testing, but may be affected by statute or the common law. Effective until January 1, 2001, when it expired, RCW 49.82.030 provided an incentive for private employers in Washington to test for drugs by providing a worker's compensation premium discount for employers who administered drug testing. The statute defined a "drug-free workplace" program that required a written policy, substance abuse testing and various other measures. "Drug-free workplaces" were then entitled to the discounted worker's compensation premiums. This law did not restrict the circumstances where an employer could administer a

drug test, but instead regulated the technical matters involved in drug testing. The statute permitted random drug testing as well as testing based on reasonable suspicion. RCW 49.82.070(2).

Oregon statutes also regulate drug testing by employers. ORS 659.442. The statute provides that an employer may administer drug tests to employees who are currently engaging in illegal use of drugs, if the employer takes action based on that conduct, without violating antidiscrimination provisions in the statute. ORS 659.442(1); ORS 659.436.

Employers must be careful to keep the results of drug and alcohol tests confidential and use extreme discretion when disciplining employees for drug or alcohol-related misconduct. See O'Brien v. Papa Ginos, 780 F.2d 1067 (1st Cir. 1987) (holding that employer's statement that employee was discharged for drug use was defamatory where drug use was only one of several reasons for discharge); see also Benassi v. Georgia Pacific, 62 Or. App. 698, 662 P.2d 760 (1983) (holding that a statement that employee had a drinking problem was defamatory).

B. Surveillance of Spoken Communications.

The 2001 study by the American Management Association reported that 8.5 percent of employers responding reported recording and reviewing telephone conversations and 7.6 percent stored and reviewed voice mail messages. See American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance Policies and Practices, Summary of Key Findings, supra. 41.6 percent of employers responding said that they record time spent on the telephone and numbers called. Id.

1. Federal Law. Statutory protections of employee privacy rights in communications include the Title III of the Omnibus Crime Control and Safe Streets Act of 1968, amended as the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C.

§ 2510-20. The statute prohibits private individuals and organizations (including employers) from intercepting wire or oral communications and sets out rules for tape recording telephone calls. It does allow a party to intercept a communication where one of the parties to the communication gives prior consent to such interception. 18 U.S.C. § 2511(2)(d). An employer may also monitor employee conversations by listening in on an extension telephone if doing so is in the ordinary course of the employer's business. 18 U.S.C. § 2510(5).

The ECPA creates a private right of action for actual and punitive damages, plus costs and attorneys fees. 18 U.S.C. §2520. Statutory damages are available as well and are calculated at a rate of \$100/day with a minimum award of \$10,000. 18 U.S.C. §2520 (c)(2)(B). To prevail on these claims a plaintiff must prove that he or she had a subjective expectation that his or her conversations were private, free from interception, and that this expectation was reasonable under the circumstances. See United States v. McIntyre, 582 F.2d 1221 (9th Cir. 1978) (holding that police chief had a reasonable expectation of privacy in his office).

2. State Law. Federal and state courts have universally held that the ECPA does not preempt state wiretapping statutes providing greater privacy protections. See Washington v. Williams, 94 Wn.2d 531, 617 P.2d 1012 (1980) (holding that the state Privacy Act is not preempted by the federal wiretap statute and that it fully applies to evidence proffered in state court). Most states, including Oregon, adopt the federal "one party" consent rule. ORS 165.540(1)(a). The Oregon statute further prohibits the recording of face-to-face conversations unless all participants are informed that the conversation is being recorded. ORS 165.540(1)(c). The Washington wiretap statute is more restrictive and requires the consent of all of the participants in order to intercept or record private telephone communications. RCW 9.73.030.

C. Video Surveillance.

The recent American Management Association study found that 11.7 percent of employers responding video record employee job performance and 33.3 percent use video surveillance for security purposes. See American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance Policies and Practices, Summary of Key Findings, supra. Video surveillance is not expressly prohibited by the ECPA. Courts, however, have applied the ECPA provisions to video surveillance conducted by law enforcement agencies in criminal investigations. Federal courts have held that the procedures established for oral and wire surveillance must be followed to determine whether video surveillance by law enforcement officials violates the Fourth Amendment. See United States v. Taketa, 923 F.2d 665, 677 (9th Cir. 1991) (holding that warrantless surveillance by law enforcement personnel for law enforcement purposes violated employee's Fourth Amendment Rights).

There are few cases regarding video surveillance by private entities, but those that exist suggest that the ECPA may create a private right of action for video surveillance. See Boddie v. American Broadcasting Cos., 731 F.2d 333, 336 (6th Cir. 1984) (affirming individual cause of action brought under the Omnibus Crime Control and Safe Street Act for unprivileged video tape recording by a private news organization). Most state laws do not expressly regulate video surveillance. However, since many states have enacted statutes similar to the federal ECPA, courts may make similar extensions in the state law context.

Employers should be cautious of setting up video surveillance in areas of the workplace in which employees have reasonable expectations of privacy in order to avoid common law claims for invasion of privacy. Employers should also consider informing employees of the possibility of video surveillance and document the need for such surveillance.

D. Monitoring Electronic Mail.

The rise of Internet and e-mail access in the workplace requires employers to determine what type of monitoring is permissible and effective. Employers have an interest in monitoring Internet and e-mail use because excessive use is a drain on employee productivity. Furthermore, an employer may be held liable for employee misuse of these systems: "The motivation [to monitor] is clear: 'Almost every workplace lawsuit today, especially a sexual harassment case, has an E-mail component.'" Dana Hawkins, Lawsuits Spur Rise in Employee Monitoring, at www.usnews.com/usnews/issue/010813/work/workplace.htm (Aug. 13, 2001) (quoting Nancy Flynn, executive director of the ePolicy Institute). Accordingly, employers are adapting policies and taking other steps designed to safeguard their organization from costly and damaging lawsuits associated with Internet and e-mail use in the workplace.

The American Management Association survey reported that 61.6 percent of responding employers monitor employee Internet connections and that 46.9 percent store and review e-mail messages. See American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings, supra. In addition, 36.3 percent store and review computer files and 20.5 percent monitor computer use, for example, time logged on and keystroke counts. Id. Over 75 percent of employers electronically monitor their employees or use some type of surveillance -- double the 1997 figure. See Hawkins, supra, at 2. Of those employers that reported active monitoring, 95 percent have written policies concerning e-mail and Internet use, compared with only 75 percent of those that do no monitoring. Id. Also, employers that have been involved in legal action concerning these matters are more likely to have a policy in place regulating use. Id.

The body of case law dealing with these issues is relatively new, but courts have generally upheld employer interests in monitoring employee use of their computer systems. The direction of this area of the law, however, has been criticized: "James M. Rosenbaum, chief judge of the U.S. District Court in Minneapolis, is challenging the conventional wisdom that businesses own not only the computers that employees use but also the personal messages, unfinished drafts, and other thoughts that they casually type into them." Hawkins, supra, at 2. Judge Rosenbaum proposes a balance between an employer's concern for proper computer use and the employee's interest in personal privacy. See James M. Rosenbaum, In Defense of the Hard Drive, 4 Green Bag 2d 169, 171 (Winter 2001). Judge Rosenbaum also questions the "legal principle" that has emerged in this area: "[i]t holds that if a corporation, business, or government entity owns a computer, and if an employee puts personal matter onto that computer, the author has neither a right nor an expectation of privacy in the computer-stored material." Id. at 169. Judge Rosenbaum calls for an examination of this principle because, as he puts it, a free society has a strong interest in preserving for its citizens a central core of privacy to protect their personal thoughts. Id. Finally, Judge Rosenbaum proposes a "cyber statute of limitations" so that electronic data cannot be retrieved without limit. See James M. Rosenbaum, In Defense of the DELETE Key, 3 Green Bag 2d 393, 395 (Summer 2000).

Ninth Circuit judges have also protested the monitoring of their computers, claiming that the practice is illegal, the judges recently had the monitoring software disabled for a week in May of last year. See Associated Press, Judges Protest Computer Monitoring, Group Claims Practice is Illegal, at www.msnbc.com/news/611195.asp (Aug. 8, 2001). The judges are pressing to have the monitoring stopped and the Supreme Court Chief Justice and other judges will consider the request next month. Judge Alex Kozinski of the Ninth Circuit Court of Appeals has

written a memo on the 1986 Electronic Communications Privacy Act explaining that because proper notice of the monitoring was not given, he thinks the monitoring system may be illegal. Id. This issue surrounding the federal judiciary may be played out in the Judicial Conference on Sept. 11, 2001, but the broader issues regarding workplace surveillance may take years to become settled. With these recent criticisms in mind and the awareness that this area of law may take a new direction, the current cases will be examined.

1. Public Employers. Public employees are afforded the protections of the Bill of Rights. However, when the government is acting as employer, the scope and application of these rights is altered. For example, in United States v. Simons, 206 F.3d 392 (4th Cir. 2000), the court held that a warrantless search of a public employee's hard drive did not violate the Fourth Amendment. The court reasoned that in light of the employer's Internet policy, the employee lacked a legitimate expectation of privacy in the files he downloaded from the Internet. Id. at 398. The policy provided that the employer would "audit, inspect, and/or monitor" employees' use of the Internet. Id. at 395.

In Urofsky v. Gilmore, 216 F.3d 401 (4th Cir. 2000), the court refused a constitutional challenge to a Virginia statute restricting state employees from accessing sexually explicit material on computers that were owned or leased by the state. The court said that the state, as employer, possesses greater authority to restrict the speech of its employees than it has as a sovereign to restrict the speech of the citizenry as a whole. See id. at 406. Because the state was acting as an employer it could restrict the Internet use of its employees without trammeling on their First Amendment rights.

2. Private Employers.

a. Federal Law.

(1) The Electronic Communications Privacy Act. The Electronic Communication Privacy Act of 1986 amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968. See 18 U.S.C. §§ 2510-2710. The scope of Title III was expanded to include all electronic communications, bringing e-mail within the coverage of the Act. The ECPA generally makes it illegal to intercept, without a court order, written or electronic communications. However, § 2701 of the Act exempts any entity providing an electronic communication service from liability for accessing stored private communications. Also, § 2702(b) of the Act allows the provider (e.g., the employer) to disclose the contents of a user's electronic communications if doing so is necessary to protect the rights or property of the provider. Therefore, it is highly unlikely that the ECPA will be held to prohibit an employer from monitoring employee e-mail stored on computer systems owned by the employer.

(2) The National Labor Relations Act. An employer's right to monitor is not equal to the employer's right to act on the information obtained. The protections of the National Labor Relations Act may protect employees' use of e-mail in certain circumstances. Because many employers (over 75 percent according to the AMA study) permit some personal use of their e-mail systems, employers should be cautious about disciplining employees for using the company e-mail system to engage in labor organizing or other even activities that are arguably protected by the NLRA provisions on "concerted activity," such as comparing compensation, criticizing management, or raising safety concerns.

In Timekeeping Systems, Inc., 323 NLRB No. 30 (1997), the Board held that a nonunionized employee could not be lawfully terminated for using e-mail to criticize his

employer's proposed vacation policy. The Board reasoned that the employee's activities fell within the scope of Section 7 of the NLRA, which gives employees' rights to engage in concerted activities "for the purpose of mutual aid or protection." The employee used his e-mail to respond to his employer's solicitation for input on the proposed policy and to inform his fellow employees about his view of the "true nature" of the proposed policy and "to correct misperceptions" about it.

b. State Law. Neither Washington nor Oregon regulates by statute employers' monitoring of e-mail. However, it is entirely possible that an invasion of privacy claim would be allowed to proceed where the employer does not warn employees that it is monitoring e-mail. See Restuccia v. Burk Tech., 1996 WL 1329386 (Mass. Aug. 13, 1996) (denying employer's motion for summary judgment and stating that an employee's invasion of privacy claim could go forward when employer failed to warn that employee's e-mail was being monitored; genuine issues of material fact remained as to whether employer's reading of e-mail constituted an unreasonable interference with employees' privacy).

3. Employer Liability for Employee Misuse.

a. Case Law. Recent cases have shown that transmission of e-mail containing offensive content may give rise to hostile work environment claims against an employer. To succeed on a claim for hostile work environment the conduct must be severe and cannot consist of isolated remarks and incidents. See Haubey v. Snow, 106 Wn. App. 666, 675-76, ____ P.3d ____ (2001) (court looks to totality of circumstances, including frequency, severity and persistence and actions); Fred Meyer v. Bureau of Labor & Industries, 152 Or. App. 302, 308-09, 954 P.2d 804 (1998); see also Owens v. Morgan Stanley & Co., Inc., 1997 U.S.

Dist. LEXIS 10351, 74 Fair Empl. Prac. Cas. (BNA) 876 (S.D.N.Y. 1997) (allegation of a single racist e-mail, although reprehensible, could not support a claim for hostile work environment).

In Curtis v. Citibank, 1998 U.S. Dist. LEXIS 21 (S.D.N.Y. 1998) (Curtis I), plaintiffs brought a claim for employment discrimination pursuant to Title VII of the Civil Rights Act claiming that they were discriminated against based on their race and gender. Plaintiffs alleged that a hostile work environment existed resulting from the transmittal of racially and sexually offensive e-mail messages among the employers' supervisory employees. Id. at *3. The plaintiffs alleged that an offensive e-mail message sent by a Citibank employee to other Citibank employees, at their work addresses, created a hostile work environment because the "humor" in the messages was derived from ethnic, racial, and gender stereotypes. See Curtis v. Citibank, 226 F.3d 133 (2d Cir. 2000) (in which plaintiffs filed a second suit based on the amended complaint that was not accepted by the court in Curtis I).

b. Recommendations for Monitoring E-mail Use. In order to protect themselves from constitutional and common law claims for invasion of privacy, many employers take steps to diminish an employee's expectation of privacy in their e-mail communications by developing an e-mail use policy and giving employees written notice of such policy. Certainly, if employees give written consent to the monitoring of e-mail, a court is unlikely to find reasonable expectation of privacy in their workplace e-mail communications. Furthermore, if employees believe that their e-mail will be monitored, they are more likely to be deterred from using the employer's e-mail system to send jokes that may contain material that is offensive to other employees and could give rise to a hostile work environment claim against the employer.

E. Monitoring Web Site Visits, Computer Use, and Access to "Private" Web-Based E-mail Systems.

Employees use workplace computers to view web sites and many use web-based e-mail services such as Hotmail and Yahoo to send personal e-mail messages. Employees are not always informed that the capability to monitor this use exists in the form of filtering software. Monitoring can be done based on various criteria, including URL or exposure to liability criteria, which includes: monitoring access to sites, which contain pornography, lingerie, hate, and weapons. Only 38 percent of respondents to the AMA Study reported using "blocking" software that prevents Internet connections to unauthorized or inappropriate sites. Therefore, many companies use monitoring to enforce their policies against unauthorized use. See American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings, supra, at 3. Management's primary concern is keeping sexually explicit material off the screens in the office; this is reflected by the statistic that 76.6 percent of respondents have a policy restricting the use of Internet sites with explicit sexual content. Id. As noted above, only 38 percent of employers enforced this policy through "blocking" software; the remainder enforced this policy through monitoring.

1. Potential Employer Criminal Liability for Employee Internet Use. In certain cases, employers could be liable for their employees' illegal online activity. See Mark Ishman, Computer Crimes and the Respondeat Superior Doctrine: Employers Beware, 6 B.U. J. Sci. & Tech. L. 6, 3 (2000). An employer providing Internet access may be held liable for the foreseeable acts of its employees conducted over the Internet. Id. at 16. An employer may be held liable under "respondeat superior" for an employee's wrongful act if: (1) the act occurred within the scope of the employee's employment; and (2) the wrongful act was known or should

have been known by the employer. Id. Some examples of illegal behavior by an employee include stock manipulation, business disparagement, copyright infringement, executing computer viruses and worms, and Internet gambling. Id. Employers should provide employees with a clear policy prohibiting the use of the employer's Internet and e-mail for nonbusiness and illegal activity.

2. Potential Employer Civil Liability for Employee Internet Use. In addition to exposure to liability for employees' use of e-mail, employers may face liability for employees' use of the Internet to view pornography or other offensive material. In Coniglio v. City of Berwyn, 2000 WL 967989 (N.D. Ill. 2000), plaintiff sued her employer, the City, alleging that her supervisor's practice of viewing pornography on the Internet in full view of city employees created a hostile work environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff observed her supervisor's computer screen displaying such images a few times a week, through the picture window into his office. Id. at *2. The court denied summary judgment for the City on the Title VII claim and determined that a question of fact existed as to the frequency and duration of the conduct in order to determine whether a hostile work environment existed. Id. at *8.

Employers may also face liability from employees for the activities of nonemployees permitted to use the employer's Internet access. Earlier this year, the Minneapolis Public Library faced an EEOC charge by its librarians based on library patrons' unlimited use and access to the Internet. See Carl S. Kaplan, Cyber Law Journal: Controversial Ruling on Library Filters, New York Times (June 1, 2001). The librarians complained that the library's policy of permitting patrons to view and print sexually explicit images on unrestricted computer terminals created a hostile work environment, as patrons viewed the pornographic websites all day, printed

explicit materials, which were discovered by other patrons, including children, and engaged in hostile and explicit activities within the library. Id. The librarians filed their charge only after repeated complaints to the library to change its policies were rejected on First Amendment grounds. The EEOC made a "probable cause" finding in that case. Id. Although not carrying the same force as a court decision, the EEOC's probable cause finding is certainly a warning that employers may be subject to hostile work environment claims for employees' and nonemployees' Internet use where such use results in a pervasive atmosphere of sexually explicit images and hostile behaviors.

Employer liability may also arise where the employer maintains an electronic bulletin board. In Blakey v. Continental Airlines, Inc., 751 A.2d 538 (N.J. 2000), the court held that although an electronic billboard may not have a physical location in the employer's workplace it might nonetheless have been so closely related to the workplace environment and beneficial to the employer, that continued harassment on the forum would give rise to the employer's duty to remedy the harassment in order to avoid liability for hostile work environment. Id. The claim arose when pilots of Continental Airlines used the employer's electronic bulletin board to post allegedly defamatory messages about the plaintiff, a female pilot for the airline. Id. at 545-46. The court held that although the employers did not have a duty to monitor private communications of their employees, they did have a duty to take effective measures to stop coemployee harassment when the employer knew or had reason to know that harassment was taking place in a setting related to the workplace. Id. at 552.

3. Employer Precautions. Once again, employers should diminish an employee's expectation of privacy in workplace use of employer provided Internet and web-based e-mail services, thereby decreasing the chance for lawsuits against employers for invasion of privacy

and for coworker harassment. Employers should publish their Internet and e-mail policies and explicitly state that website visits and e-mail sent through a third-party server, e.g., Hotmail from workstations, are also subject to monitoring. Of course, employers that promulgate, train on and enforce an active antiharassment policy can assert an affirmative defense to liability for coworker harassment. Thus, an employer who receives allegations that harassment may be taking place over electronic communications should treat the situation as it would any other harassment situation.

F. Searches of Work Areas.

Employers may have reason to search the workplace. An employer may need to do something as simple as search for a file at an employee's desk or as serious as searching to prevent the use or sale of drugs in the workplace or to look for weapons or other dangerous items. Again, the validity of the search will most likely be judged by balancing the employee's reasonable expectations of privacy in the area searched against the employer's legitimate interest in the search.

1. Public Sector. The Fourth Amendment protects public employees from "unreasonable" searches. A search is reasonable if the employee's expectations of privacy are outweighed by the government's need for supervision, control and efficient operation of the workplace. Each case is to be determined based on the individual circumstances. See O'Connor v. Ortega, 480 U.S. 709 (1987) (holding that a hospital psychiatrist had a reasonable expectation of privacy in his desk and his filing cabinet because he had exclusively occupied his office for 17 years and the file cabinet contained only personal files).

2. Private Sector. Private employees are rarely covered by the Fourth Amendment, but may still be protected from employer searches under common law privacy theories. These

theories typically require balancing the employee's expectation of privacy against the employer's interest in the search. See K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984) (holding that employee's expectation of privacy in a locker furnished by K-Mart, but for which she provided the lock, outweighed K-Mart's business interest in the locker; K-Mart's reason for the search failed to justify the intrusion).

As with all of the other areas discussed, an employer's best protection against these types of claims is to diminish an employee's expectation of privacy by developing a search policy and making employees aware of the policy.

G. Search and Surveillance of Employees.

The Fourth Amendment protects public sector employees from unreasonable personal searches. Because personal searches are highly intrusive, they must be reasonable and will only be justified if counterbalanced by a strong showing of need. Employers should avoid conducting personal searches of employees unless absolutely necessary or obviously called for in light of suspected misconduct.

Private employees have strong common law protections against searches of their bodies. Aggrieved employees can bring claims for invasion of privacy, intentional and/or negligent infliction of emotional distress or outrage, and assault and battery. Rarely will circumstances justify a body search. In Bodewig v. K-Mart, 54 Or. App. 480, 635 P.2d 657 (1981), an employee stated a claim for intentional infliction of severe emotional distress when she was forced to endure a strip search in a public restroom in the presence of a customer, who had accused her of stealing \$20, and the assistant manager. Id. The court held that the jury could find that the employer's conduct was deliberately calculated to cause emotional distress. Id.

Employers should avoid personal searches whenever possible. If a search must be done, confine the search to the employee's belongings if at all possible. Searches should be authorized by a publicized company rule that specifically announces the company's right to conduct searches. Never conduct a search without consent. Employees should understand that they are free to leave and are not required to participate in a search. The employee should be informed in advance regarding how extensive the search will be. An employee should be present during the search of his or her belongings, desk, or locker, even when the company owns the desk or locker.

IV.

MONITORING AND INVESTIGATING OFF-DUTY CONDUCT OF EMPLOYEES

A. Employers Must Show Adverse Impact on Employee Job Performance or on Business Concerns Before Intruding Into Off-Duty Activities.

As discussed above, an employee does not lose his or her right to privacy when he or she goes to work. Because an employee still enjoys certain privacy protections in the workplace, when an employee leaves work, an employer's ability to monitor and/or attempt to control the employee's activities becomes extremely limited. When employee misconduct is off duty and non-work-related, courts are usually unwilling to presume that dismissing the employee will promote "efficiency of service" and the employer is required to demonstrate by sufficient evidence that the off-duty conduct adversely impacts the performance of the duties of the employee. See Bonet v. United States Postal Serv., 661 F.2d 1071, 1078 (5th Cir. 1981).

In Washington, RCW 50.20.060 states that an individual will be disqualified from unemployment compensation if the employee's discharge was for misconduct connected with his or her work. In Nelson v. Employment Security, 98 Wn.2d 370, 374-75, 655 P.2d 242 (1982),

the Washington Supreme Court laid out the meaning of misconduct off the job for the purpose of the statute:

We adopt the rule that in order to establish misconduct connected with an employee's work as required by RCW 50.20.060 the employer must show by a preponderance of the evidence that a reasonable person would find the employee's conduct: (1) had some nexus with the employee's work; (2) resulted in some harm to the employer's interest; and (3) was in fact conduct which was (a) violative of some code of behavior contracted for between employer and employee, and (b) done with intent or knowledge that the employer's interest would suffer.

The court noted that this interpretation was identical to the standard applied in Oregon. Id. at 374; see also 2001 Oregon Session Laws Ch. 144 (H.B. 2767) (amending ORS 657.176 (2)(a) to add a provision exempting employees who quit work because of domestic violence issues from disqualification). The court held that a cashier could not be denied unemployment benefits due to her conviction for shoplifting because the off-duty misconduct was not in violation of any code of behavior agreed upon between the cashier and her employer. See Nelson, 98 Wn.2d at 375. In order for an employer to demonstrate that the employer's interest would suffer due to employee misconduct and that the employer is therefore justified in disciplining or terminating an employee for such off duty conduct, the conduct must be closely related to the employee's work. Id.

B. Types of Off-Duty Conduct Employers May Sanction and Control.

Having discussed the general principles applicable to the discipline of employees for off-duty conduct, specific situations that recur in case law will be discussed.

1. Illegal Conduct. Employers may terminate an employee for illegal or disreputable conduct, although, as always, employees should be careful to do so for legitimate business reasons, e.g., workplace safety, business reputation. Two Washington cases have upheld an

employer's discharge of an employee for disreputable or illegal conduct against the employee's public policy arguments. Selix v. Boeing, 82 Wn. App. 736, 919 P.2d 620 (1996); Winspear v. Boeing, 75 Wn. App. 870, 880 P.2d 1010 (1994).

In Selix, the employer terminated plaintiff after he was charged with felony child molestation and convicted of a lesser included misdemeanor offense of fourth degree assault. The employer terminated plaintiff for violating a Boeing Company rule forbidding the "commission of a penal offense." The Court of Appeals affirmed the trial court's grant of summary judgment to the employer, stating that there was no public policy in RCW 9.96A.010 (supporting rehabilitation of felons) or RCW 9.96A.020 (which is applicable only to public employers) prohibiting an employer's termination of an employee based solely on his criminal conviction. Selix, 82 Wn. App. at 743-44.

In Winspear, the employee was charged with two counts of indecent liberties and two counts of second degree rape of a child. The employee pled guilty to a misdemeanor charge of fourth degree assault. After he was terminated by his employer, the employee alleged that his termination violated an implied contract and violated the public policy of the state against discriminating on the basis of a criminal conviction. The court first found that there was no implied contract, then moved to the employee's public policy argument. Noting that the regulation on which the employee relied, WAC 162-16-060, had been declared invalid in Gugin v. Sonico, 68 Wn. App. 826, 846 P.2d 571 (1993), the court denied the employee's public policy claims. Winspear, 75 Wn. App. at 882. The current regulation on preemployment inquiries about prior convictions restricts such inquiries to felonies occurring within the last ten years and justified by "business necessity," which the WAC defines as "relating reasonably" to job duties.

2. Drug and Alcohol Use. Employers usually must show that off-duty drug and alcohol use adversely affected an employee's employment in order to be consistent with employee privacy rights and standards for good cause termination. Ordinarily, the misconduct complained of must be contemporaneous in time to the employee's work. Even if an employee tests positive for drug use, if the use cannot be proven to have interfered with the employee's work, the test results are not considered "misconduct," and the former employee is eligible for unemployment compensation. See Stone Forest Industries Inc. v. Employment Division, 127 Or. App. 568, 570, 873 P.2d 474 (1994) (holding that even though employee tested positive for marijuana use and admitted to using it two to three days before the test, it could not be proven that the employee was under the influence of or impaired by the drug on the job and therefore he couldn't be denied unemployment compensation); accord, Glide Lumber Products Co. v. Employment Division, 86 Or. App. 669, 741 P.2d 907 (1987).

However, if the position is one in which public image or expectations are important to the business the misconduct may not need to be contemporaneous. In Washington v. City of Seattle, 69 Wn.2d 816, 818, 420 P.2d 704 (1967), the court held that the dismissal of a police officer for being affected by intoxicating liquors on two occasions to the point where it was not safe for him to drive, even though off-duty, constituted just cause for his dismissal.

3. Intimate Relationships. Employers should not attempt to restrict social relationships absent a work-related reason. Eliminating sexual harassment or protecting against trade secret disclosure may constitute work-related reasons. Discharging an at-will employee for engaging in an affair with a coworker may, but will not always, be permitted by the courts. Compare Patton v. J.C. Penney, 301 Or. 117, 719 P.2d 854 (1986) (rejecting wrongful discharge claim), with Rulon-Miller v. Int'l Bus. Machs., 162 Cal. App. 3d 241 (1984) (upholding a

\$300,000 jury verdict where an employee was discharged for having an affair with the manager of a rival firm, stating that employee had a contractual right to privacy conferred by the employer's written policy statement). Policies that proscribe obvious conflicts of interest and/or superior-subordinate relationships will usually survive the challenge. See, e.g., *Born v. Blockbuster Videos, Inc.*, 941 F. Supp. 868 (S.D. Iowa 1996) (rejecting wrongful discharge claim brought by employees terminated for dating each other in violation of the policy that prohibited employees from dating their supervisors because employees failed to note a well recognized public policy exception to the at-will doctrine).

4. Nepotism. Oregon law makes it unlawful employment practice for an employer to refuse to hire or employ an individual solely because another member of that individual's family works or has worked for the employer. ORS 659.340. Exceptions include situations where one family member would supervise another or be in a grievance adjustment position with respect to the other. Washington's antidiscrimination in employment statute, RCW 49.60.180, provides that it is unlawful practice for any employer to refuse to hire or to discharge any person on the basis of marital status; however, WAC 162-16-250 provides the following exception:

(2) Exceptions to the rule. There are narrow exceptions to the rule that an employer, employment agency, labor union, or other person may not discriminate on the basis of marital status:

(a) If a bona fide occupational qualification applies (please see WAC 162-16-240).

(b) If an employer is enforcing a documented conflict of interest policy limiting employment opportunities on the basis of marital status:

(i) Where one spouse would have the authority or practical power to supervise, appoint, remove, or discipline the other;

(ii) Where one spouse would be responsible for auditing the work of the other;

(iii) Where other circumstances exist which would place the spouses in a situation of actual or reasonably foreseeable conflict between the employer's interest and their own; or

(iv) Where, in order to avoid the reality or appearance of improper influence or favor, or to protect its confidentiality, the employer must limit the employment of close relatives of policy level officers of customers, competitors, regulatory agencies, or others with whom the employer deals.

5. Employee Appearance. Employers may legitimately ask that an employee maintain a specific appearance as long as there is a reasonable relationship between the employer's image or safety concerns and the rules regarding the employee appearance. Although employers may have legitimate interests in regulating employees' appearance while on the job, this interest usually disappears for off-duty appearance. However, some requirements for on the job appearances will affect off-duty appearances because they require certain hair length or prohibitions on facial hair. Employers should be aware that restrictions on facial hair or certain dress could violate the religious accommodation requirements of Title VII and state antidiscrimination law.

An employer's discharge of a male grocery clerk for failing to conform to the employer's hair length regulations for male employees was not found to constitute discrimination in employment on the basis of sex, contrary to a Washington statute on unfair employment practices. See Albertson's, Inc. v. Washington State Human Rights Comm'n, 14 Wn. App. 697, 544 P.2d 98 (1976). The Act was interpreted as only prohibiting classifications that afforded a significant employment opportunity to one sex in favor of the other. Id. at 700. Because hair length is not the type of characteristic that is immutable, unalterable, or constitutionally protected, a private employer could regulate it as to only males without violating the Act. Id. "The employee who objects to an employer's grooming code may reject the constraint and seek

other employment, or subordinate to the policy in order to obtain or retain his job." Id. at 701. Also, the suspension of a male bus driver for wearing a beard in violation of a company policy was found to be reasonable based on evidence that drivers with beards or long hair alienated customers. See Brookes v. Tri-County Metro. Transp. Dist. of Oregon, 18 Or. App. 614, 526 P.2d 590 (1974). It is questionable whether such a rule would withstand a challenge by an employee whose religion required him to maintain a beard of long hair.

6. Business Activities. Employers may be permitted to place limited restrictions on their employee's off-duty business activities -- e.g., moonlighting and other outside employment for financial gain -- but only on those activities that would impair an employee's ability to give his or her best services to the employer. In other words, employers must have a legitimate business reason for any such restrictions and may not provide a blanket prohibition against outside business activities. In Organon v. Hepler, 23 Wn. App. 432, 433-34, 595 P.2d 1314 (1979), a pharmaceutical company brought an action against one of its employees, a drug salesman, for breach of an agreement not to perform any outside business activities for financial gain, such as moonlighting, part-time jobs on evenings and weekends, and selling any product or service. The employee had solicited business for another company that produced medical machines while on duty. The court noted that, generally, courts refuse to interpret contracts which require employees to devote their whole time and attention to their employment to include time normally devoted to rest and recreation, but upheld the employer in this case, finding that the extra employment impaired the employee's ability to give his best services to the employer. Id. at 436.