Chapter

13

The Employee's Right to Privacy and Management of Personal Information

Learning Objectives

When you finish this chapter, you should be able to:

- LO1 Describe the nature of privacy as a fundamental right.
- LO2 Explain the three general ways in which privacy is legally protected in the United States.
- LO3 Identify and apply the standard for unreasonable searches and seizures under the Fourth Amendment.
- **LO4** Explain the distinctions between the protections for public- and private-sector privacy protections.
- ldentify and differentiate the prima facie cases for common-law claims of privacy invasions (intrusion into seclusion, public disclosure of private facts, publication in a false light, and breach of contract/defamation).
- LO6 Explain the extent to which an employer can legally dictate the off-work acts of its employees.
- LO7 Discuss how advances in technology have impacted employee privacy.
- LO8 State the key business justifications for employee monitoring.
- LO9 Explain the most effective means by which to design and to implement a technology use policy.

© The McGraw-Hill Companies, 2009

Opening Scenarios

SCENARIO 1

Aravinda has been reading in the news lately of the skyrocketing costs of health Scenario care, particularly surrounding the HIV epidemic. She is concerned that her small 10-employee company would suffer a financial disaster if one of its workers contracted the virus since the company's insurance costs would increase. Therefore, she wants to conduct a confidential HIV test of each present employee and future applicant. Aravinda has several concerns. First, what if an individual refuses to take the test based on the grounds of invasion of privacy? Second, if someone tests positive, can Aravinda refuse to hire or can she discharge her or him without violating federal law protecting employees with disabilities? Third, how can she otherwise protect against rising costs? Fourth, if an employee tests negative, but Aravinda decides to terminate the employee anyway, is she liable for the appearance that the employee is HIVpositive and that Aravinda terminated her or him as a consequence of the test results? How can she ensure that the test results are kept confidential?

SCENARIO 2

Abraham, a Realtor, has three children, two of whom are in college. In order to earn exScenario tra money to help with college tuition payments, Abraham (who studied modern dance during his college career) finds a job dancing in a club that caters specifically to women. While not exactly erotic dancing (he keeps all of his clothes on), it is not ballroom dancing either. Celebrating during a bachelorette party, one of the partners of the real estate firm for which Abraham works catches sight

of him dancing. When he arrives at the office the next day, she calls him into her office and orders him to quit his night job. She claims that both clients and potential clients might see him there and he would lose all credibility as a Realtor. Does she have a right to require Abraham to do this as a condition of future employment? (Presume that he is an employee and not an independent contractor.)

SCENARIO 3

Solange receives a "spam" e-mail asking her to go look at a certain Web site. Since Scenario she does not know who it is from or why she is receiving it, she clicks on the link and finds herself at a Web site devoted to XXX-rated videos. She is so perturbed by this occurrence that she spends a few moments looking around the Web site trying to find its site administrator. She intends to send off a message to the administrator asking this person not to send her any more junk mail. After searching for several minutes with no luck, she leaves the Web site and goes back to reading her e-mail. A few days later, she is called into her manager's office and reprimanded for using employerowned computer equipment for personal interests such as this XXX-rated video site. It seems that her manager was using a program that alerted him any time an employee perused certain inappropriate Web sites. She tries to explain, but leaves with a written reprimand in her hand and a copy in her files. She is furious, not only at her manager's unwillingness to understand, but also at the invasion of her privacy posed by this computer monitoring. Does her employer have a right to monitor her computer use in this way?

Are There Guarantees in Life?

Privacy is a surprisingly vague and disputed value in contemporary society. With the tremendous increase in computer technology in recent decades, calls for greater protection of privacy have increased. Yet, there is widespread confusion concerning the nature, extent, and value of privacy. Philosophers have argued that our society cannot maintain its core values without simultaneously guaranteeing the privacy of the individual. Edward Bloustein writes that "an individual deprived of privacy merges with the mass. His opinions, being public, tend never

LO1

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

662 Part Three Regulation of the Employment Environment

to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual."

Recent inventions and business methods call attention to the next step that must be taken for the protection of the person and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."²

The concept of privacy as a fundamental right is certainly not limited to the United States or even Western culture. Privacy is protected in the Qur'an³ and was recognized by Mohammed.⁴ Ancient Greece already had laws protecting privacy, and the Jewish Talmud considers privacy an aspect of one's sanctity, providing rules for protecting one's home. In fact, the Talmud contains reference to "harm caused by seeing" (hezeq re'ivvah) when one intrudes upon another.

But do employees actually have a "fundamental right to privacy" as many believe? The answer to this question is not as easy as one might presume, given the wide recognition of employee rights in the workplace. The right to privacy may not be as fundamental as employees generally believe it to be, which makes it all the more important in these days of advancing information technology. Computer technology, though largely beneficial, can have a negative effect on employees if the easily obtained information is misused, incorrect, or misleading. Employers now have a greater capacity to invade an employee's privacy than ever before. Among other devices, there are chairs that can sense and record the time an employee spends at his or her desk, computer programs that measure employees' computer keystrokes to ensure they are as productive as they should be, phones that monitor employees' phone calls, and policies related to workplace communication to make sure all communications are work-related. Monitoring is only increasing in power, ability, and frequency. Sales of computer monitoring and surveillance software have increased almost 500 percent to \$622 million in 2006.⁵ But perhaps there is presently a greater employer need for seemingly private information, with more than 75 percent of 14.8 million drug users in the United States employed.⁶ Drug use in American industry costs employers approximately \$82 billion per year in overall productivity due to absenteeism and attrition; theft of employer property by employees is estimated at \$10 billion per year; and failure to perform an intensive reference and background check of an applicant may cost the employer enormous amounts in litigation fees defending claims of negligent hiring, easily outweighing the cost of a drug test, usually less than \$50. In this time of increased competition in the global marketplace, each employee becomes all the more crucial to the workings of the company. An employer has a justified basis for attempting to choose the most appropriate and qualified person for the job; the means by which the employer obtains that information, however, may be suspect.

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 663

The right to privacy is not only balanced with the arguably legitimate interests of the employer but also with the employer's responsibility to protect the employees' personal information. A 2007 study of more than 800 North American privacy and security professionals reported that there is a strong likelihood of a security breach relating to personally identifiable information. In fact, 85 percent of those responding had experienced or observed a security breach within the past 12 months and 63 percent had experienced multiple breaches during that time—between 6 and 20 occurrences.⁷

Since erosion of at-will employment was the dominant issue of the 1980s, scholars have predicted that privacy will be the main theme for the 1990s and beyond. This chapter will address the employee's rights regarding personal information and the employer's responsibilities regarding that information, as well as the employer's right to find out both job-related and nonrelated personal information about its employees. Chapter 3 previously addressed other issues regarding the legality of information gathering through testing procedures. This chapter will not address issues relating to consumer privacy since they fall outside the scope of the chapter's and the text's primary focus.

Background

LO₂

There are three ways in which privacy may be legally protected: by the Constitution (federal or state), by federal and/or state statutes, and by the common law. The U.S. Constitution does not actually speak of privacy, but privacy has been inferred as a necessary adjunct of other constitutional rights we hold. The right to privacy was first recognized by the Supreme Court in Griswold v. Connecticut, 8 when the Court held that a Connecticut statute restricting a married couple's use of birth control devices unconstitutionally infringed on the right to marital privacy.

The Court held a constitutional guarantee of various zones of privacy as a part of the **fundamental rights** guaranteed by the Constitution, such as the right to free speech and the right to be free from unreasonable searches and seizures. The latter right is that on which many claims for privacy rights are based; the Court has held that under certain circumstances the required disclosure of certain types of personal information should be considered an unreasonable search. It has protected against the mandatory disclosure of personal papers, and it decided in favor of the right to make procreation decisions privately.

While baseless or unjustified intrusions, at first blush, may appear to be completely abhorrent in our society, proponents of the argument that employers can ask whatever they please argue that if an employee does not want to offer a piece of information, there is something the employee is trying to hide. For example, why would an employee refuse to submit to a drug test if that employee is not abusing drugs? Do private-sector employers have the right to ask their employees any question they choose and take adverse employment actions against the employee if she or he refuses to answer since they are not necessarily constrained by constitutional protections? (See Exhibit 13.1, "Myths about Employee Privacy Rights.")

fundamental right

A right that is guaranteed by the Constitution, whether stated or not.

private sector

That segment of the workforce represented by private companies (companies that are not owned or managed by the government or one of its agencies).

664 Part Three Regulation of the Employment Environment

Exhibit 13.1 MYTHS about Employee Privacy Rights

- 1. Employees have an absolute right to privacy in their workplace.
- 2. It is a breach of an employee's right to privacy for an employer to ask with whom the employee lives.
- 3. In the private sector, the Constitution protects employees' right to be free from unreasonable searches and seizures.
- 4. Without constitutional protection, employees in the private sector are left with no protection against invasions of privacy.
- 5. Once an employee gives information to an employer, the employer may use it for whatever purpose it desires.

Additionally, employees are concerned about the type of information gathered in the course of applying for and holding a job. Who has access to that information? What information may be deemed "confidential," and what does that mean to the employee? Evidently, employers perceive challenging issues among these and others with regard to privacy; as of 2004, there were more than 2,000 chief privacy officers (CPOs) in businesses around the world, more than 10 times the estimate three years ago.⁹

Public Sector Employee Privacy

public sector

That segment of the workforce represented by governmental employers and governmental agency employers. In some situations, this term may include federal contractors.

With regard to the **public sector**, the Constitution protects individuals from wrongful invasions by the state or by anyone acting on behalf of the government. The personal privacy of federal, state, and local employees is therefore protected from governmental intrusion and excess. As we will see later in this chapter, private-sector employees are subject to different—and often fewer—protections.

Constitutional Protection

The Fourth Amendment and Its Exceptions

For the Fourth Amendment's protection against unreasonable search and seizure to be applicable to a given situation, there must first exist a "search or seizure." The Supreme Court has liberally interpreted "search" to include a wide variety of activities such as the retrieval of blood samples and other bodily invasions, including urinalyses, as well as the collection of other personal information. One might imagine how this umbrella gets wider as technology advances.

LO3



For the search to violate the Fourth Amendment, that search must be deemed unreasonable, unjustified at its inception, and impermissible in scope. You will read in the seminal Supreme Court case, *O'Connor v. Ortega*, included at the end of the chapter, that a search is justified "at its inception" where the employer has reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or where the search is necessary for a noninvestigatory work-related purpose such as to retrieve a file.

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 665

It is critical to review the *O'Connor* case to understand both the fundamental basis of public-sector search and seizure law as it applies to the workplace as well as much of current case law today. The Court held that a search is permissible in scope where "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the misconduct being investigated."

Generally, all searches that are conducted without a judicially issued warrant based on a finding of reasonable cause are held to be per se unreasonable. But there are several exceptions to this rule, including searches that happen as part of an arrest, some automobile searches, pat-down searches with probable cause to believe the subject is armed, and administrative searches of certain regulated industries.

One example of an exception occurred in Shoemaker v. Handel¹⁰ where the Supreme Court held that a drug-related urine test of jockeys without a warrant was acceptable because it satisfied the court's two-pronged test. The Court held that (1) where there is a strong state interest in conducting the unannounced warrantless search and (2) where the pervasive regulation of the industry reduces the expectation of privacy, the search does not violate the Fourth Amendment. Similarly, in Skinner v. Railway Labor Executives Association, 11 decided three years after Shoemaker, the Court again addressed the question of whether certain forms of drug and alcohol testing violate the Fourth Amendment. While this case is discussed in this text in connection with testing, it is relevant here for the Court's analysis of the privacy right challenged. In Skinner, the defendant justified testing railway workers based on safety concerns: "to prevent accidents and casualties in railroad operations that result from impairment of employees by alcohol or drugs." The Court held that "[t]he Government's interest in regulating the conduct of railroad employees to ensure safety, like its supervision of probationers or regulated industries, or its operation of a government office, school, or prison, likewise presents 'special needs' beyond normal law enforcement that may justify departures from the usual warrant and probable-cause requirements."

It was clear to the Court that the governmental interest in ensuring the safety of the traveling public and of the employees themselves "plainly justifies prohibiting covered employees from using alcohol or drugs on duty, or while subject to being called for duty." The issue then for the Court was whether the means by which the defendant monitored compliance with this prohibition justified the privacy intrusion absent a warrant or individualized suspicion. In reviewing the justification, the Court focused on the fact that permission to dispense with warrants is strongest where "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search," and recognized that "alcohol and other drugs are eliminated from the bloodstream at a constant rate and blood and breath samples taken to measure whether these substances were in the bloodstream when a triggering event occurred must be obtained as soon as possible." In addition, the Court noted that the railway workers' expectations of privacy in this industry are diminished given its high scrutiny through regulation to ensure safety. The Court therefore concluded that the railway's compelling interests

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

666 Part Three Regulation of the Employment Environment

outweigh privacy concerns since the proposed testing "is not an undue infringement on the justifiable expectations of privacy of covered employees." Consider the possible implications of this and related decisions on genetic testing in governmental workplaces or in employment in heavily regulated industries such as that involved in *Skinner*:

Finally, the employer may wish to conduct a search of employee lockers. Would this be acceptable? Under what circumstances is an employer allowed to conduct searches? A search may constitute an invasion of privacy, depending on the nature of the employer and the purpose of the search. The unreasonableness of a search is determined by balancing the extent of the invasion and the extent to which the employee should expect to have privacy in this area against the employer's interest in the security of its workplace, the productivity of its workers, and other job-related concerns.

Prior to any search of employer-owned property, such as desks or lockers, employees should be given formal written notice of the intent to search without their consent. Where the employer intends to search personal effects such as purses or wallets, employees should be forewarned, consent should be obtained prior to the search, and employees should be made well aware of the procedures involved. ¹² Consent is recommended under these circumstances because an employee has a greater expectation of privacy in those personal areas. These rights are significantly diminished where the employer is not restrained by constitutional protections.

In an interesting combination of private/public workplace rights, the Ninth Circuit addressed these issues in the 2007 case, *United States v. Ziegler.* ¹³ In that case, Ziegler worked for a private company that had a clear policy in technology use. It explained that equipment and software were company-owned, to be used for business purposes only, and that employees' e-mails would be constantly monitored. The FBI received a complaint from the firm's Internet provider that Ziegler had accessed child pornography from a company computer and requested access to his computer. 14 The employer consented to the request. The court held that the employer had the right to consent to the search because the computer was workplace property and the contents of Ziegler's hard drive were work-related items that contained business information and that were provided to, or created by, the employee in the context of a business relationship. Ziegler's downloading of personal items (pornography) did not destroy the employer's common authority over the computer given the company's policies that informed employees that electronic devices were company-owned and subject to monitoring—two key components necessary to the reasonable expectation element in any employment context.¹⁵

When an employee is detained during a search, the employer may have a claim for *false imprisonment*, which is defined as a total restraint on freedom to move against the employee's will, such as keeping an employee in one area of an office. The employee need not be "locked" into the confinement to be restrained; but when the employee remains free to leave at any time, there is no false imprisonment.

The Fifth and Fourteenth Amendments

The Fifth and Fourteenth Amendments also protect a government employee's right to privacy in that the state may not restrict one's rights unless it is justified.

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 667

For instance, the Supreme Court has consistently held that everyone has a fundamental right to travel, free of government intervention. Where the state attempts to infringe on anything that has been determined to be a fundamental right, that infringement or restriction is subject to the strict scrutiny of the courts. For the restriction to be allowed, the state must show that the restriction is justified by a compelling state interest. Moreover, the restriction must be the least intrusive alternative available.

On the other hand, for those interests not deemed by the courts to constitute fundamental rights, a state may impose any restrictions that can be shown to be rationally related to a valid state interest, a much more lenient test.

To determine whether the state may restrict or intrude on an employee's privacy rights, it must first be determined whether the claimed right is fundamental. Two tests are used to make this determination. First, the court may look to whether the right is "implicit in the concept of ordered liberty, such that neither liberty nor justice would exist if [the rights] were sacrificed." Second is whether the right is "deeply rooted in this Nation's history and tradition."

While conception, child rearing, education, and marriage have been held to be within the area of privacy protected by the Constitution, other issues have not yet been addressed or determined by the Court, including the right to be free from mandatory pre-employment medical tests. Moreover, the Court has found no general right of the individual to be left alone.

The Privacy Act of 1974

Governmental intrusion into the lives of federal employees is also restricted by the Privacy Act of 1974. Much of the discussion in the area of employee privacy is framed by governmental response to the issue, both because of limitations imposed on the government regarding privacy and because of the potential for abuse. The Privacy Act of 1974 regulates the release of personal information about federal employees by federal agencies. Specifically, but for 11 stated exceptions, no federal agency may release information about an employee that contains the means for identifying that employee without the employee's prior written consent. (See Exhibit 13.2, "Privacy Act of 1974.")

There are four basic principles that underlie the Privacy Act:

- 1. Employees should have access to their own personnel files, and there should be some way for them to find out the purposes for which the files are being
- 2. There should be some mechanism by which an employee may correct or amend an inaccurate record.
- 3. The employee should be able to prevent information from being inappropriately revealed or used without her or his consent, unless such disclosure is required by law.
- 4. The person who is in charge of maintaining the information must ensure that the files are not falling into the wrong hands and that the information contained within the files is accurate, reliable, and used for the correct reasons.

© The McGraw-Hill Companies, 2009

668 Part Three Regulation of the Employment Environment

Exhibit 13.2 Privacy Act of 1974

PRIVACY ACT OF 1974

No Agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be

- 1. To those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.
- 2. Required under section 552 of this title; (the Freedom of Information Act). (Note that this act does not apply to "personnel, medical, and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.")
- 3. Or a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section; (a purpose that is specifically compatible with the purpose for which the information was gathered).
- 4. To the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity. . . .
- 5. To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.
- 6. To the National Archives of the United States as a record which has sufficient historical or

- other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value.
- 7. To another federal agency or to an instrumentality of any government jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.
- 8. To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.
- To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee or subcommittee of any such joint committee.
- 10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office.
- 11. Pursuant to the order of a court of competent jurisdiction.

By affording the employee with these rights, Congress has effectively put the right of disclosure of personal information in the hands of the employee, at least when none of the 11 specified exceptions applies.

When one of the Privacy Act exceptions applies, the act dismisses the employee consent requirement, which gives the agency total control over the use of the file. The right to privacy is not absolute; the extent of protection varies with the extent of the intrusion, and the interests of the employee are balanced against the interests of the employer. Basically, the information requested under either the Privacy

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 669

Act or the Freedom of Information Act is subject to a balancing test weighing the need to know the information against the employee's privacy interest.

The Ninth Circuit Court of Appeals has developed guidelines to assist in this balancing test. The court directs that the following four factors be looked to in reaching a conclusion relating to disclosure:

- 1. The individual's interest in disclosure of the information sought.
- 2. The public interest in disclosure.
- 3. The degree of invasion of personal privacy.
- 4. Whether there are alternative means of getting the information.

Critics of the act suggest that it is enormously weakened as a result of one particular exemption that allows disclosure for "routine use" compatible with the reason the information was originally collected. In addition, certain specific agencies are exempted. For instance, in March 2003, the Department of Justice exempted the National Crime Information Center, which is a resource for 80,000 law enforcement agencies.

The Privacy Act grants employees two options for relief: criminal penalties and civil remedies, including damages and injunctive relief. The act also allows employees who are adversely affected by an agency's noncompliance to bring a civil suit against the agency in federal court.

Privacy Protection Study Commission

The Privacy Protection Study Commission was formed by Congress with the purpose of studying the possibility of extending the Privacy Act to the private sector. In 1977, the commission concluded that the Privacy Act should not be extended to private employers but that private-sector employees should be given many new privacy protections. The suggested protections required a determination of current information-gathering practices and their reasons, a limitation on the information that may be collected to what is relevant, a requirement that the employer inform its employees to ensure accuracy, and a limitation on the usage of the information gathered both internally and externally.

The commission further found that certain issues demanded federal intervention and, for this reason, recommended that (1) the use of polygraph tests in employment-related issues be prohibited; (2) pretext interviews be prohibited; (3) the use of arrest or criminal records in employment decisions be prohibited except where otherwise allowed or required by law; (4) employers be required to use reasonable care in selection of their investigating agencies; and (5) the Federal Fair Credit Reporting Act provisions be strengthened. These recommendations have yet to be implemented by Congress, primarily due to private employers' vocal rejection of such an extension of federal law due to the cost of the implementation of the recommendations.

The commission has since established three general policy goals: (1) to attempt to create a balance between what an employee will divulge to the recordkeeping department and what that employee seeks in return for his or her information;

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

670 Part Three Regulation of the Employment Environment

(2) to find a manner by which to ensure fairness to all employees, in that the information that has been processed will not be used against them; and (3) to create and define rules regarding the type of information that may be disclosed and those to whom the information may be given.

Many large corporations have embraced privacy protection programs on their own in accordance with recommendations from the Privacy Commission and in anticipation of federal regulation. In light of this advance implementation, the Privacy Commission recommends that any program guarantee five basic employee procedural rights. The list includes

- Notice
- Authorization
- Access
- Correction
- Confidentiality

Though the list seems rather specific, the problem lies within the depth and scope of each component.

Federal Wiretapping—Title III

Title III, as amended (particularly by the Electronic Communications Privacy Act of 1986, discussed below), is codified at 18 U.S.C. §§ 2510–2521. These statutes provide privacy protection for and govern the interception of oral, wire, and electronic communications. Title III covers all telephone communications regardless of the medium, except that it does not cover the radio portion of a cordless telephone communication that is transmitted between the handset and base unit. The law authorizes the interception of oral, wire, and electronic communications by investigative and law enforcement officers conducting criminal investigations pertaining to serious criminal offenses, or felonies, following the issuance of a court order by a judge. The Title III law authorizes the interception of particular criminal communications related to particular criminal offenses. In short, it authorizes the acquisition of evidence of crime. It does not authorize noncriminal intelligence gathering, nor does it authorize interceptions related to social or political views.

Thirty-seven states have statutes permitting interceptions by state and local law enforcement officers for certain types of criminal investigations. All of the state statutes are based upon Title III, from which they derive. These statutes must be at least as restrictive as Title III, and in fact most are more restrictive in their requirements. In describing the legal requirements, we will focus on those of Title III since they define the baseline for all wiretaps performed by federal, state, and local law enforcement agencies. In recent years, state statutes have been modified to keep pace with rapid technological advances in telecommunications. For example, New Jersey amended its electronic surveillance statute in 1993 to include cellular telephones, cordless telephones, digital display beepers, fax transmissions, computer-to-computer communications, and traces obtained through caller-ID.

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 671

Wiretaps are limited to the crimes specified in Title III and state statutes. Most wiretaps are large undertakings, requiring a substantial use of resources. In 1992, the average cost of installing intercept devices and monitoring communications was \$46,492. Despite budget constraints and personnel shortages, law enforcement conducts wiretaps as necessary, but obviously, because of staffing and costs, judiciously.

Electronic Communications Privacy Act (ECPA)

At first, Title III was created to combat invasion of the government for eavesdropping in large part due to the Watergate scandal in the 1970s. Originally the federal statutes targeted government eavesdropping on telephone discussion without the consent of the speakers. The federal statute required the government agents to obtain a warrant before they could intercept any oral discussions (though in 2003 no wiretap applications were denied). In late 1986, Congress increased the coverage by broadening the range of electronic communications, resulting in the ECPA.

The ECPA covers all forms of digital communications, including transmissions of text and digitalized images, in addition to voice communications on the telephone. The law also prohibits unauthorized eavesdropping by all persons and businesses, not only the government. However, courts have ruled that "interception" applies only to messages in transit and not to messages that have actually reached company computers. Therefore, the impact of the EPCA is to punish electronic monitoring only by third parties and not by employers. Moreover, the ECPA allows interception where consent has been granted. Therefore, a firm that secures employee consent to monitoring at the time of hire is immune from ECPA liability. Therefore, an employer does not violate the ECPA when it opens and reads employee e-mails on its own system. 16

Private Sector Employee Privacy

LO4

Despite the fact that public and private employers have a similar legitimate need for information about applicants and employees to make informed decisions about hiring, promotion, security, discipline, and termination, privacy rights in the private sector of employment are limited; an employee who is arbitrarily treated, but who is without a union or contract is generally left with fewer rights in the private sector environment.

The distinction between the treatment of employees in the private and public sectors is one that is created by the constitutional requirement of state action as precedent to its application. The Constitution is a limitation made to curb government excesses.

Whether there should be a right to privacy in both the public and the private sectors, employers suggest that the employee has three choices when faced with objectionable intrusions by employers: quit, comply, or object and risk termination. Employees argue that they are defenseless because of their economic

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

672 Part Three Regulation of the Employment Environment

condition and that their privacy in the private sector is subject to greater abuse precisely because there are no protections and the option to quit is unrealistic.

One explanation offered for the difference between public- and private-sector privacy protections is compliance-related costs. The implementation of the Privacy Act throughout its agencies costs the government relatively little because it is conducting self-regulation.

By contrast, ensuring compliance within the private sector requires administration of the compliance and adjudication of violations. The Privacy Protection Study Commission found that requiring an employer to change its manner of maintaining and using records can drastically increase the cost of operation.

These costs include the costs of changing employment record-keeping practices, removing relevant information from employment decisions, and implementing a social policy of employee privacy protection. These costs are not necessarily "burdensome" to the employer, however. One study found that protecting the rights of employees on a computer system could cost as little as \$4 per person. Employers' concern for compliance costs may well be an unrealistic barrier to the development of regulations for privacy rights of private-sector employees.

A second distinction between public- and private-sector employers offered to justify different privacy standards is that more stringent regulation is needed for government employees because it is common for federal agencies to be overzealous in surveillance and information gathering. Private-sector employers, in contrast, do not generally have similar resources and, therefore, are unable to duplicate these invasive activities.

Bases for Right to Privacy in the Private Sector

Private-sector employers are not bound by constitutional structures. On a state-by-state basis, however, private-sector employees may be afforded protection either by the **common law** or by statute. All but two states provide common-law tort claims to protect individual privacy, such as intrusion into seclusion. Various torts described below have developed to protect individual solitude, the publication of private information, and publications that present personal information in a false light. (See Exhibit 13.3, "U.S. Companies with Operations in Europe Must Comply with Data Protection Laws," for the manner in which privacy protection is handled somewhat differently in the European context.)

Statutory Claims

State legislatures have responded to the issue of private-sector employee privacy in one of four ways:

- 1. Enacting legislation mirroring federal law regarding the compilation and dissemination of information.
- 2. Recognizing a constitutional right to privacy under their state constitutions, as in California, Illinois, and Arizona. For example, California appellate courts have found that employees terminated for refusing to submit to drug tests were wrongfully discharged in violation of the state's constitutional guarantee of a right to privacy, which requires employers to demonstrate a compelling

common law

Law made and applied by judges, based on precedent (prior case law). **Chapter Thirteen** The Employee's Right to Privacy and Management of Personal Information 673

Exhibit 13.3 U.S. Companies with Operations in Europe Must Comply with Data Protection Laws

The European Union's approach to data privacy is completely alien to American companies. But, as a recent decision from CNIL (Commission Nationale de l'Informatique et des Libertés, the French Data Protection Authority) makes clear, an American company with operations in Europe that does not learn how to play by European rules runs a serious risk of getting slapped with a hefty fine.

[T]he European Union's Directive governing the protection of individuals' personal data and the processing of such data mandates that the member nations adopt laws that cover *all* "processing" (defined to include even collection and storage) of data about personally-identifiable individuals. The EU Directive includes provisions addressing, among other things, limitations on the use of date [sic], data accuracy, and data destruction requirements. The Directive is not limited to electronic or computerized data, and therefore reaches written, Internet, and even oral communications.

The EU Directive offers a blueprint for data privacy laws across Europe but, in any given situation, the Directive itself is not legally binding. As to each specific data privacy issue arising within Europe, the *relevant country's* local statue [sic] that adopts ("transposes") the Directive will determine data privacy rights an[d] responsibilities.

The Extraterritorial Reach of the EU's Data Privacy Directive Means That Any Company with Operations in Europe Must Comply; Cross-Border Data Transfer Is Particularly Thorny

An important aspect of the Directive for businesses headquartered outside of Europe, such as in the U.S., is the Directive's extraterritorial reach. The Directive specifically prohibits sending personal data to any country without a "level of [data] protection" considered "adequate" by EU standards. Significantly, the EU has ruled that the United States, with its patchwork of privacy laws, does *not* possess an adequate level of data protection.

The directive authorizes a number of exceptions, legally permitting transmission of personal

data outside of Europe even to a "third country" that fails to offer an "adequate level of protection."

Exceptions Permitting Cross-Border Transfers of Personal Data

The EU recognizes three "transborder data flow vehicles": (i) a company can self-certify with the U.S. Department of Commerce that it adheres to specified data protection principles (known as the "safe harbor" system); (ii) a company can enter into "model contracts" with its European subsidiaries, agreeing to abide by mandatory data protection provisions; or (iii) a company can develop a set of "binding corporate rules"—company-drafted data protection regulations that apply throughout the company, which must be ratified by each EU member state's data protection authority. Failure to implement at least one of these methods could result in significant liability.

Obtaining the data subject's free, unambiguous consent to transmit his or her data overseas is theoretically another permissible way in which to transfer data to a country outside the EU—even to a country without comparable data protection law—provided that the consent specifically lists the categories of data and the purposes for the processing outside the EU. Practically speaking, however, obtaining consent to legitimize a transfer overseas is often not an available alternative for employers; in the employment context, because of the imbalance in bargaining power between employer and employee, consents may be presumed *not* to have been freely given.

Also, of course, there is no prohibition against transmitting genuinely *anonymized* data out of the EU. Where the identity of the data subject is impossible to determine, the data transmission falls outside the scope of the directive.

Source: Labor & Employment Practice Group, Proskauer Rose LLP © 2008. Reprinted with permission.

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

674 Part Three Regulation of the Employment Environment

interest in invading an employee's privacy. In Pennsylvania, a court held that a drug test violates that state's policy against invasions of privacy where the methods used do not give due regard to the employee's privacy or if the test results disclose medical information beyond what is necessary. Other states that provide constitutional recognition and protection of privacy rights include Alabama, Florida, Hawaii, Louisiana, Montana, South Carolina, and Washington. However, in all states except California, application of this provision to private-sector organizations is limited, uncertain, or not included at all.

- 3. Protecting employees only in certain areas of employment, such as personnel records or the use of credit information.
- 4. Leaving private-sector employees to fend for themselves while the federal laws and the Constitution afford protection to federal employees and those subject to state action.

Tort Law Protections/Common Law

As mentioned above, courts in almost all states have developed case law, the "common law," which identifies certain torts in connection with private-sector invasion of privacy. Georgia was the first jurisdiction whose courts recognized a common-law right to privacy. As the court explained in *Pavesich v. New England Life Ins. Co.*, ¹⁷ "a right of privacy is derived from natural law, recognized by municipal law, and its existence can be inferred from expressions used by commentators and writers on the law as well as judges in decided cases. The right of privacy is embraced within the absolute rights of personal security and personal liberty." Though some states rely on statutory protections rather than common law, only two states—North Dakota and Wyoming—fail to recognize *any* of the four privacy torts discussed in this chapter. ¹⁸ A **tort** is a legal wrong, for which the law offers a remedy. The torts of particular interest in this chapter include intrusion into solitude or seclusion, the publication of private information, and publication that places another in a false light. Defamation also will be discussed.

Publication as used in these torts means not only publishing the information in a newspaper or other mass media but generally "bringing it to light" or disseminating the information. In addition, the concept of publication is defined slightly differently depending on the tort. Truth and absence of malice are generally not acceptable defenses by an employer sued for invasion of an employee's privacy. They are acceptable, however, in connection with claims of defamation.

LO5

Intrusion into Seclusion To state a prima facie case for the tort of intrusion into seclusion, the plaintiff employee must show that

- The defendant employer intentionally intruded into a private area.
- The plaintiff was entitled to privacy in that area.
- The intrusion would be objectionable to a person of reasonable sensitivity.

tort

Private (civil) wrong against a person or her or his property.

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 675

The intrusion may occur in any number of ways. An employer may

- Verbally request information as a condition of employment.
- Require that its employees provide information in other ways such as through polygraphs, drug tests, or psychological tests.
- Require an annual medical examination.
- Ask others personal information about its employees.
- Go into private places belonging to the employee.

Any of these methods may constitute a wrongful invasion where it so invades the employee's private sphere that it would be objectionable to a reasonable person. On the other hand, if the employer can articulate a justifying business purpose for the inquiry/invasion, the conduct is more likely to be deemed acceptable.

In Rogers v. Loews L'Enfant Plaza Hotel, 19 an employee was continually sexually harassed by her supervisor, including bothersome telephone calls to her home, during which he made lewd comments to her about her personal sex life. The sexual harassment evolved into harassment in the workplace, where the supervisor verbally abused her in front of her co-workers, kept important business-related information from her, and refused to include her in meetings. Her employer, refusing to take formal action, suggested that she change positions. The court determined that the telephone calls were not of a benign nature but, instead, were unreasonably intrusive and not normally expected. Further, the harassment constituted an intrusion into a sphere from which the employee could reasonably exclude the defendant. On these bases, the court found in favor of the employee.



In connection with opening scenario 1, Aravinda's decision in connection with the HIV tests may be governed in part by the law relating to employment testing as discussed in Chapter 3 and in part by the law relating to disability discrimination as discussed in Chapter 12 (since HIV is considered a disability under the Americans with Disabilities Act). On the other hand, the law relating to intrusion into seclusion also would have application here in terms of disclosure of the test results. If Aravinda discloses the results to anyone or, through her actions, leads someone to a belief about the employee's HIV status, she might be liable under this tort. In addition, it is important to consider that it is highly unlikely that Aravinda has any right to know any employee's HIV status as it is unlikely that the information would be job-related. (Can you imagine what employment position might warrant this type of information? Is HIV status ever considered jobrelated?) Consider the application of the prima facie case for intrusion into seclusion as you review Michael A. Smyth v. The Pillsbury Company, included at the end of chapter. The court in that case considers the nature of a reasonable expectation of privacy, as well as why an employer might wish to intercept e-mails.



Public Disclosure of Private Facts To state a prima facie case for the tort of public disclosure of private facts, the plaintiff employee must show that

676 Part Three Regulation of the Employment Environment

- There was an intentional or negligent public disclosure
- · Of private matters, and
- Such disclosure would be objectionable to a reasonable person of ordinary sensitivities.

The information disclosed must not already be publicized in any way, nor can it be information the plaintiff has consented to publish. Therefore, in *Pemberton v. Bethlehem Steel Corp.*, ²⁰ publication of an employee's criminal record did not constitute public disclosure of private facts because the criminal record did not contain private facts; it was information that was already accessible by the public.

As you shall see, at the end of the chapter, in the *Yoder v. Ingersoll-Rand Company a.k.a. ARO* case, the publication also must be made public, which involves more than mere disclosure to a single third party. The public disclosure must be communication either to the public at large or to so many people that the matter must be regarded as substantially certain to become one of public knowledge or one of knowledge to a particular public whose knowledge of the private facts would be embarrassing to the employee. Therefore, publication to all of the employees in a company may be sufficient, while disclosure to a limited number of supervisors may not.

Several states have enacted legislation codifying this common-law doctrine under the rubric of "breach of confidentiality." Connecticut, for instance, has passed legislation requiring employers to maintain employee medical records separate from other personnel records. Other states have limited an employer's ability to disclose personnel-related information or allowed a cause of action where, through the employer's negligent maintenance of personnel files, inaccurate employee information is communicated to a third party.

Publication in a False Light The prima facie case of publication in a false light requires that there was a public disclosure of facts that place the employee in a false light before the public if the false light would be highly offensive to a reasonable person and the person providing the information had knowledge of or recklessly disregarded the falsity or false light of the publication.

Voluntary consent to publication of the information constitutes an absolute bar to a false-light action. This type of tort differs from defamation, where disclosure to even one other person than the employer or employee satisfies the requirements. The tort of publicizing someone in a false light requires that the general public be given a false image of the employee. In a false-light action, the damage for which the employee is compensated is the inability to be left alone, with injury to one's emotions and mental suffering, while defamation compensates the employee for injury to his or her reputation in the public's perception.

Note that any of the above claims may be waived by the employee if the employee also publishes the information or willingly or knowingly permits it to be published. For example, in *Cummings v. Walsh Construction Co.*, ²¹ the employee complained of public disclosure of embarrassing private facts, consisting of information relating to a sexual relationship in which she was engaged with



III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 677

her supervisor. The court held that, where the employee had informed others of her actions, she waived her right not to have her supervisor disclose the nature of their relationship.

As with defamation, an exception to this waiver exists in the form of compelled self-publication, where an employer provides the employee with a false reason as the basis for termination and the employee is compelled to restate this reason when asked by a future employer the basis of departure from the previous job. Therefore, where the employer intentionally misstates the basis for the discharge, that employer may be subject to liability for libel because it is aware that the employee will be forced to repeat (or "publish") that reason to others.

Breach of Contract An employee also may contest an invasion of privacy by her or his employer on the basis of a breach of contract. The contract may be an actual employment contract, collective bargaining agreement, or one found to exist because of promises in an employment handbook or a policy manual.

Defamation Libel refers to defamation in a written document, while slander consists of defamation in an oral statement. Either may occur during the course of a reference process. And, while the prima facie case of defamation requires a false statement, even a vague statement that casts doubt on the reputation of an individual by inference can cause difficulties for an employer if it cannot be substantiated.

The elements of a claim for defamation include

- False and defamatory words concerning employee,
- Negligently or intentionally communicated to a third party without the employee's consent (publication), and
- Resulting harm to the employee defamed.

One cautious solution to this problem area is to request that all employees fill out an exit interview form that asks, "Do you authorize us to give a reference?" If the applicant answers yes, she or he should be asked to sign a release of liability for the company.

Ordinarily defamation arises from someone other than the defamed employee making defamatory statements about an employee; but one interesting form of defamation has evolved over the past decade where an employee is given a false or defamatory reason for her or his discharge. In that case, the employee is the one who is forced to publicize it to prospective employers when asked for the reason for her or his discharge. These circumstances give rise to a cause of action for defamation, termed compelled self-disclosure, because the employee is left with no choice but to tell the prospective employer the defamatory reasons for her or his discharge. Barring this result, the employee would be forced to fabricate reasons different from those given by the former employer and run the risk of being reprimanded or terminated for not telling the truth. This cause of action has been recognized, however, only in Colorado, Iowa, Minnesota, Connecticut, and California. (For a more detailed discussion, see Chapter 3.)

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

678 Part Three Regulation of the Employment Environment

An employer may defend against an employee's claim of defamation by establishing the truth of the information communicated. While truth is a complete defense to defamation, it can be difficult to prove without complex paper management.

Employers also may be immune from liability for certain types of statement because of court-recognized privileges in connection with them. For example, in some states, an employer is privileged to make statements, even if defamatory, where the statement is made in the course of a judicial proceeding or where the statement is made in good faith by one who has a legitimate business purpose in making the communication (e.g., ex-employer) to one who has a business interest in learning the information (e.g., a prospective employer). This privilege would apply where a former employer offers a good-faith reference to an employee's prospective employer. (See additional discussion of liability for references, below.) "Good faith" means that the employer's statement, though defamatory, is not made with malice or ill will toward the employee.

Regulation of Employee's Off-Work Activities

L06

Employers may regulate the off-work or otherwise private activities of their employees where they believe that the off-work conduct affects the employee's performance at the workplace. This legal arena is a challenging one since, in the at-will environment, employers can generally impose whatever rules they wish. However, as discussed earlier in this chapter, they may then run afoul of common-law privacy protections. In addition, some states have enacted legislation protecting against discrimination on the basis of various off-work acts. For instance, New York's lifestyle discrimination statute prohibits employment decisions or actions based on four categories of off-duty activity: legal recreational activities, consumption of legal products, political activities, and membership in a union.

Across the nation, there are other less-broad protections of off-work acts. A number of states have enacted protections specifically on the basis of consumption or use of legal products off the job, such as cigarettes.²³ These statutes originated from the narrower protection for workers who smoked off-duty. Currently, abstention from smoking cannot be a condition of employment in at least 29 states and the District of Columbia (and those states provide antiretaliation provisions for employers who violate the prohibition). In fact, instead of simply identifying the right to use lawful products outside of work, Rhode Island goes further by specifically prohibiting an employer from banning the use of tobacco products while not at work. Some states have responded a bit differently. In Georgia, for instance, certain state workers are charged an additional premium of \$40 per month in connection with their state-provided health insurance if they or a covered family member uses tobacco products. While the policy is based on an affirmative response to a simple survey question, any employee who misleads the system will lose her or his health coverage for an entire year. The State of Georgia is not alone; a survey by the Society for Human Resource Management found

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 679

that 5 percent of firms charge a similar premium while 32 percent of firms offer smoking cessation programs as an alternate means by which to reduce costs.

You might be asking yourself, though, how do these firms know? What happens if employees lie about their habits? Alaska Airlines uses a pre-employment urine screening and will not even hire candidates if they are smokers.²⁴ For an alternate approach, in what might seem like a program destined for problems, Whirlpool Corporation had imposed a \$500 surcharge on employees who smoked—or at least those who admitted to being smokers—based on its increased benefits costs. When thirty-nine individuals who had not paid the surcharge, thus claiming to be non-smokers, were observed smoking in the firm's designated smoking areas, they were suspended by Whirlpool for lying. Presumably, they also owed the surcharge.²⁵

On the other hand, the issue of weight is handled slightly differently than smoking. Employers are not prohibited from making employment decisions on the basis of weight, as long as they are not in violation of the Americans with Disabilities Act (ADA) when they do so (see Chapter 12). The issue depends on whether the employee's weight is evidence of or due to a disability. If so, the employer will need to explore whether the worker is otherwise qualified for the position, with or without reasonable accommodation, if necessary. If the individual cannot perform the essential functions of the position, the employer is not subject to liability for reaching an adverse employment decision. However, employers should be cautious in this regard since the ADA also protects workers who are not disabled but who are perceived as being disabled, a category into which someone might fall based on her or his weight.

One recent trend with regard to weight is to offer incentives to encourage healthy behavior. Some employers have adopted health plans with significantly lower deductibles for individuals who maintain healthier lifestyles (if an employee is not obese or does not smoke, and has yearly physicals). In one audacious statement along these lines, a hospital in Indiana has begun to require its employees to pay as much as \$30 every two weeks unless they meet certain companydetermined weight, cholesterol, and blood-pressure guidelines.²⁶

Laws that protect against discrimination based on marital status exist in just under half of the states. However, though a worker might be protected based on marital status, she or he is not necessarily protected against adverse action based on the identity of the person to whom she or he is married. For instance, some companies might have an antinepotism policy under which an employer refuses to hire or terminates a worker based on the spouse working at the same firm, or a conflict-of-interest policy under which the employer refuses to hire or terminates a worker whose spouse works at a competing firm.

Since about one-third of workers have dated an office colleague, policies and attitudes on workplace dating have the greatest impact.²⁷ Though only about 12 percent of workplaces have policies prohibiting workplace dating, ²⁸ a New York decision reaffirms the employer's right to terminate a worker on the basis of romantic involvement. In McCavitt v. Swiss Reinsurance America Corp., 29 the court held that an employee's dating relationship with a fellow officer of the 680 Part Three Regulation of the Employment Environment

corporation was not a "recreational activity" within the meaning of a New York statute that prohibited employment discrimination for engaging in such recreational activities. The employee contended that, even though "[t]he personal relationship between plaintiff and Ms. Butler has had no repercussions whatever for the professional responsibilities or accomplishments of either" and "Swiss Re... has no written anti-fraternization or anti-nepotism policy," he was passed over for promotion and then discharged from employment largely because of his dating. The court agreed with the employer and found that dating was not a recreational activity.

The majority of states protect against discrimination on the basis of political involvement, though states vary on the type and extent of protection. Finally, lifestyle discrimination may be unlawful if the imposition of the rule treats one protected group differently than another. For instance, as discussed elsewhere, if an employer imposes a rule restricting the use of peyote in Native American rituals that take place during off-work hours, the rule may be suspect and may subject the employer to liability. Similarly, the rule may be unlawful if it has a disparate impact on a protected group.

Most statutes or common-law decisions, however, provide for employer defenses for those rules that (a) are reasonably and rationally related to the employment activities of a particular employee, (b) constitute a bona fide occupational requirement, or (c) are necessary to avoid a conflict of interest or the appearance of conflict of interest. For example, drug testing in positions that affect the public safety, such as bus driver, would not constitute an unlawful intrusion because the employer's interest in learning of that information is justified. Where the attempted employer control goes beyond the acceptable realm, courts have upheld an exception to the employment-at-will doctrine based on public policy concerns for personal privacy or, depending on the circumstances, intentional infliction of emotional distress.³⁰



In connection with opening scenario 2, does Abraham have to quit his night-time dancing job? Recall that Abraham is an at-will employee, making the answer somewhat easier. Since he can be terminated for any reason, as long as it is not a wrongful reason, the partner can impose this condition. But consider Abraham's arguments and the ethical, as well as the legal, implications. As long as Abraham can show that his dancing truly has no impact on his work (i.e., that the club is located in a different town from that of his clientele or that the club has an excellent reputation for beautiful, artistic dancing styles), then he would not have to quit his night job. On the other hand, if Abraham's reputation is soiled by his connection with this club and his boss can show that his work has a negative impact on his ability to perform, then she may be justified in her ultimatum.

In fact, in a case (albeit more extreme) from Arizona, a husband and wife who worked as nurses were fired from a hospital after hospital officials learned that they ran a pornographic Web site when not at work. The couple explained that they engaged in this endeavor in order to save more money for their children's college education. "We thought we could just do this and it really shouldn't be a big deal," said the husband.³¹ Though their dismissal attracted the attention of the

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 681

American Civil Liberties Union for what it considered was at-will gone awry, the nurses had no recourse. In another case, a police office was docked three days' pay when his wife posted nude pictures of herself on the Internet as a surprise to her husband. However, the pay suspension was justified by the department in that case since police officers could arguably be held to a higher standard of conduct than average citizens.

What about the well-intentioned employer who believes that employees who smoke cigarettes will benefit from a "no smoking any time, anywhere" policy? The employer also may be concerned about the financial impact of disease and other health problems related to smoking. The employer may first encounter obstacles in applying this policy in the workplace itself: Some states specifically prohibit discrimination against smokers in employment. Other states regulate smoking in the workplace only in government agencies or public buildings that are also workplaces. Of course, there are other states, like California, that prohibit smoking in all enclosed places of employment and require employers to warn of any toxic substances in the workplace, including tobacco smoke.³²

The problem in enforcement would grow as the employer tries to encourage or require employees to quit smoking altogether. How would the employer know whether the employees are smoking when not at the workplace? Would the employer's desire to have healthy employees support the intrusion into employees' decisions regarding their own health? Employers who seek to establish an exercise or "healthy eating" program may encounter similar issues. Emphasizing the work-related benefits of such a program and limiting its reach to the workplace (e.g., creating an exercise room at work where employees may take their breaks if they choose) may allow the employer to reach its goal of a healthier workforce. For more information about this issue, see Exhibit 13.4, "Legal Restrictions on Off-Duty Behavior of Private Employee."



The French v. United Parcel Service, Inc. case, provided for your review, explores the intersection of an employee's privacy rights with the employer's interest in regulating the working environment, however broadly it defines that scope. As you consider the facts of that case, try to put yourself in the place of an employer who sincerely strives to create the safest workplace, the most supportive working environment, and a sense among its workforce that employees can rely on the employer to protect them from external (or internal) threats to their safety. How would you foster that environment without excessively regulating off-duty activities or unduly invading the private lives of your workers?

Employer's Information-Gathering Process/Justified Use/ Disclosure of Information

The above discussion focused on the scope of the privacy rights of the employee in connection with the dissemination of information. Privacy, however, can be invaded not only by a disclosure of specific types of information but also by the process by which the information has been obtained. An employer may be liable

Bennett-Alexander-Hartman:
Employment Law for
Business. Sixth Edition

Moonlighting

Social relationships

with employees

of a competitor

13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

48 states allow employers

to regulate moonlighting

48 states allow employers

to regulate

682 Part Three Regulation of the Employment Environment

Off-Duty Behavior of Private Employee	Business Justification	State Statutory Restrictions on Employer Policy
Illicit drug use	Concern that worker may come to work impaired, jeopardizing the worker's safety and the safety of other workers	46 states allow employers to test for illicit drugs
	Quality of work of impaired worker may affect the product or service provided by the company, which, in turn, can affect the business's reputation and profitability	
	Conduct is illegal and not deserving of legal protection	
Alcohol use	Same justifications as applied to those who use illicit drugs, except for the issue of legality	40 states allow employers to regulate off-duty alcohologous consumption
Cigarette smoking	Smokers increase employer's healthcare costs and affect productivity by missing more work due to illness than nonsmokers	22 states allow employers to prohibit off-duty use of tobacco products
Use of weight standards	Same justifications as apply to smokers	49 states allow employers to establish weight stan- dards that do not violate the ADA
Dating between employees	A romantic relationship between employees may affect their productivity	48 states allow employers to regulate dating between employees
	The relationship could lead to sexual harassment charges against the employer, especially if one employee is a supervisor of the other	
	Other employees may believe that an involved supervisor is showing favoritism and may then feel that they are victims of discrimination	

Source: Reprinted with permission from John D. Pearce II and Dennis Kuhn, "The Legal Limits of Employees' Off-Duty Privacy Rights," *Organizational Dynamics* 32, no. 4 (2003), pp. 372–83, 376.

Working too many hours may impair worker's

Working for a competitor could jeopardize privacy

Concern that information could be exchanged that

productivity

of employer information

would cause harm to the business

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 683

for its process of information gathering, storing, or utilization. Improper gathering of information may constitute an invasion where the process of collection constitutes harassment, where improper filing or dissemination of the information collected may leave the employer liable for defamation actions, and/or where inappropriate use of data for other purposes than those for which the information was collected may inflict other harms.

A final concern is called *function creep* and may begin with the voluntary transmission of information by an individual for one purpose for which the individual consents. For instance, an individual may offer personal information to her or his employer without understanding or intending that the employer then share more information than required with the Immigration and Naturalization Service. Similarly, information gathered during a preemployment physical for purposes of appropriate job placement may seem perfectly appropriate to share with an employer; but, the employee might have concerns if that information is later shared with her or his manager or co-workers for other purposes.

The collection or retrieval of information may occur in a variety of ways, depending on the stage of employment and the needs of the employer. For example, an employer may merely make use of the information provided by an applicant on her or his application form, or it may telephone prior employers to verify the data provided by the applicant. One employer may feel confident in an employee's educational background when she sees the employee's diplomas hung on the office wall, while a different employer may feel the need to contact prior educational institutions to verify attendance and actual graduation. On the more lenient end of the spectrum, the employer may rest assured that the employee is all that he states that he is on the application form, while, in more extreme situations, an employer may subject its employees to polygraph analyses and drug tests.

As is covered extensively in other chapters, employers are limited in the questions that may be asked of a potential employee. For example, an employer may not ask an applicant whether she or he is married or plans to have children, or the nature of her or his family's origin. These questions are likely to violate Title VII of the Civil Rights Act; in most cases this is not because the employer should not have the information, literally, but instead because an employer is prohibited from reaching any employment decision on the basis of their answers. In addition, employers are limited in their collection of information through various forms of testing, such as polygraphs or medical tests. These are discussed further in Chapter 3, but employers are constrained by a business necessity and relatedness standard or, in the case of polygraphs, by a requirement of reasonable suspicion. With regard to medical information specifically, employer's decisions are not only governed by the Americans with Disabilities Act but also restricted by the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191). HIPAA stipulates that employers cannot use "protected health information" in making employment decisions without prior consent. Protected health information includes all medical records or other individually identifiable health information. (See Exhibit 13.5, "Protecting Workers' Personal Data.")

In connection with the storage of the information collected, employers must be careful to ensure that the information is stored in such a manner that it will 684 Part Three Regulation of the Employment Environment

Exhibit 13.5 Protecting Workers' Personal Data

In 1997, the International Labour Organization published a Code of Practice on the Protection of Workers' Personal Data. Though not binding on employers, they serve to help codify ethical standards in connection with the collection and use of employee personal information. The code includes, among others, the following principles:

5. GENERAL PRINCIPLES

- 5.1 Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.
- 5.2 Personal data should, in principle, be used only for the purposes for which they were originally collected....
- 5.4 Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behavior of workers.
- 5.5 Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.
- 5.6 Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance. . . .
- 5.8 Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights. . . .
- 5.10 The processing of personal data should not have the effect of unlawfully discriminating in employment or occupation. . . .
- 5.13 Workers may not waive their privacy rights.

6. COLLECTION OF PERSONAL DATA

- 6.1 All personal data should, in principle, be obtained from the individual worker.
- 6.2 If it is necessary to collect personal data from third parties, the worker should be informed in advance, and give explicit consent. The employer should indicate the purposes of the processing, the sources and means the

- employer intends to use, as well as the type of data to be gathered, and the consequences, if any, of refusing consent. . . .
- 6.5 An employer should not collect personal data concerning a worker's sex life; political, religious, or other beliefs; or criminal convictions. In exceptional circumstances, an employer may collect personal data concerning those in named areas above if the data are directly relevant to an employment decision and in conformity with national legislation.
- 6.6 Employers should not collect personal data concerning the worker's membership in a workers' organization or the worker's trade union activities, unless obliged or allowed to do so by law or a collective agreement.
- 6.7 Medical personal data should not be collected except in conformity with national legislation, medical confidentiality and the general principles of occupational health and safety, and only as needed to determine whether the worker is fit for a particular employment; to fulfill the requirements of occupational health and safety; and to determine entitlement to, and to grant, social benefits. . . .
- 6.10 Polygraphs, truth-verification equipment or any other similar testing procedure should not be used.
- 6.11 Personality tests or similar testing procedures should be consistent with the provisions of this code, provided that the worker may object to the testing.
- 6.12 Genetic screening should be prohibited or limited to cases explicitly authorized by national legislation.
- 6.13 Drug testing should be undertaken only in conformity with national law and practice or international standards.

11. INDIVIDUAL RIGHTS

11.1 Workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

continued

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 685

- 11.2 Workers should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual worker or in any other file which includes workers' personal data.
- 11.3 The workers' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that worker's personal data....
- 11.9 Workers should have the right to demand that incorrect or incomplete personal data,

- and personal data processed inconsistently with the provisions of this code, be deleted or rectified. . . .
- 11.11 If the employer refuses to correct the personal data, the worker should be entitled to place a statement on or with the record setting out the reasons for that worker's disagreement. Any subsequent use of the personal data should include the information that the personal data are disputed and the worker's statement.

not fall into the "wrong" hands. If an improper party has access to the personal information, the employer, again, may be subject to a defamation action by the employee based on the wrongful invasion of her personal affairs, as discussed above. In today's world of advanced computer data storage, new issues arise that have not been previously litigated. For instance, where an item is stored in a computer, it is crucial either to close the file to all but those who have a correct entry code or to delete private information. Access to computer terminals throughout an office creates a problem concerning the dissemination of the private information and the control of access.

The employer offering the reference is responsible for its dissemination only to appropriate parties. A fax machine or postcard would be unacceptable means of transmitting a reference since this would allow access by innumerable others. Similarly, an employer may get caught wrongfully disclosing information to an inappropriate individual in the case of the telephone reference. Failure to confirm the identity of the caller and purpose of the call may allow disclosure to one who otherwise should have no access to this information.

Electronic Monitoring or Surveillance of Employee Activities

The ACLU reports that the number of people subject to surveillance in the workplace rose from 8 million in 1991 to more than 30 million in 1997.³³ With the dramatic increase in the use of technology in the workplace, several issues have recently developed surrounding the use of e-mail and the Internet. Many state and district courts have dealt with the issues differently or have not faced them at all. On the other hand, 84 percent of companies surveyed for a 2005 report have written policies concerning e-mail use; 81 percent have Internet use policies; 23 percent have policies regarding personal postings on corporate blogs; and 15–20

686 Part Three Regulation of the Employment Environment

percent have policies that discuss the use of personal blogs on company time.³⁴ In fact, almost 10 percent of firms have fired employees for violating blogging policies.³⁵

Though, at first blush, blogs might seem an innocent environment in which employees can vent comments regarding their employment situation, imagine the impact of a viral message when placed on the Web and then allowed to have the exponential impact experienced by some blogs. Since it is estimated that blog readership is in the millions, ³⁶ corporate reputations are at stake and legal consequences can be severe; 26 percent of firms in 2007 were affected by the exposure of sensitive or embarrassing information via the Internet of e-mail. ³⁷ In one situation, a Google employee compared the firm's health plan to Microsoft's, and it did not fare too well. He also blogged about how the company's provision of free food was merely an incentive to work through the dinner hour. The employee was subsequently terminated. The term to be "dooced" refers to have lost one's job as a result of one's Web site. ³⁸ Consider the challenges involved in the implementation of a company-wide blogging policy, as discussed in Exhibit 13.6, "Bloggers Beware: New Rules for CBC Employees."

LO7

Of course, little did anyone anticipate what dilemmas would arise as a result of advances in technology over the past few decades. Who would have thought that one might begin her or his workday by placing a hand on a scanner to confirm one's identity and time of arrival at work³⁹ or that location-based technologies would allow employers to know an employee's whereabouts at all times?⁴⁰ Notwithstanding issues in connection with production, marketing, finance, and other areas of a firm's operations, we now have countless issues that intersect law and ethics with which we were never before confronted. For instance, consider the implications of new technology on the following areas:

- Monitoring usage.
- Managing employee and employer expectations.
- Distinguishing between work use and personal use of technology.
- Managing flextime.
- Maintaining a virtual workplace.
- Protecting against medical concerns for telecommuters.
- Managing/balancing privacy interests.
- Monitoring the use of the Web to spread information and misinformation.
- Managing fair use/disclosure.
- Responding to accessibility issues related to the digital divide.
- · Managing temporary workforces.
- Adapting to stress and changing systems.
- Managing liability issues.
- Maintaining proprietary information.
- Measuring performance.

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 687

Exhibit 13.6 Bloggers Beware: New Rules for CBC Employees

My name is Chris MacDonald, and I work for the Canadian Broadcasting Corporation. OK, that second part isn't true, but if it were, I might not be allowed to write this blog, or at least I wouldn't be allowed to tell you who I work for, according to a new "guideline" issued by the CBC's management. (CBC managers have asserted that it's a guideline, not a policy. As far as most of the concerns about the document are concerned, it's a spurious distinction.)

The document is not publicly available—in fact, it hasn't been officially distributed within the CBC yet—but it got leaked internally, and lots of CBC employees have seen it. It caught CBC-based bloggers off-guard; despite the fact that several of them had proactively written their own set of voluntary guidelines a few years ago, they weren't included or consulted in the process of devising the new official guideline.

According to the InsideCBC blog (an official, sanctioned, insider's blog), the new policy applies to a CBC employee's personal blog "if the content clearly associates them with CBC/Radio-Canada."

Among the requirements of the guideline/policy:

- Bloggers are "expected to behave in a way that is consistent with our journalistic philosophy, editorial values and corporate policies."
- "[T]he blog cannot advocate for a group or a cause, or express partisan political opinion. It should also avoid controversial subjects or contain material that could bring CBC/Radio-Canada into disrepute."
- To start and maintain a blog of this kind, you need your supervisor's approval.

Note, also, that the guideline/policy applies to *all* employees, not just to journalists (whose blogs might reasonably be mistaken for news) or to marquee on-air personalities.

The guideline has caused a stir among CBC-employee-bloggers and beyond.

A lot of objections have already been raised in the Comments section of the InsideCBC blog. And while some elements of the document seem

unproblematic and even constructive, I see a couple of *types* of problems with it. One has to do with content. The other has to do with process.

Content:

There are clearly a number of elements of the guideline/policy that are either unclear or unenforceable or both. For example, the stipulation that it applies to blogs "if the content clearly associates them with CBC/Radio-Canada." Several commentators have pointed out that there are lots of ways, intentional and unintentional, that a blog could associate itself with the CBC. The blogger might self-identify as a CBC employee, or merely imply or even just let slip that she or he is an employee. In terms of specific requirements, the one that has most angered those involved is the stipulation that employees must seek their supervisors' permission to write a personal blog. This seems on the face of it a pretty serious restriction on freedom of speech. Maybe (maybe) CBC has the right to make that stipulation as a matter of employment contract, but having a right to do so doesn't make it appropriate, or wise, to exercise that right.

Process

It's pretty bad that bloggers at the CBC were caught off-guard by this guideline/policy, for at least 3 reasons

- For policies and codes of all kinds, buy-in is crucial. Given how difficult this policy will be to enforce (i.e., very) it's utterly essential that the people to be governed by it accept it as legitimate and wise. Oops.
- 2) The CBC employees with blogs are a pretty smart bunch, who have thought a fair bit about what their obligations are. And, just through experience, they understand blogging better than anyone in CBC's editorial offices is going to. What a shame not to draw on that knowledge and experience. Serious error.
- 3) By drafting a document that doesn't reflect, acknowledge, or draw upon the bloggers' own manifesto, CBC management is neglecting the fact that some of their very bright employees

continued

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

688 Part Three Regulation of the Employment Environment

Exhibit 13.6 Continued

have expected considerable effort on the very issue they're now seeking to regulate. At very least that seems disrespectful.

Now that the errors have been made, the serious ethics & leadership challenge lies in whether & how CBC managers can recover. "Recovery" here means ending up with a policy that is clear and enforceable, and retaining some semblance of moral authority in the eyes of their employees.

Disclosure of potential bias: I've got a friend among the CBC-employee-bloggers affected by this new guideline/policy.

Update

According to [an] update, the document referred to above was "only a proposed early draft." (Note

that "proposed" doesn't make sense there: either it was a draft, or it wasn't.) Also according to the update, "There are currently no specific corporate policies in effect relating directly to blogging." (This update is brought to you by the nice Media Relations and Issues Management people at CBC, who asked me to correct the above posting.)

Source: Christopher MacDonald, "Bloggers Beware: New Rules for CBC Employees," August 6, 2007, http://www.businessethics.ca/blog/2007/08/bloggers-beware-new-rules-for-cbc.html. © Christopher MacDonald, reprinted with permission.

Author's note: The blog that includes the text of the CBC update mentioned above also includes the original text of the introduction to the blogging policy that indicates nowhere that the document contained "proposed" guidelines. Instead, it said, "[a]ttached are personal blogging guidelines the Editor in Chief's office distributed a while back."

In order to better understand the impact of new technology on these segments of our working environment, it is critical to comprehend the nature of that technology and its capabilities. For instance, while you might expect that location-based technologies such as a radio frequency identification device (RFID) might be used to track the activities of an employee to be sure that she or he is not slacking off, the attorney general in Mexico implanted the tiny devices under the skin of some of his workers in order to more effectively track them in case they were kidnapped because of their line of work.⁴¹

Though seemingly monumental on the surface, advances in the information-gathering abilities of these technologies are actually merely geometric rather than exponential. Employers have always gathered information about their employees; the only element that has changed in recent decades is how that information is collected rather than the values that underlay the decision to do so.

For instance, Milton Hershey of Hershey's Chocolate used to tour Hershey, Pennsylvania, to see how well his employees maintained their homes. He hired detectives to spy on Hershey Park dwellers in order to learn who threw trash on its lawns. Henry Ford used to condition wages on his workers' good behavior *outside the factory*, maintaining a Sociological Department of 150 inspectors to keep tabs on workers. Technology, therefore, does not present us with new value judgments but, instead, simply presents new ways to gather the information on which to base them. Sorting through these issues is challenging nevertheless. Consider the impact of September 11, 2001, on an employer's decision to share personal

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 689

employee information with law enforcement. Private firms may be more willing today to share private information than they would have been previously. Consider more specifically the issues raised above and the implications of technology on some of these traditional workplace challenges:

- Technology allows for in-home offices, raising issues of safety as well as privacy concerns; there are now more than 15.7 million U.S. telecommuters. (Efforts by OSHA in the late 1990s to impose workplace safety standards on home offices received huge flack!)
- Technology allows for greater invasions by the employer but also allows for additional misdeeds by employees.
- Technology blurs the lines between personal and professional lives.
- Technology allows employers to ask more of each employee—each is capable of much greater production.
- What constitutes a "workday"? When is enough enough?
- Should the ability to find something out make it relevant (e.g., off-work activities)?
- · Many of the new technologies (e-mail, voice mail) allow for faceless communication.
- Research has shown that excessive exertion of power and authority over employees may actually lead to insecurity, feelings of being overwhelmed and powerless, and doubts about worthiness.⁴²

"The psychological impact of constant observation is serious and represents a major assault on the ethical rights of workers. Furthermore, productivity may also be compromised as a by-product of the growth of surveillance in the workplace."⁴³

Consider the following overview of the implications of the technology economy as reported in the World Employment Report 2001, issued by the International Labour Office:

More and more, boundaries are dissolving between leisure and working time, the place of work and place of residence, learning and working. . . . Wherever categories such as working time, working location, performance at work and jobs become blurred, the result is the deterioration of the foundations of our edifice of agreements, norms, rules, laws, organizational forms, structures and institutions, all of which have a stronger influence on our behavioral patterns and systems of values than we are aware.44

Finally, intrusions may come from unexpected arenas. For instance, while employees perhaps are concerned about their rights with regard to employer monitoring in the workplace, they might contemplate the possibility of informal intrusions such as from their colleagues rather than their supervisors. In a 2007 survey of information technology employees, a security vendor found that one-third of 200 respondents admitted to having used their administrative passwords in order to access confidential employee information including compensation information.

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

690 Part Three Regulation of the Employment Environment

One of the survey respondents was quoted as saying, "Why does it surprise you that so many of us snoop around your files? Wouldn't you if you had secret access to anything you can get your hands on?" Unfortunately, this same survey reported that access continued long after many of these respondents had left their employers. Further exploration into the subject only uncovers greater vulnerabilities. In a much larger survey of more than 16,000 IT practitioners, almost two-thirds reported that they had intruded into another employee's personal computer without permission, and this number includes one-third of respondents who were at the manager level or above!

Forms of Monitoring

Monitoring in the workplace can take several forms and occurs for numerous reasons. Privacy scholar Colin Bennett identifies four types of surveillance that can specifically impact workers. 46 The first is surveillance by glitch, in which information is uncovered by mistake. This occurred, for example, when Microsoft discovered that expired Hotmail accounts retained buddy lists, which were then shared with new subscribers who were given those accounts' e-mail addresses. In the workplace, a glitch could occur when a technician checks to see if a computer's hard drive has been erased by the previous user for use by someone else. That technician might notice inappropriate content on the hard drive. A similar circumstance arose when the dean of Harvard's Divinity School asked a Harvard information management technician to do some work on his Harvard-owned laptop. The technician found inappropriate pornographic materials, and the media frenzy that erupted has only recently subsided. Oddly enough, the CFO of Mesa Airlines defended himself with pornography in a different case where he was accused of deleting company information to an ongoing lawsuit from three computers. Instead, he claimed, he was simply trying to delete files of pornography he had downloaded and that he thought might embarrass him. Funny how our concepts of the "lesser evil" shift, depending on the nature of the harm done.⁴⁷

In another example of a glitch or mistake, cheating by a worker in a government agency was discovered when the worker left a copy of a stolen promotion exam in the copying machine. Such glitches may uncover violations of a usage policy even when no systematic monitoring is being conducted.

Bennett's second form of surveillance is *surveillance by default*. This occurs when the default setting is "monitor," whereby all information that is sent through a system is caught and cataloged. An example of this type of monitoring would be the "Cue Cat." A Cue Cat is a mouse-like device that was sent to subscribers of certain magazines. They were told that they could scan bar codes in the magazine in order to gather more information on the accompanying topics later through their computers. What these users were not told was that each Cue Cat was individually coded to send subscriber information along with the information request. Therefore, the publishers or advertisers were able to surreptitiously collect data from anyone who used the device at all times. In the workplace, surveillance by default occurs when there is a video camera recording every transaction or activity by default, rather than recording only specific activities. Though they

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 691

did not repeat the question on subsequent surveys, the American Management Association reports that 75 percent of firms surveyed in 2001 regularly record their employees' e-mail transmissions by means of a default setting.⁴⁸

The third form of monitoring is *surveillance by design*, where the entire purpose of the technology is to collect information and, generally, the user is aware of this purpose. Supermarkets often trade discounts on products in exchange for an individual's personal information on the application form for the encoded key chain device that allows the discount. The shopper is fully aware of the exchange when the information is collected, and the entire purpose of the key chain device is to provide information to the store. Often customer service representatives will be notified by an audible "beep" on the telephone that they are being monitored, and they understand that this monitoring will have implications for their performance evaluations. Another type of surveillance by design occurs when firms conduct either random or periodic keyword searches of e-mail or other transmissions. One-fourth of firms surveyed by the American Management Association reported that they perform keyword searches, generally seeking sexual or scatological language to protect themselves from later liability. 49

Surveillance by possession exists where the employer maintains employee information in a database or some other list. Bennett refers to this form of surveillance as gathering information that could be sold or acquired, such as employee personal information from application forms.

Much of the monitoring that occurs today in American firms is surveillance by design or by default. For instance, an e-mail program that systematically sorts and saves all e-mail that contains certain terms (such as those used in a job search or those that might be considered sexually harassing) would constitute surveillance by default. A monitoring program that tracks Internet accesses and blocks inappropriate Web sites would be surveillance by design.

How Does Monitoring Work?

Advances in information-gathering technology have allowed monitoring to an extent that was never before possible. Worldwide sales of monitoring technology are estimated at \$140 million annually.⁵⁰ One example of this new technology is Raytheon's Silentrunner, which allows firms to track everything that occurs on a network, including not only e-mail but also instant messaging ("IM," one of the ways employees thought they had foiled e-mail monitoring).⁵¹ Approximately 11 million people in the United States use IM at work.⁵² While some firms may encourage its use since it can cut down on travel, in-person meeting, and conference call expenses, IM also poses a significant risk since there is no built-in security measure in IM systems.

Other products called location-based monitoring services allow trucking firms to track their vehicles across the nation using global positioning⁵³ or allow managers to test a worker's honesty by using a truth-telling monitor during telephone calls.⁵⁴ The most prevalent Internet-monitoring product in the United States is Websense, with 8.25 million users worldwide. While Websense merely *blocks* certain Web sites, Websense Reporter, an add-on, records all Web accesses—not only

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

692 Part Three Regulation of the Employment Environment

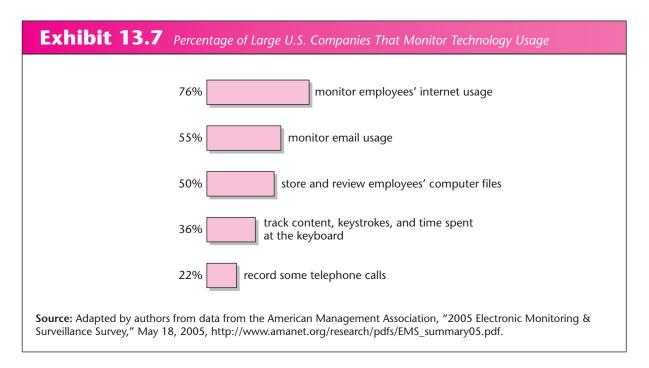
attempted accesses blocked by Websense but also all nonprohibited Web surfing (70 percent of Websense's customers install Reporter). MIMEsweeper is the most used e-mail monitoring system in the United States, with 6,000 corporate customers and over 6 million ultimate users worldwide. In a less-publicized form of monitoring, SWS Security offers a product that allows managers to track the messages a worker receives on a portable paging device so that one could track whether the employee is being distracted by outside messages. Another provider, www.tracingamerica.com, offers the following information at the listed prices:

- Social Security numbers, \$25.
- General all-around background search, \$39.
- Countywide search for misdemeanors and felonies, \$35.
- Whether subject has ever spent time in prison, \$25.
- Whether subject has ever served time in a federal prison, \$50.
- National search for outstanding warrants for subject, \$50.
- Countywide search for any civil filings filed by or against subject, \$50.
- Subject's driving record for at least three years back, \$30.

In the American Management Association's 2003 survey, 55 more than half of the respondents reported that they engaged in e-mail monitoring as a result of their concerns for legal liability (Exhibit 13.7, "Percentage of Large U.S. Companies That Monitor Employee E-mail"). Monitoring does not stop with e-mail and the Internet; the ACLU reports that employers monitor an estimated 400 million telephone calls annually.⁵⁶ Given the courts' focus in many cases on employer response to claims of sexual harassment or unethical behavior, among other complaints, firms believe that they need a way to uncover these inappropriate activities. More than 24 percent of firms have reported receiving a subpoena for employee e-mail, and 26 percent of the firms reported firing employees for inappropriate e-mail.⁵⁷ Without monitoring, how would companies know what occurs? Moreover, as courts maintain the standard in many cases of whether the employer "knew or should have known" of wrongdoing, the state-of-the-art definition of "should have known" becomes all the more vital. If most firms use monitoring technology to uncover such wrongdoing, the definition of "should have known" will begin to include an expectation of monitoring. Finally, some recent state cases have held that, where an employer provides notice to employees that e-mail is the property of the employer and that it will be monitored, communications by the employee over that system cannot be privileged or confidential, even if sent to a private attorney.⁵⁸

One of the most recent advances in monitoring technology involves the use of biometrics, including identification by fingerprint verification, iris and retinal scanning, hand geometry analysis, or facial feature scanning. Approximately 6 percent of employers in the United States use biometrics for a variety of purposes from allowing customers to purchase goods and services or for airline check-in. Those in favor of the technology contend that it will reduce the high economic and emotional costs of identity theft, among other benefits. Those opposed argue that it is subject

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 693



to inaccuracies, provides more information than employers have a right to know, and is one additional way in which "big brother" can keep an eye on employees at all times.

Employee theft has led both public and private employers to increase monitoring of their employees by using video surveillance. According to the National Retail Security Survey, 47 percent of an annual retail loss to employers of almost \$37.4 billion in 2005 was due to employee theft—more than \$17 billion. ⁵⁹ Another study conducted in 2005 by Hayes International reported that one out of every 26.5 employees was apprehended for theft from her or his employer in 2005. The survey also found that respondents caught 68,994 dishonest employees in 2005, which represented an increase of 11.49 percent over 2004's apprehensions, and that money gained by identifying dishonest employees totaled over \$49.9 million. ⁶⁰ Nevertheless, video surveillance may cost the employer through loss of morale. "Would you like to work in an environment where every time you blow your nose . . . it's on videotape?" asks Lewis Maltby, president of the National Workrights Institute in Princeton, New Jersey. ⁶¹

While no case of employer monitoring has yet reached the Supreme Court, these actions have received lower-court attention. As early as 1990, Epson America survived a lawsuit filed by a terminated employee who had complained about Epson's practice of reading all employee e-mail. ⁶² In that case, the court distinguished the practice of *intercepting* an e-mail transmission from storing and reading e-mail transmissions once they had been sent. However, relying on court precedent for protection is a double-edged sword. An employee-plaintiff in one federal action won a case against his employer where

© The McGraw-Hill Companies, 2009

694 Part Three Regulation of the Employment Environment

the employer had monitored the worker's telephone for a period of 24 hours in order to determine whether the worker was planning a robbery. The court held that the company had gone too far and had insufficient evidence to support its claims. ⁶³ In another action, Northern Telecom settled a claim brought by employees who were allegedly secretly monitored over a 13-year period. In this case, Telecom agreed to pay \$50,000 to individual plaintiffs and \$125,000 for attorney fees. ⁶⁴

Courts have supported reasonable monitoring of employees in open areas as a method of preventing and addressing employee theft. For example, in *Sacramento County Deputy Sheriff's Association v. County of Sacramento*, ⁶⁵ a public employer placed a silent video camera in the ceiling overlooking the release office countertop in response to theft of inmate money. The California Court of Appeals determined that the county had engaged in reasonable monitoring because employee privacy expectations were diminished in the jail setting. ⁶⁶

Though courts do not, per se, *require* notice in order to find that no reasonable expectation of privacy exists and to therefore allow monitoring by employers, notice of monitoring is favored by the courts. ⁶⁷ The court in *Thygeson v. U.S. Bancorp* ⁶⁸ held that an employer's specific computer usage policy precluded anemployee's reasonable expectation of privacy. As you see, though, in the *Smyth v. Pillsbury* case, discussed earlier and included at the end of the chapter, even where an employer says it will not monitor e-mail, courts may find no reasonable expectation of privacy.

While, as stated earlier, there is little legislation that actually relates to these areas specifically, there is some statutory protection from overt intrusions, though the statute does not apply in all circumstances. The federal wiretapping statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, ⁶⁹ protects private- and public-sector employees from employer monitoring of their telephone calls and other communications without a court order.

There are two exceptions to this general prohibition. First, interception is authorized where one of the parties to the communication has given prior consent. Second, the "business extension" provision creates an exception where the equipment used is what is used in the ordinary course of business. An employer must be able to state a legitimate business purpose and there must be minimal intrusions into employee privacy such that they would not be objectionable to a reasonable person.

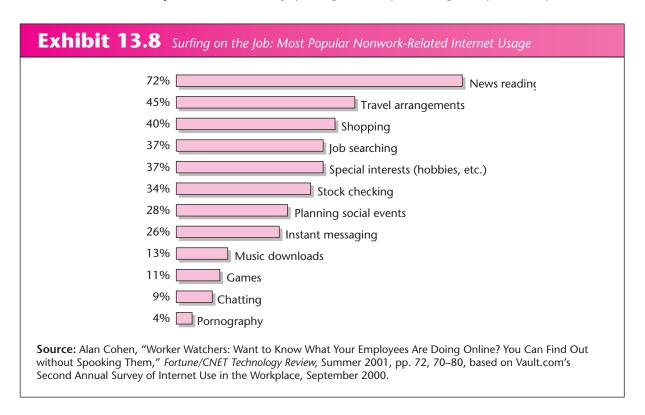
Business Justifications for Monitoring Employees' Technology Use

LO8

Web access at work may allow employees to be more creative and productive, but it also creates great risks. A survey by the Web site Vault.com found that 90 percent of employees surf nonwork-related Web sites while at work. (See Exhibit 13.8, "Surfing on the Job: Most Popular Nonwork-Related Internet Usage.") Wasted time, overclogged networks, and inappropriate material seeping into the work-place are all reasons why employers may seek to limit employees' Internet use at



Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 695



work. Of employers who monitor, almost half report that they restrict employees' Internet use.⁷¹



As mentioned above, monitoring is made simpler through an employee's use of a computer. Employers now customarily provide many employees with personal computers that are linked either to the Internet or, at least, to an internal network. Employers can monitor the computer user's activities. As to the type of information that can be gathered, the Privacy Demonstration Page of the Center for Democracy and Technology can feed back to viewers information that it finds out merely because one has accessed the page. For instance, the page tells one individual viewer the type of computer that the viewer is using, the browser the individual is using, the server from which the viewer is operating, and some of the pages the viewer has recently visited. While this information may not necessarily seem personal to some, consider the facts of scenario two. The employer in that case seems to be within its rights to monitor the use of its computers.

The need to monitor employees' usage becomes clear when one focuses on five areas of potential employer liability: defamation, copyright infringement, sexual harassment, discrimination, and obscenity.

As discussed previously in this chapter, the guidelines that apply to a general defamation claim also apply to issues surrounding the Internet. However, some contend that the opportunity for harm is far greater. This is because employees and employers can easily disseminate information to a wide range of media. Not

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

696 Part Three Regulation of the Employment Environment

only can employers be subject to defamation claims by their own employees, but the far greater threat is the liability a company faces when an employee, as a representative of the employer, defames another individual using the Internet (with access provided by the employer) as the medium.

Further, firms are concerned about inappropriate use of Web software such as occurs when an employee downloads program files without compensating the creator or when employees use copyrighted information from the Web without giving credit to the original author, thereby exposing the firm to potentially significant copyright infringement liability. Finally, when an employee downloads software programs from the Web, the computer systems within the firm have the potential to be compromised by viruses or even unauthorized access.

Sexual harassment and discrimination by employees via the Web are governed by the same general guidelines that were previously discussed in the chapters addressing sexual harassment and discrimination. However, many employees believe that once an e-mail message is deleted, it is permanently removed from the system. This is not the case. Because of this, e-mail sent on company time, with contents that constitute sexual harassment, that might create a hostile working environment, or that contain other forms of discrimination, may easily be discovered, both by the employer and by opposing parties to litigation against the employer. In fact, in 2003, 14 percent of companies in the American Management Association survey had been ordered by a court to produce employee e-mail. For example, female warehouse employees alleged that a hostile work environment was created in part by inappropriate e-mail, and they sought \$60 million in damages in federal court. The case settled out of court. 72 In another case, Zubulake v. UBS Warburg, the plaintiff was awarded a jury verdict in the amount of \$29.2 million. 73 The award ended up so large in part due to sanctions imposed by the trial judge as a result of the employer's failure to preserve e-mails for evidentiary purposes. E-mail is discussed in greater detail in the next section. Finally, obscenity becomes a critical issue, and the company may be placed at risk when employees download pornographic images while at the workplace.

Moreover, a firm might be concerned about the impression created when an employee visits various sites. Consider these scenarios: A customer service representative at an electronics store is surfing the Internet using one of the display computers. She accesses a Web site that shows graphic images of a crime scene. A customer in the store who notices the images is offended. Another customer service representative is behind the counter, using the store's computer to access a pornographic site, and starts to laugh. A customer asks him why he is laughing. He turns the computer screen around to show her the images that are causing him amusement.

Certainly, the employer would be justified in blocking employees' access to such Web sites. But what about sites of activist groups regarding sensitive issues such as abortion? Should an employer be allowed to block or restrict access to such sites? If such access may be restricted in order to promote efficiency and professionalism, then should employers be allowed to limit access to such innocuous sites as eBay or ESPN.com? The Vault.com survey mentioned above

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 697

revealed that over half of the employees who make personal use of the Internet at work restrict their surfing to less than half an hour a day. By limiting or restricting access to Web sites, the employer may be creating an environment in which employees do not feel trusted and perhaps feel inhibited about using the Internet for creative, work-related purposes because they fear being reprimanded for misusing access.⁷⁴

Employers seem to have business justification for other types of monitoring: "If [the employer] sees you doing something on the screen that they think you can do in a quicker way, they can tell you. They can even tell you ways to talk to people, or they can tell you ways to do things quicker to end your [customer service] call quicker," says Kathy Joynes, a travel agent for American Express who works out of her home, but whose supervisor can shadow her computer screen at any time.75

Because of the overall potential liability for their employees' actions, employers should develop a formal policy or program regulating employee usage of the Internet. In addition to having a formal policy, employers may choose to establish a process of monitoring their employee's Internet usage. This may involve tracking Web sites visited and the amount of time spent at each site using software programs designed for that specific purpose. However, employers need to consider the employees' rights to free speech and privacy when developing such policies and systems. (See Exhibits 13.9, "Monitoring Employees' Technology Usage," and 13.10, "Allowable Monitoring.")

The Case of Employee E-mail

An employer's need to monitor e-mail must be weighed against an employee's right to privacy and autonomy. The employer is interested in ensuring that the e-mail system is not being used in ways that offend others or harm morale, or for disruptive purposes—a significant concern when two-thirds of employees admit to using e-mail, specifically, for personal reasons having nothing to do with work. ⁷⁶ Likewise, an employer may choose to review e-mail in connection with a reasonable investigation of possible employee misconduct. Also, companies that maintain sensitive data may be concerned about disclosure of this information by disloyal or careless employees, apparently justifying this type of intrusion.

In a well-publicized case, perhaps because the behavior rose to the highest levels of the organization, the CEO of Boeing resigned amid allegations of unethical conduct. In March 2005, Boeing officials discovered that its CEO, Harry Stonecipher, had transmitted sexually explicit e-mails to another Boeing executive. The case is instructive in that, apparently, Stonecipher and the executive were involved in a consensual relationship and no complaints had been received from any individuals regarding the relationship. However, Stonecipher was originally hired after Boeing had experienced previous circumstances of alleged wrongdoings and after he, himself, had spearheaded the creation of an ethics policy in response. With notice of the e-mails and the possible later contention that a hostile environment existed for other workers, Boeing executives felt that they had no choice but to ask for his resignation.

698 Part Three Regulation of the Employment Environment

Exhibit 13.9 Monitoring Employees' Technology Usage

WHY DO FIRMS MONITOR TECHNOLOGY USAGE?

- Managing the workplace:
 - —Ensuring compliance with affirmative action.
 - —Administering workplace benefits.
 - —Placing workers in appropriate positions.
- Ensuring effective, productive performance:
 - Preventing loss of productivity to inappropriate technology use.
- Protecting information and guarding against theft.
- Protecting investment in equipment and bandwidth.
- Protecting against legal liability, including possible
 - —Perceptions of hostile environments.
 - —Violations of software licensing laws.

- —Violations regarding proprietary information or trade secrets.
- —Inappropriate gathering of competitive intelligence.
- -Financial fraud.
- —Theft.
- —Defamation/libel.
- —Discrimination.
- Maintaining corporate records (including e-mail, voice mail, and so on).
- Investigating some personal areas. (Consider Infoseek executive Patrick Naughton's pursuit of a tryst with an FBI agent posing as a 13-year-old girl in a chat room.)

ARGUMENTS IN FAVOR OF LIMITS MONITORING

- Monitoring may create a suspicious and hostile workplace.
- Monitoring constrains effective performance (employees claim that lack of privacy may prevent "flow")
- It may be important to conduct *some* personal business at the office, when necessary.
- Monitoring causes increased workplace stress and pressure, negatively impacting performance.
- Employees claim that monitoring is an inherent invasion of privacy.

- Monitoring does not always allow for workers to review and correct misinformation in the data collected.
- Monitoring constrains the right to autonomy and freedom of expression.
- Monitoring intrudes on one's right to privacy of thought. ("I use a company pen; does that mean the firm has a right to read my letter to my spouse?")

continued

While monitoring e-mail transmissions over telephone lines is forbidden by the ECPA, communications within a firm do not generally go over the phone lines and therefore may be legally available to employers. In addition, there are numerous exceptions to the ECPA's prohibitions as discussed earlier in this chapter, including situations where one party to the transmission consents, where the provider of the communication service can monitor communications, or where the monitoring is done in the ordinary course of business. In order to satisfy the ECPA consent exception, however, the employer's interception must not exceed the scope of the employee's consent. Employers must be aware, as well, that an

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 699

• Consider:

- —Surveys report alarming statistics about the use of the Internet while at work. Among them, up to 40 percent of workplace Internet use is not business-related, 64 percent of workers admit to using the Internet for personal purposes at some point during the workday, and the total amount of time spent on the Web can average more than 18 hours per week.a
- —It is estimated that 35 million workers, or approximately 25 percent of U.S. employees, spend an average of 3.5 hours a week on blogs.^b Men spend a bit more time on nonwork-related Web surfing than women, 2.3 hours per week versus 1.5 hours among women.c
- —13 percent of employees spend over two hours a day surfing nonbusiness sites.^d
- -24 percent of employees spend working hours at least one time each week watching or listening to streaming media.e

-70 percent of all traffic to Internet pornography Web sites is clocked during the traditional working hours of 9:00 a.m. and 5:00 p.m.^f

^aDeon Fair et al., "Internet Abuse Continues to Steal Workplace Productivity Despite the Use of Filters," April 27, 2005, http://www.minitrax.com/bw/whitepapers/ AIWhitePaper.pdf.

^bEzra Palmer, "The Work Force Is Surfing," *I-Media Con*nection, October 28, 2005, http://www.imediaconnection .com/content/7068.asp.

^cDeborah Rothberg, "As Crucial as Coffee: Web Surfing at Work," e-week, May 17, 2006, http://www.eweek.com/ article2/0,1895,1963997,00.asp. See also Websense, "Web @ Work Survey."

^dAlan Cohen, "Worker Watchers: Want to Know What Your Employees Are Doing Online? You Can Find Out without Spooking Them," Fortune/CNET Technology Review, Summer 2001, pp. 70, 76.

eRothberg, "As Crucial as Coffee."

fStaff Monitoring, "Staff Computer and Internet Abuse Statistics," 2007, http://staffmonitoring.com/P32/stats

Exhibit 13.10 Allowable Monitoring

Telephone calls Monitoring is permitted in connection with quality control. Notice to

the parties to the call is often required by state law, though federal law allows employers to monitor work calls without notice. If the employer realizes that the call is personal, monitoring must cease

immediately.

E-mail messages Under most circumstances, employers may monitor employee e-mails.

> Even in situations where the employer claims that it will not, its right to monitor has been held to persist. However, where the employee's reasonable expectation of privacy is increased (such as a passwordprotected account), this may impact the court's decision, though it is

not determinative.

Voice mail system

messages

Though not yet completely settled, it appears that voice mail system

messages are analyzed in the same manner as e-mail messages.

Internet use Where the employer has provided the equipment and/or the

access to the Internet, the employer may track, block, or review

Internet use.

700 Part Three Regulation of the Employment Environment

employee's knowledge that the employer is monitoring certain communications is insufficient to be considered implied consent. To avoid liability, employers must specifically inform employees of the extent and circumstances under which e-mail communications will be monitored.



Despite the failure of legislative attempts to require employers to notify employees that their e-mail is being monitored, such as the proposed Notice of Electronic Monitoring Act, employers should provide such notification, as described below.⁷⁷ In addition, some states have now imposed notice requirements before monitoring, including Delaware and Connecticut.

Developing Computer Use Policies



An employer can meet its business necessity to monitor e-mail, protect itself from liability, and, at the same time, respect the employees' legitimate expectation of privacy in the workplace in numerous ways. Moreover, research demonstrates that monitoring may be more acceptable to employees when they perceive that monitoring takes place within an environment of procedural fairness and one designed to ensure privacy. 78 Accordingly, employers should develop concise written policies and procedures regarding the use of company computers, specifically e-mail. The Society for Human Resource Management strongly encourages companies both to adopt policies that address employee privacy and to ensure that employees are notified of such policies. Any e-mail policy should be incorporated in the company policies and procedures manuals, employee handbooks, and instruction aids to ensure that the employee receives consistent information regarding the employer's rights to monitor employee e-mail. Additionally, a company could display a notice each time an employee logs on to a company computer indicating the computers are to be used only for business-related communication or explaining that the employee has no reasonable expectation of privacy in the electronic messages. Employers also can periodically send memos reminding employees of the policy. For a sample e-mail, voice mail, and computer systems policy, see Exhibit 13.11, "Sample E-mail, Voice Mail, and Computer Systems Policy."

Some experts advocate policies that restrict the use of e-mail to business purposes only and that explain that the employer may access the e-mail both in the ordinary course of business and when business reasons necessitate. If the employer faithfully adheres to this policy 100 percent of the time, this process is certainly defensible. However, such a standard is one that is difficult to honor in every case and the employer may be subject to claims of disparate treatment if applied inconsistently. Therefore, a more realistic approach—and one that is generally accepted in both the courts and common practice—suggests that employees limit their use of technology to reasonable personal access that does not unnecessarily interfere with their professional responsibilities or otherwise unduly impact the workplace financially or otherwise (referring to bandwidth, time spent online, impact on colleagues, and so on).

Kevin Conlon, district counsel for the Communication Workers of America, suggests these additional guidelines that may be considered in formulating an accountable process for employee monitoring:

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 701

Exhibit 13.11 Sample E-mail, Voice Mail, and Computer Systems Policy

Subject: E-mail, Voice Mail and Computer Systems Policy

Purpose: To prevent employees from using the Company computer and voice mail systems for

harassing, defamatory, or other inappropriate communications. To preserve the Company's right to monitor and retrieve employee communications. To prohibit excessive personal use

of the company's electronic systems.

Related Other related policies are: Harassment Prevention, Rules of Conduct, Confidentiality of

Policies: Company Information, Solicitations.

Background: Inappropriate employee use of Company computer, e-mail, and voice mail systems can sub-

ject the Company to significant legal exposure. Due to the effervescent nature of computer communications, employees will often say things in e-mail that they would never put in writing. Thus, it is important that all employers have a policy which strongly prohibits the inappropriate use of the Company's electronic systems, and puts employees on notice that

the employer reserves the right to monitor such use.

Policy: The Company provides its employees with access to Company computers, network, Internet access, internal and external electronic mail, and voice mail to facilitate the conduct of

Company business.

Company Property: All computers and data, information and software created, transmitted, downloaded, or stored on the Company's computer system are the property of Company. All electronic mail messages composed, sent, and received are and remain the property of Company. The voice mail system and all messages left on that system are Company property.

Business Use and Occasional Personal Use: The Company's computers, network, Internet access, electronic mail, and voice mail systems are provided to employees to assist employees in accomplishing their job responsibilities for the Company. Limited occasional personal use of such facilities is acceptable, provided such use is reasonable, appropriate, and complies with this policy. If you have any questions as to whether a particular use of such facilities is permissible, check with your supervisor before engaging in such use. The use of Company's computers, network, Internet access, electronic mail, and voice mail for personal use does not alter the facts that the foregoing remain Company property, and that employees have no reasonable expectation of privacy with respect to such use.

Privacy: Employees shall respect the privacy of others. Except as provided below, messages sent via electronic mail are to be read only by the addressed recipient or with the authorization of the addressed recipient. The data, information and software created, transmitted, downloaded, or stored on the Company's computer system may be accessed by authorized personnel only. Employees should understand that the confidentiality of electronic mail cannot be ensured. Employees must assume that any and all messages may be read by someone other than the intended recipient. Personal passwords are not an assurance of confidentiality. There is no reasonable expectation of privacy in any e-mail, voice mail, and/or other use of Company computers, network, and systems.

Prohibited Conduct:

- Employees may not use the Company's computers, network, Internet access, electronic mail, or voice mail to conduct illegal or malicious activities.
- Employees may not transmit or solicit any threatening, defamatory, obscene, harassing, offensive, or unprofessional material. Offensive content would include, but not

702 Part Three Regulation of the Employment Environment

Exhibit 13.11 Continued

be limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her race, religion, color, national origin, ancestry, disability, age, sex, marital status, sexual orientation, or any other class protected by any federal, state, or local law.

- Employees may not create, transmit, or distribute unwanted, mass, excessive or anonymous e-mails, electronic vandalism, junk e-mail, or "spam."
- Employees may not access any Web site that is sexually or racially offensive or discriminatory.
- Employees may not display, download, or distribute any sexually explicit material.
- Employees may not violate the privacy of individuals by any means, such as by reading private e-mails or private communications, accessing private documents, or utilizing the passwords of others, unless officially authorized to do so.
- Employees may not represent themselves as being someone else, or send anonymous communications.
- Employees may not use the e-mail, voice mail, or computer systems to solicit for religious causes, outside business ventures, or personal causes.
- Employees may not transmit any of Company's confidential or proprietary information including (without limitation) customer data, trade secrets, or other material covered by Company's policy re: Confidentiality of Company information.
- Employees may not install, run, or download any software (including entertainment software or games) not authorized by the Company.
- Employees may not disrupt or hinder the use of the Company computers or network, or infiltrate another computer or computing system.
- Employees may not damage software or propagate computer worms or viruses.

Only authorized employees may communicate on the Internet on behalf of the Company. *Monitoring:* Company maintains the right to monitor and record employee activity on its computers, network, voice mail and e-mail systems. Company's monitoring includes (without limitation) reading e-mail messages sent to received, files stored or transmitted, and recording Web sites accessed.

Archiving: It is Company's practice to archive (i.e., make backup copies) all electronic documents, files, and e-mail messages incident to the Company's normal back-up procedures. Employees should therefore understand that even when a document, file, or message is deleted, it may still be possible to access that message. Management and law enforcement agencies have the right to access these archives.

Copyright Laws: Any software or other material downloaded into the Company's computers may be used only in ways consistent with the licenses and copyrights of the vendors, authors, and owners of the material. No employee shall make illegal or unauthorized copies of any software or data.

Violations of this Policy: Any violation of this policy may result in disciplinary action up to and including immediate termination. Any employee learning of any violation of this policy should notify his or her [e.g., immediate supervisor] immediately.

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 703

Dates: Be sure to date policies when they become effective. Hang on to old policies and be sure to change the date on revised versions.

Source: Lee T. Paterson, ed., Sample Personnel Policies (El Segundo, CA: Professionals in Human Resources Association (PIHRA), 2002).

- 1. There should be no monitoring in highly private areas such as restrooms.
- 2. Monitoring should be limited to the workplace.
- 3. Employees should have full access to any information gathered through monitoring.
- 4. Continuous monitoring should be banned.
- 5. All forms of secret monitoring should be banned. Advance notice should be given.
- 6. Only information relevant to the job should be collected.
- 7. Monitoring should result in the attainment of some business interest.

Philosopher William Parent conceives the right to privacy more appropriately as a right to liberty and therefore seeks to determine the potential affront to liberty from the employer's actions. He suggests the following six questions to determine whether those actions are justifiable or have the potential for an invasion of privacy or liberty:

- 1. For what purpose is the undocumented personal knowledge sought?
- 2. Is this purpose a legitimate and important one?
- 3. Is the knowledge sought through invasion of privacy relevant to its justifying purpose?
- 4. Is invasion of privacy the only or the least offensive means of obtaining the knowledge?
- 5. What restrictions or procedural restraints have been placed on the privacyinvading techniques?
- 6. How will the personal knowledge be protected once it has been acquired?⁷⁹

Both of these sets of guidelines also may respect the personal autonomy of the individual worker by providing for personal space within the working environment, by providing notice of where that "personal" space ends, and by allowing access to the information gathered, all designed toward achievement of a personal and professional development objective.

As is apparent from the above discussion, it is possible to implement a monitoring program that is true to the values of the firm and accountable to those it impacts—the workers. Appropriate attention to the nature and extent of the monitoring, the notice given to those monitored, and the ethical management of the information obtained will ensure a balance of employer and employee interests.

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

704 Part Three Regulation of the Employment Environment

Waivers of Privacy Rights

search

A physical invasion of a person's space, belongings, or body.

waiver

The intentional relinquishment of a known right.

On occasion, an employer may request that an employee waive her or his privacy rights as a condition of employment. This condition could be a **search**. A **waiver** would exempt the employer from liability for claims the employee may have as a result of privacy issues. While a valid waiver must be voluntarily given, requiring a waiver as an employment condition is a questionable approach. Employers maintain a superior bargaining position from which to negotiate such an arrangement, so voluntariness is questionable.

Waivers exist at all stages of employment, from pre-employment medical screenings to a waiver of age discrimination claims when being bought out of one's job at an old age. Courts are not consistent in their acceptance of these waivers, but one common link among those that are approved is that there exists some form of consideration in which the employee receives something in return for giving up rights.

It has thus been held that the waiver at least be accompanied by an offer of employment. No waiver that is given by an applicant prior to a job offer would be considered valid and enforceable. Other requirements articulated by the courts include that the waiver be knowingly and intelligently given and that it be clear and unmistakable, in writing, and voluntary.

Privacy Rights since September 11, 2001

The United States has implemented widespread modifications to its patchwork structure of privacy protections since the terrorist attacks of September 11, 2001. In particular, proposals for the expansion of surveillance and information-gathering authority were submitted and many, to the chagrin of some civil rights attorneys and advocates, were enacted.

The most public and publicized of these modifications was the adoption and implementation of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Public Law 107-56. The USA PATRIOT Act expanded states' rights with regard to Internet surveillance technology, including workplace surveillance and amending the Electronic Communications Privacy Act in this regard. The act also grants access to sensitive data with only a court order rather than a judicial warrant, among other changes, and imposes or enhances civil and criminal penalties for knowingly or intentionally aiding terrorists. In addition, the new disclosure regime increased the sharing of personal information between government agencies in order to ensure the greatest level of protection.

Title II of the act provides for the following enhanced surveillance procedures, among others, that have a significant impact on individual privacy and may impact an employer's effort to maintain employee privacy:

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 705

- · Expanded authority to intercept wire, oral, and electronic communications relating to terrorism and to computer fraud and abuse offenses.
- Provided roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978 (FISA) to track individuals. (FISA investigations are not subject to Fourth Amendment standards but are instead governed by the requirement that the search serve "a significant purpose)."
- Allowed nationwide seizure of voice mail messages pursuant to warrants (i.e., without the previously required wiretap order).
- Broadened the types of records that law enforcement may obtain, pursuant to a subpoena, from electronic communications service providers.
- Permitted emergency disclosure of customer electronic communications by providers to protect life and limb.
- Offered nationwide service of search warrants for electronic evidence.

Pursuant to these provisions, the government is now allowed to monitor anyone on the Internet simply by contending that the information is "relevant" to an ongoing criminal investigation. In addition, the act provides anti-money laundering provisions designed to combat money laundering activity or the funding of terrorist or criminal activity through corporate activity or otherwise. All financial institutions must now report suspicious activities in financial transactions and keep records of foreign national employees, while also complying with antidiscrimination laws discussed throughout this text. It is a challenging balance, claim employers.

The USA PATRIOT Act was not the only legislative response. Both federal and state agencies have passed a number of new pieces of legislation responding to terrorism. Not everyone is comfortable with these protections. Out of concern for the USA PATRIOT Act's permitted investigatory provisions, some librarians now warn computer users in their libraries that their computer use could be monitored by law enforcement agencies (especially since reforms to the act were defeated in 2006 and certain provisions will stay in place for another 4 years). The Washington Post reports that some are even ensuring privacy by destroying records of sites visited, books checked out, and logs of computer use. 80 The American Civil Liberties Union reports that a number of communities have passed Anti-USA PATRIOT Act resolutions.81

Employers have three choices in terms of their response to a governmental request for information. They may

- 1. Voluntarily cooperate with law enforcement by providing, upon request (as part of an ongoing investigation), confidential employee information.
- 2. Choose not to cooperate and ask instead for permission to seek employee authorization to release the requested information.
- 3. Request to receive a subpoena, search warrant, or FISA order from the federal agency before disclosing an employee's confidential information.⁸²

13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

Management Tips

- Public-sector employees are subject to protection by the Constitution and the Privacy Act; private-sector employees are instead protected by common law and state-by-state restrictions on invasions of privacy.
- As an employer, you may search your employees' property where the employee does not have any expectation of privacy; the difficulty comes in determining where that expectation exists.
- Since many privacy protections exist on a state-by-state level, be sure to investigate the specific protections for which you are responsible in the states in which you do business.
- While it may appear reasonable for you to want to regulate certain off-work activities of your employees, be wary of overrestricting since courts do not look on these regulations positively.
- Where you do opt to regulate the off-work activities of your employees, you
 may wish to consider focusing the policy on the possible negative impact of offduty conduct to the employer's business interests and to the publics perception
 of the employer, rather than on the specific off-duty conduct, in particular.
- You are less likely to find problems with a waiver of privacy rights where the waiver is accompanied by an offer of employment.
- When you do collect personal information about your employees, be sure to regulate access to this information since unwarranted disclosure might constitute an invasion of privacy even where the original collection of information is allowed.
- In designing a monitoring process, avoid content-based and real-time monitoring as both give rise to subjective action rather than standardized procedures and may violate the Federal Wiretap Act.
- Monitoring policies should be clearly stated and should explain that use of technology is subject to review, notwithstanding password protection. They should explain that passwords are provided for the user's protection from external intrusion, as opposed to the creation of an expectation that e-mail is actually private with regard to the employer.

Chapter Summary

Basic rules that, if followed, may preclude employer liability for invasions of privacy are

• First, conduct an information audit for the purpose of determining those areas of the company's practices and procedures that have the potential for invasion, including what type of information is collected, how that information is maintained, the means by which the information is verified, who has access to the information, and to whom the information is disclosed. The audit should cover all facets of the organization's activities, from recruitment and hiring to termination. In addition, it may be helpful to ascertain what type of information is maintained by different sectors of the organization.

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 707

- Second, in connection with sensitive areas where the company maintains no formal policy, develop a policy to ensure appropriate treatment of data. It is recommended that a policy and procedure be maintained in connection with the acquisition of information, the maintenance of that information, the appropriate contents of personnel files, the use of the information contained therein, and the conduct of workplace investigations. For instance, in connection with the maintenance of personnel files and the accumulation of personal information about company employees, the employer should request only information justified by the needs of the firm and relevant to employment-related decisions.
- Third, the information collected should be kept in one of several files maintained on each employee: (1) a personnel file, which contains the application, paperwork relating to hiring, payroll, and other nonsensitive data; (2) a medical file, which contains physicians' reports and insurance records; (3) evaluation files, which contain any evidence of job performance including, but not limited to, performance appraisals; and (4) a confidential file, which contains data relating to extremely sensitive matters that should not be disclosed except with express and specific authority, such as criminal records or information collected in connection with workplace investigations.
- Fourth, information should be gathered from reliable sources, rather than sources of questionable repute such as hearsay, lie detector tests, and subjective indicators. Irrelevant or outdated material should periodically be expunged from these records as well.
- Fifth, publicize privacy policies and procedures, and educate employees regarding their rights as well as their responsibilities.

Chapter-End Questions

- 1. Can a government employee state a claim for a violation of the constitutional right to privacy when she was required, as a job applicant, to sign an affidavit stating that she had not used tobacco products for one year prior to the application date?
- 2. A homosexual employee files a claim for invasion of privacy against his employer who shared with co-workers the fact that the employee's male partner was listed on his insurance policy and pension plan as his beneficiary. Does he have a claim?
- 3. In March and April 1998, John Doe, an employee of the U.S. Postal Service, missed several weeks of work because of an AIDS-related illness. Doe's supervisor told him that he had to submit an administrative form and a medical certificate explaining why he has sick or he would face disciplinary action for his unexplained absence. He was informed that he may qualify for coverage under FMLA and his supervisor provided him with the appropriate forms to fill out and return. Doe decided to pursue an FMLA request and his physician completed the forms, indicating that Doe had "AIDS related complex" and "chronic HIV infection." Doe submitted the request forms to his employer and, upon his return to work, discovered that his HIV status had become

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

708 Part Three Regulation of the Employment Environment

common knowledge among co-workers. Several co-workers made comments to him about his condition and many identified his supervisor as the source of the information. Doe filed a suit against the U.S. Postal Service for violation of the Privacy Act, alleging that Postal Service employees disclosed medical information contained in his FMLA forms. Can Doe prove his case? [*John Doe v. U.S. Postal Service*, No. 01-5395 (DC. Cir. Feb. 7, 2003).]

- 4. Marriott Resorts had a formal company party for more than 200 employees. At one point during the party, they aired a videotape that compiled employees' and their spouses' comments about a household chore that they hated. However, as a spoof, the video was edited to make it seem as if they were describing what it was like to have sex with their partner. For instance, though the plaintiff's husband (an employee) was actually responding to the question about housework, the plaintiff's husband was quoted on the video as seemingly responding to a provocative question by saying, "the smell. The smell, the smell. And then you go with the goggles. You have to put on the goggles. And then you get the smell through the nose. And as you get into it things start flying all over the place. And the smell. And you get covered in these things." The plaintiff herself was never mentioned by name, nor did she appear on the video. The plaintiff was terribly upset by the video and sued Marriott for intrusion into seclusion and portrayal of facts in a false light. Is Marriott liable? [Stein v. Marriott Ownership Resorts, Inc., 944 P.2d 374 (UT. 1997).]⁸³
- 5. David Patton, a merchandising manager for J.C. Penney Company, was having an intimate relationship with a co-worker. The store manager, McKay, told Patton that if he did not cease this relationship with a co-employee, his job would be in danger. Patton refused to break off his relationship, claiming that he did not socialize with this woman at work and the relationship did not have an adverse effect on his performance, as evidenced by his awards "Merchant of the Month" and "Merchant of the Year," both earned while dating this co-employee. The company had no specific written policies about dating co-workers; however, McKay maintained that dating co-workers was not allowed and continued to threaten Patton's job. Finally, Patton asked for a transfer to another department because McKay threatened to discharge him for unsatisfactory performance. McKay denied the transfer and discharged him for unsatisfactory performance. Patton filed charges against the company and McKay that his discharge was outrageous conduct that violated his privacy. Did it? [Patton v. J.C. Penney Co., 719 P.2d 854 (Or. 1986).]
- 6. The employer of an over-the-road trucker customarily rented and then paid for the trucker's hotel room during business travel. When a permit book went missing, the employer searched the trucker's hotel room without authorization from the employee. Does the trucker have a reasonable expectation of privacy in that hotel room? [Sowards v. Norbar Inc., 605 N.E.2d 468 (Ohio Ct. App. 1992).]
- 7. In 1992, a K-mart distribution facility in Illinois suspected that employees were stealing and vandalizing merchandise and using and selling drugs in the workplace. In order to identify the responsible individuals, K-mart hired two undercover private investigators to work and mingle among employees, while periodically submitting reports to the general manager of the facility. After months of interacting with and disclosing personal information to the undercover agents, employees discovered that the two "co-workers" were, in fact, undercover agents and sued K-mart for invasion

III. Regulation of the **Employment Environment** 13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 709

- of privacy, citing "intrusion into seclusion." Do they have a valid claim? Why or why not? [Johnson et al. v. K-mart Corp., 311 Ill. App. 3d 573, 723 N.E.2d 1192 (2000).]
- 8. Kristine Naragon was a graduate assistant for Louisiana State University at Baton Rouge's School of Music. She mainly had teaching responsibilities and was often praised for her work and dedication. When the university discovered that she was a lesbian and was involved with a student, the school of music renewed her yearly contract but revoked teaching responsibilities and replaced them with purely researchoriented responsibilities. Naragon claims that her privacy rights and her freedom of association rights were violated because she is a lesbian, and she wants her teaching privileges restored. The university maintains that there was no obligation to renew Naragon's contract as it stood, and the university felt that her conduct with a student, lesbian or not, warranted less contact with the students. Naragon defends her conduct by showing that this student was not and never had been a student in her class. Was there an invasion of privacy by the employer? Why or why not? [Naragon v. Wharton, 572 F. Supp. 1117 (1983).]
- 9. In 2003, Weyco, Inc., gave employees a 15-month advance warning of a new policy that went into effect on January 1, 2005. The policy prohibited employees from smoking, on or off the job. The company provided smoking cessation programs to employees to help them quit before the policy went into effect, but employees still complained that this policy violated their privacy rights. Can Weyco legally forbid their employees from smoking when they are not at work?
- 10. As fire marshall for a town in Texas, Joe had his own office in which he had a computer but no Internet. In Joe's absence, Smith, the city's network administrator, entered Joe's office to install the city network on his computer. Smith discovered that Joe had installed a password, without which Smith could not access the computer's hard drive to complete his task. Smith notified Joe's supervisor, who called Joe at home to get his password. After resuming work on the computer, Smith noticed the presence of newsgroups. Smith knew that no one was permitted to have newsgroups on his or her computer, but the policy had not been communicated to the fire station employees, including Joe. Looking at the newsgroups, Smith noticed three titles suggesting the presence of pornography. He clicked on one newsgroup title, alt.erotica.xxx.preteen, and saw that about 25 of the approximately 60 files had been read. The city's public safety director, Keller, instructed Smith and Fire Chief Ure to get what was needed from Joe's office to view the contents of his computer, as well as any zip disks or drives. The material taken from Joe's office revealed explicit child pornography. Joe was convicted for possession of child pornography. Did the collection of evidence from Joe's office violate his Fourth Amendment rights? Explain. [United States v. Slanina, 283 F.3d 670 (5th Cir. 2002).]
- 11. In June of 1995, a hidden camera and VCR were installed at Salem State College in their off-campus Small Business Development Center. The camera was installed to investigate possible illegal entries into the center after regular business hours. The camera recorded 24 hours a day and was angled to view the entire length of the office, including private areas such as cubicles. During the summer of 1995, Gail Nelson, a secretary at the center, often brought a change of clothes to work and changed in a cubicle, either early in the morning before anyone else was in the office or after work when the office was empty. These activities were recorded on the hidden

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

710 Part Three *Regulation of the Employment Environment*

camera. When Nelson later learned about the covert surveillance from a co-worker, she filed suit against the college and officials, arguing that they had violated her Fourth Amendment right to privacy. Was this an invasion of privacy? [Gail Nelson v. Salem State College & others, SJC-09519 (MA., Dec. 8, 2005–Apr. 13, 2006).] What if the video surveillance had taken place in a back room such as an employee locker area? [Thompson v. Johnson County Community College, 930 F. Supp. 501 (D. Kan. 1996), aff'd, 108 F.3d 1388 (10th Cir. 1997).]

12. A college provided its security officers with a locker area in which to store personal items. The security officers occasionally used the area as a dressing room. After incidents of theft from the lockers and reports that the employees were bringing weapons to campus, the college installed a video surveillance camera in the locker area. Did the employees have a reasonable expectation of privacy that was violated by the video surveillance? Explain. [*Thompson v. Johnson County Community College*, 930 F. Supp. 501 (D. Kan. 1996), *aff'd*, 108 F.3d 1388 (10th Cir. 1997).]

End Notes

- 1. E. J. Bloustein, "Privacy as an Aspect of Human Dignity" in F. D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (New York: cambridge University Press 1984), p. 188.
- 2. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 193 (1890).
- 3. an-Noor 24, pp. 27–28 (Yusufali); al-Hujraat 49, pp. 11–12 (Yusufali).
- 4. Vol. 1, Book 10, no. 509 (Sahih Bukhari); Book 31, no. 4003 (Sunan Abu Dawud).
- 5. R. L. Wakefield, "Computer Monitoring and Surveillance: Balancing Privacy with Security," *CPA Journal* 74, no. 7 (2004), pp. 52–55.
- 6. Delia Fahmy, "More U.S. Employers Testing Workers for Drug Use," *International Herald Tribune*, May 10, 2007, http://www.iht.com/articles/2007/05/10/business/drugtests.php (last visited August 5, 2007).
- Deloitte & Touche, Poneman Institute, LLC, "Enterprise @ Risk: 2007 Privacy & Data Protection Survey," December 12, 2007, http://www.deloitte.com/dtt/article/0%2C1002%2Ccid%25253D182733%2C00.html.
- 8. 381 U.S. 479 (2965).
- 9. Steve Ulfelder, "CPOs on the Rise?" *Computerworld*, March 15, 2004, http://www.computerworld.com/securitytopics/security/story/0.10801.91166.00.html, quoting Alan F. Westin, president of the nonprofit Privacy & American Business organization.
- 10. 795 F.2d 1136, 1141 (3d Cir. 1986).
- 11. 489 U.S. 602, 109 S. Ct. 1402 (1989), aff'd, 934 F.2d 1096 (9th Cir. 1991).
- 12. U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002); Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001).
- 13. 474 F.3d 1184 (9th Cir. 2007), http://bulk.resource.org/courts.gov/c/F3/474/474. F3d.1184.05-30177.html.
- 14. As an interesting side note, though U.S. law considers child pornography illegal, most states have no legal obligation to report it. Only Arkansas, Missouri, Oklahoma, South Carolina, and South Dakota have laws that require workers in the information technology arena to report child pornography when it is found on workers' computers. Tam Harbert, "Dark Secrets and Ugly Truths: When Ethics and IT Collide," *Computerworld*, September 12, 2007.

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 711

- 15. Ziegler, 474 F.3d at 1199.
- 16. Fraser v. National Mutual Insurance, 352 F.3d 107 (3d Cir. 2003). See also United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); and Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).
- 17. 50 S.E. 68 (Ga. 1905).
- 18. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998).
- 19. 526 F. Supp. 523 (D.D.C. 1981).
- 20. 66 Md. App. 133, 502 A.2d 1101, cert. denied, 306 Md. 289, 508 A.2d 488, cert. denied, 479 U.S. 984 (1986).
- 21. 561 F. Supp. 872 (S.D. Ga. 1983).
- 22. Certain states, however, provide no statutory protection, including Alabama, Connecticut, Mississippi, Nebraska, New Jersey, New York, Vermont, and Washington.
- 23. As of publication, these included Arizona, Connecticut, the District of Columbia, Illinois, Indiana, Kentucky, Louisiana, Maine, Mississippi, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Virginia, West Virginia, and Wyoming. See also John Pearce and Dennis Kuhn, "The Legal Limits of Employees' Off-Duty Privacy Rights," Organizational Dynamics 32, no. 4 (2003), pp. 372–83.
- 24. R. Parekh, "States Hit Public Employees with Smoking Surcharge," Business Insurance, May 23, 2005.
- 25. M. McDonough, "Whirlpool Plant Suspends 39 Employees Caught Smoking," ABA Journal, April 23, 2008, http://www.abajournal.com/news/whirlpool_plant_ suspends 39 employees caught smoking/; J. Wojcik, "Smoke Gets in Your Lies," Workforce Week, April 22, 2008, http://www.workforce.com/section/00/article/25/49/15 .html.
- 26. D. Costello, "Workers Are Told to Shape up or Pay up," Los Angeles Times, July 29, 2007, http://www.latimes.com/news/nationworld/nation/la-fi-obese29jul29,1,7252935 .story?coll=la-headlines-nation&ctrack=3&cset=true.
- 27. American Management Association, "AMA's 2003 Survey on Workplace Dating," (2003), http://www.amanet.org/research/pdfs/dating_workplace03.pdf.
- 28. Ibid.
- 29. 237 F.3d 166 (2d Cir. 2001).
- 30. J. T. A. Gabel, and N. R. Mansfield, "The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace," American Business Law Journal 40 (2003), pp. 301–51.
- 31. Mike Brunker, "Cyberporn Nurse: I Feel Like Larry Flynt," MSNBC, July 16, 1999.
- 32. CCH Human Resources Workforce Online, Do Workplace Smoking Laws Regulate Your Business? http://www.workforceonline.com/section/03/0005085.htm.
- 33. American Civil Liberties Union, Press Release, "New Study on Workplace Surveillance Highlights Lack of Protections, ACLU Says," May 23, 1997.
- 34. American Management Association and the ePolicy Institute, "2005 Electronic Monitoring & Surveillance Survey," May 18, 2005, http://www.amanet.org/ research/pdfs/EMS_summary05.pdf; James Petrie, "Work-Related Blogging by Employees," Lexology, September 5, 2007, http://www.lexology.com/library/detail aspx?g=b505c2c3-4ea5-4696-bc89-fb44e127e143.

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

712 Part Three *Regulation of the Employment Environment*

- 35. Proofpoint, "Outbound Email and Content Security in Today's Enterprise," 2007, http://www.proofpoint.com/outbound (last visited July 27, 2007).
- 36. Philip Gordon, and Katherine C. Franklin, "Blogging and the Workplace," *Law.com*, August 8, 2006.
- 37. Ibid.
- 38. *The Urban Dictionary*, http://www.urbandictionary.com/define.php?term=dooced.
- 39. Graeme Smith, "Is Big McBrother Invading Workplace Privacy?" *The Globe and Mail*, January 13, 2004, p. A8.
- 40. Philip Gordon, "It's 11 a.m. Do You Know Where Your Employees Are? Effective Use of Location-Based Technologies in the Workplace," 2005, http://library.findlaw.com/2005/Mar/10/163970.html.
- 41. Ibid.
- 42. Ashley Benigno, "Total Surveillance Is Threatening Your Health," *Asian Labour Update* (Hong Kong: Asia Monitor Resource Center, http://www.amrc.org.hk/Arch/3405.htm, last visited February 5, 2002).
- 43. Richard Rosenberg, "The Technological Assault on Ethics in the Modern Workplace," in *The Ethics of Human Resources and Industrial Relations*, ed. John W. Budd and James G. Scoville (Champaign, IL: Labor and Employment Relations Assn., 2005).
- 44. U. Klotz, "The Challenges of the New Economy," October 1999, cited in *World Employment Report 2001: Life at Work in the Information Economy*, p. 145 (Geneva: International Labour Office, 2001).
- 45. Tam Harbert, "Dark Secrets and Ugly Truths: When Ethics and IT Collide," *Computerworld*, September 12, 2007.
- 46. Colin Bennett, "Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web," *Ethics and Information Technology* 3 (2001), pp. 197–210.
- 47. Ethisphere, "Mesa Airlines CFO Scrambled to Erase Porn," September 27, 2007, http://ethisphereblog.com/mesa-airlines-cfo-scrambled-to-erase-porn-not-valuable-evidence/#more-1273 (last visited September 28, 2007).
- 48. Dana Hawkins, "Lawsuits Spur Rise in Employee Monitoring," U.S. News & World Report, August 13, 2001.
- 49. Ibid.
- 50. Andrew Schulman, "One-Third of U.S. Online Workforce under Internet/Email Surveillance," *Workforce Surveillance Project* (Privacy Foundation), July 9, 2001, http://www.privacyfoundation.org/workplace/business/biz_show.asp?id=70&ac.
- 51. Jeffrey Benner, "Privacy at Work? Be Serious," *Wired Magazine*, March 2001, http://www.wired.com/news/business/0,1367,42029,00.html (accessed February 26, 2002).
- 52. Pew Internet and American Life Project, *How Americans Use Instant Messaging*, September 1, 2004, p. 2, http://www.pewinternet.org.
- 53. http://www.omnitracs.com.
- 54. http://www.spyzone.com.
- 55. American Management Association, "2003 E-Mail Rules, Policies and Practices Survey," May 28, 2003, http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf.
- 56. American Civil Liberties Union, "Privacy in America: Electronic Monitoring," December 31, 1997, http://www.aclu.org/privacy/workplace/15104res19971231.html (last visited July 26, 2007).

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 713

- 57. American Management Association and the ePolicy Institute, "2005 Electronic Monitoring & Surveillance Survey."
- 58. Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436 (2007); but see, contra, Curto v. Medical World Communications, Inc., 2006 WL 1318387 (E.D.N.Y. 2006).
- 59. R. Hollinger and L. Langton, "2005 National Retail Security Survey," 2005, http:// www.crim.ufl.edu/research/srp/finalreport_2005.pdf.
- 60. Hayes International, 18th Annual Retail Theft Survey, http://www.hayesinternational .com/ts_emply_thft.html (last visited July 25, 2007).
- 61. Karen Robinson-Jacobs, "Retailers Taking Aim at Employee Pilferage," Los Angeles *Times*, February 16, 2002, p. C1.
- 62. Shoars v. Epson America, Inc., No. SCW 112749 (Cal. Super. Ct., L.A. Cty., 1990), appeal denied, 994 Cal. LEXIS 3670 (Cal. 1994); James McNair, "When You Use E-mail at Work, Your Boss May Be Looking In," Telecom Digest, http://icg .stwing.upenn.edu/cis500/reading.062.htm, reprinted from the Miami Herald, February 9, 1994.
- 63. Winn Schwartau, "Who Controls Network Usage Anyway?" Network World, May 22, 1995, p. 71.
- 64. Bureau of National Affairs, "Northern Telecom Settles with CWA on Monitoring," Individual Employment Rights, March 10, 1992, p. 1.
- 65. 59 Cal. Rptr. 2d 834 (Cal. Ct. App. 1996).
- 66. See Ted Clark, "Legal Corner: Monitoring Employee Activities: Privacy Tensions in the Public Workplace," NPLERA Newsletter, June 1999, http://www.seyfarth.com/ practice/labor/articles/II_1393.html.
- 67. Lisa Reed and Barry Freidman, "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use," Employee Responsibilities and Rights Journal 19, no. 2 (June 2007), pp. 75-83.
- 68. 2004 U.S. Dist. LEXIS 18863 (D. Or. 2004).
- 69. 18 U.S.C. §§ 2510–2520.
- 70. Alan Cohen, "Worker Watchers: Want to Know What Your Employees Are Doing Online? You Can Find Out without Spooking Them," Fortune/CNET Technology Review, Summer 2001, p. 70.
- 71. Ibid.
- 72. Harley v. McCoach, 928 F. Supp. 533 (E.D. Pa. 1996), cited in "Cyberliability: An Enterprise White Paper," Elron Software, http://www.internetmanager.com.
- 73. 217 F.R.D. 309, 312 (S.D.N.Y. 2003); see also "Jury Awards \$29.2 Million in Damages to Discharged Equities Saleswoman," Daily Labor Report (BNA), April 13, 2005, p. 449.
- 74. Cohen, "Worker Watchers," p. 76.
- 75. Dan Charles, "High-Tech Equipment in the Workplace," All Things Considered, National Public Radio, April 1, 1996.
- 76. Websense, "Web @ Work Survey," 2006, http://www.websense.com/global/en/Press-Room/PressReleases/PressReleaseDetail/?Release=0605161213.
- 77. Christopher A. Weals, "Workplace Privacy," Legal Times, March 6, 2002.
- 78. Reed and Freidman, "Workplace Privacy," pp. 75–83.
- 79. Miriam Schulman, "Little Brother Is Watching You," Issues in Ethics 9, no. 2 (Spring 1998).

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

714 Part Three *Regulation of the Employment Environment*

- 80. Rene Sanchez, "Librarians Make Some Noise over Patriot Act," *The Washington Post*, April 10, 2003, p. A20.
- 81. http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11256&c=206.
- 82. Vance Knapp, "The Impact of the Patriot Act on Employers," 2003, http://www.rothgerber.com/newslettersarticles/le0024.asp.
- 83. http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=ut&vol=appopin&invol=stien.

Cases

Case 1 O'Connor v. Ortega 714

Case 2Michael A. Smyth v. The Pillsbury Company 717Case 3Yoder v. Ingersoll-Rand Company a.k.a. ARO 718

Case 4 French v. United Parcel Service, Inc. 720



O'Connor v. Ortega 480 U.S. 709 (1987)

The respondent, Dr. Ortega, was a physician and psychiatrist and an employee of a state hospital who had primary responsibility for training physicians in the psychiatric residency program. Hospital officials became concerned about possible improprieties in his management of the program. In particular, the officials thought that Dr. Ortega may have misled the hospital into believing that the computer had been donated when, in fact, the computer had been financed by the possibly coerced contributions of residents. Hospital officials were also concerned about charges that Dr. Ortega had sexually harassed two female hospital employees, and that he had taken inappropriate disciplinary action against a resident.

While he was on administrative leave pending investigation of the charges, hospital officials, allegedly in order to inventory and secure state property, searched Dr. Ortega's office and took personal items from his desk and file cabinets that later were used in administrative proceedings resulting in his discharge. The employee filed an action against the hospital officials, alleging that the search of his office violated the Fourth Amendment. The trial court found that the search was proper in order to secure state property. The court of appeals held that the employee had a *reasonable expectation of privacy* in his office, and thus the search violated the Fourth Amendment. The Supreme Court explains that a search must be reasonable both from its inception as well as in its scope, and remands the case to the district court for review of the reasonableness of both of those questions.

O'Connor, J.

Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas,

are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.

Not everything that passes through the confines of the business address can be considered part of the workplace context, however. . . . The appropriate standard for a workplace search does not necessarily apply 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 715

to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

Given the societal expectations of privacy in one's place of work, we reject the contention made by the Solicitor General and petitioners that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. 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. The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public-may have frequent access to an individual's office....

The undisputed evidence discloses that Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos. The files on physicians in residency training were kept outside Dr. Ortega's office. Indeed, the only items found by the investigators were apparently personal items because, with the exception of the items seized for use in the administrative hearings, all the papers and effects found in the office were simply placed in boxes and made available to Dr. Ortega. Finally, we note that there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinets, although the absence of such a policy does not create

an expectation of privacy where it would not otherwise exist.

On the basis of this undisputed evidence, we accept the conclusion of the Court of Appeals that Dr. Ortega had a reasonable expectation of privacy at least in his desk and file cabinets.

Having determined that Dr. Ortega had a reasonable expectation of privacy in his office, . . . we must determine the appropriate standard of reasonableness applicable to the search. A determination of the standard of reasonableness applicable to a particular class of searches requires "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.

The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace. Government agencies provide myriad services to the public, and the work of these agencies would suffer if employers were required to have probable cause before they entered an employee's desk for the purpose of finding a file or piece of office correspondence. Indeed, it is difficult to give the concept of probable cause, rooted as it is in the criminal investigatory context, much meaning when the purpose of a search is to retrieve a file for work-related reasons. Similarly, the concept of probable cause has little meaning for a routine inventory conducted by public employers for the purpose of securing state property. To ensure the efficient and proper operation of the agency, therefore, public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons.

We come to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct. Even when employers conduct an investigation, they have an interest substantially different from "the normal need for law enforcement." Public employers have an interest in ensuring that their agencies operate in an effective and efficient manner, and the work of these agencies inevitably suffers from the inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees. Indeed, in many cases, public employees are entrusted with tremendous responsibility, and the consequences of their misconduct

13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

716 Part Three *Regulation of the Employment Environment*

or incompetence to both the agency and the public interest can be severe.... Public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner. In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers. The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest. Additionally, while law enforcement officials are expected to "schoo[l] themselves in the niceties of probable cause," no such expectation is generally applicable to public employers, at least when the search is not used to gather evidence of a criminal offense. It is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard. . . .

Balanced against the substantial government interests in the efficient and proper operation of the workplace are the privacy interests of government employees in their place of work which, while not insubstantial, are far less than those found at home or in some other contexts.... The employer intrusions at issue here "involve a relatively limited invasion" of employee privacy. Government offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may avoid exposing personal belongings at work by simply leaving them at home.

... We hold ... that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable:

Determining the reasonableness of any search involves a twofold inquiry: first, one must consider "whether the . . . action was justified at its inception," second, one must determine whether

the search as actually conducted "was reasonably related in scope to the circumstances which justified the interference in the first place."

Ordinarily, a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file. Because petitioners had an "individualized suspicion" of misconduct by Dr. Ortega, we need not decide whether individualized suspicion is an essential element of the standard of reasonableness that we adopt today. The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."

On remand, therefore, the District Court must determine the justification for the search and seizure, and evaluate the reasonableness of both the inception of the search and its scope.

Accordingly, the judgment of the Court of Appeals is REVERSED and the case is REMANDED to that court for further proceedings consistent with this opinion.

Case Questions

- Do you think the standard of the search articulated in this opinion is the correct standard for determining whether a search violates the Fourth Amendment? Think of arguments for both perspectives—the employer and employee.
- 2. How can an employer protect itself from a claim of an unreasonable search conducted in the workplace? Note the court stated that a policy regarding this issue was not a determinative factor in determining the constitutionality of the search.
- 3. What could you do as an employee to protesct yourself from a company search?

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 717



Michael A. Smyth v. The Pillsbury Company

914 F. Supp. 97 (E.D. Pa. 1996)

Michael Smyth worked for the Pillsbury Company. Pillsbury installed an electronic mail (e-mail) system in order to "promote internal communications between its employees." Pillsbury told its employees that e-mail transmissions were confidential and would not be intercepted or used by Pillsbury against its employees as grounds for termination. Smyth exchanged e-mails with his supervisor, which were, in fact, intercepted by Pillsbury management. Three months later, Smyth was terminated for transmitting what it deemed to be "inappropriate and unprofessional comments" over its e-mail system. (The e-mails contained threats to "kill the backstabbing bastards" in discussions of management and referred to the company holiday party as the "Jim Jones Kool Aid affair.")

Weiner, J.

Pennsylvania is an employment at-will jurisdiction and an employer "may discharge an employee with or without cause, at pleasure, unless restrained by some contract."

However, in the most limited of circumstances, exceptions have been recognized where discharge of an at-will employee threatens or violates a clear mandate of public policy. A "clear mandate" of public policy must be of a type that "strikes at the heart of a citizen's social right, duties and responsibilities."

Plaintiff claims that his termination was in violation of "public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law." In support for this proposition, Smyth directs our attention to a decision by our Court of Appeals in Borse v. Piece Goods Shop, Inc. In Borse, the plaintiff sued her employer alleging wrongful discharge as a result of her refusal to submit to urinalysis screening and personal property searches at her work place pursuant to the employer's drug and alcohol policy. After rejecting plaintiff's argument that the employer's drug and alcohol program violated public policy encompassed in the United States and Pennsylvania Constitutions, our Court of Appeals stated "our review of Pennsylvania law reveals other evidence of a public policy that may, under certain circumstances, give rise to a wrongful discharge action related to urinalysis or to personal property searches. Specifically, we refer to the Pennsylvania common law regarding tortious invasion of privacy."

The Court of Appeals in Borse observed that one of the torts which Pennsylvania recognizes as encompassing an action for invasion of privacy is the tort of "intrusion upon seclusion." As noted by the Court of Appeals,

the Restatement (Second) of Torts defines the tort as follows:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Liability only attaches when the "intrusion is substantial and would be highly offensive to the 'ordinary reasonable person." Although the Court of Appeals in Borse observed that "the Pennsylvania courts have not had occasion to consider whether a discharge related to an employer's tortious invasion of an employee's privacy violates public policy," the Court of Appeals predicted that in any claim where the employee claimed that his discharge related to an invasion of his privacy "the Pennsylvania Supreme Court would examine the facts and circumstances surrounding the alleged invasion of privacy. If the court determined that the discharge was related to a substantial and highly offensive invasion of the employee's privacy, [the Court of Appeals] believe[s] that it would conclude that the discharge violated public policy." In determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, the Court of Appeals predicted that Pennsylvania would adopt a balancing test which balances the employee's privacy interest against the employer's interest in maintaining a drug-free workplace. Because the Court of Appeals in *Borse* could "envision at least two ways in which an employer's drug and alcohol program might violate the public policy protecting

III. Regulation of the Employment Environment 13. The Employee's Right to Privacy and Management of Personal Information © The McGraw-Hill Companies, 2009

718 Part Three Regulation of the Employment Environment

individuals from tortious invasion of privacy by private actors" the Court vacated the district court's order dismissing the plaintiff's complaint and remanded the case to the district court with directions to grant Borse leave to amend the Complaint to allege how the defendant's drug and alcohol program violates her right to privacy.

Applying the Restatement definition of the tort of intrusion upon seclusion to the facts and circumstances of the case sub judice, we find that plaintiff has failed to state a claim upon which relief can be granted. In the first instance, unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an email system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of a urinalysis or personal property search, to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.

In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person

would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

In sum, we find that the defendant's actions did not tortiously invade the plaintiff's privacy and, therefore, did not violate public policy. As a result, the motion to dismiss is GRANTED.

Case Questions

- 1. Do you agree with the court's conclusion that, even if Smyth had a reasonable expectation of privacy of his transmissions, an interception would not be highly offensive to a reasonable person?
- 2. Are you sympathetic to an employer's reasons for wanting to intercept e-mail such as that involved in this case?
- 3. The court seems to be saying that, even though Pillsbury stated that it would not intercept e-mail, the employee should not have relied on this promise. Do you agree with this conclusion?



Yoder v. Ingersoll-Rand Company a.k.a. ARO

31 F. Supp. 2d 565 (W.D. Ohio 1997)

Lavern Yoder sued his employer, Ingersoll-Rand Company, to recover for damages he alleged were caused as a result of the employer's failure to keep his medical records confidential. Yoder was employed as a tow motor driver. After he learned that he was HIV-positive, Yoder made every effort to keep his HIV-positive status confidential from his employer because he was concerned that he might suffer adverse employment consequences if his employer or co-workers learned of his condition. A year and a half later, his doctor recommended that he take a medical leave of absence because of stress-induced asthma. An employment disability form was sent by mistake through the employer's mail system, through inner office mail, and then finally to Yoder's home, where it was read by his mother. She learned from the Physician's Statement that he had AIDS. She had known her son was HIV-positive but did not know he had AIDS. Yoder brought a complaint against the firm for permitting the unauthorized disclosure of his medical condition. Count four alleged state common-law claim for invasion of privacy. Both sides moved for summary judgment.

13. The Employee's Right to **Privacy and Management** of Personal Information

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 719

Katz, J.

E. Invasion of Privacy

Yoder alleges an invasion of privacy under the theory, public disclosure of private facts about the plaintiff with which the public has no legitimate concern, which is also known as the "publicity" tort. In order successfully to make out a claim under the "publicity" prong, Plaintiff must show five elements:

- (1) there must be publicity, i.e., the disclosure must be of a public nature, not private;
- (2) the facts disclosed must be those concerning the private life of an individual, not his public life;
- (3) the matter publicized must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities;
- (4) the publication must have been made intentionally, not negligently; and
- (5) the matter publicized must not be a legitimate concern to the public.

Plaintiff can show neither the first nor the fourth element of this test. As to the first element, Plaintiff can prevail only if he shows that the matter has been communicated to "the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." It is not enough to show merely that the matter was communicated by the defendant to a third person. The record evidence indicates that Plaintiff's HIV/AIDS status was actually communicated to only one unauthorized person. Even if the Court accepts Plaintiff's argument that mail clerk Kornrumpf and supervisor Chroninger should be treated as having received the information because they had the opportunity to read Plaintiff's medical report, the information was communicated to three people at most. Three

people do not constitute "the public at large." Plaintiff cannot meet the publicity prong of the test.

As to the fourth element, Plaintiff cannot show that Defendant, or its authorized agents, made the disclosure intentionally, even as to Plaintiff's mother. It is undisputed that nothing on the outside of the envelope received in the ARO mail room indicated that it contained a confidential medical record. Kornrumpf's testimony that she did not read the form beyond Plaintiff's name, and did not know that it was a confidential medical record, is undisputed. Chroninger's testimony that he did not read the form, and did not know that it was a confidential medical record, is undisputed. It is a logical impossibility for a party intentionally to disclose information that it does not know it has. Furthermore, the disclosure would not have occurred without Plaintiff's mother's intervening act of opening and reading the medical records without authorization from Defendant. Plaintiff cannot meet the intent prong of the test. Defendant's motion for summary judgment on Count IV is granted.

Plaintiff's motion for summary judgment is DENIED. Defendant's motion for summary judgment is GRANTED.

Case Questions

- 1. Do you think Yoder should have prevailed on his state law claim of invasion of privacy? Why or why not?
- 2. Do you think this case would have been decided differently if the mail clerk and Yoder's supervisor did read the doctor's statements?
- 3. How many people would have to read a sensitive document such as this to meet the public disclosure requirement for an individual to prevail on his or her claim?

720 Part Three *Regulation of the Employment Environment*



French v. United Parcel Service, Inc. 2 F. Supp. 2d 128 (D. Mass. 1998)

French began employment with UPS in March 1984. During the next 14 years, he rose through the ranks to become Business Manager of a UPS facility. One night after completing his shift, French invited three fellow UPS employees from the facility to attend a beer festival. One of the employees, DeButts, was a supervisory employee, but lower in rank than French. While at French's home, DeButts became intoxicated, emotionally volatile, and uncontrollable. When he was left alone in French's garage to "dry out," he lost control, went into a violent rage and caused injury to himself. French and the two other employees found DeButts lying in the garage bleeding. An ambulance was called and DeButts was taken to a local hospital where he was treated and released after 24 hours.

Following the incident, French's supervisor, Clark, requested that French report it to his superiors at the facility. Believing that the incident was none of UPS's business, French initially decided not to do so. Clark continued to press French, and later French informed the division manager of operations, his superior, of the incident. French was put on leave pending an investigation. As a result of this suspension, French began treatment for depression. During the next several months while French was still on leave, UPS personnel demanded that French meet with them to discuss the incident. In addition, UPS repeatedly contacted the mental health professionals who were treating French for depression to determine his condition and prognosis for recovery. At the end of the month, French was demoted to the position of supervisor. He returned to work but resigned about five weeks later because of the humiliation he felt in having to perform tasks that had not been his responsibility since the late 1980s. French brought this complaint, alleging four causes of action against UPS: invasion of privacy; reckless infliction of emotional distress; a violation of the Massachusetts Civil Rights Act; and wrongful constructive discharge. UPS moved to dismiss all four counts of French's complaint. The excerpt of the case provided below addresses only the invasion of privacy claims relevant to this chapter.

O'Toole, J.

Count I: Invasion of Privacy

The Massachusetts right of privacy statute provides that "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy." To constitute an invasion of privacy, the invasion must be both unreasonable and serious or substantial. French alleges that UPS violated his right to privacy by: (a) insisting that he disclose details concerning an incident that occurred during off-work hours at his home; (b) repeatedly contacting his mental health providers without his consent; and (c) penalizing him, in the form of involuntary leave and demotion, for the incident.

(A) Requiring Disclosure about the Incident

For purposes of the Massachusetts Privacy Act, "private" facts are not necessarily simply those that are "not

public," that is, not generally or widely known. Rather, [the Act] proscribes the "required disclosure of facts about an individual that are of a highly personal or intimate nature." The fact that a fellow employee drank too much at French's house is not a fact about French that is "highly personal or intimate." More importantly, the facts of what happened in the incident were not information that was "private" to French. Three other UPS employees took part in and observed the events, one of whom, Clark, was French's superior in the company hierarchy. Any of these persons was free to describe the incident; none had any apparent relationship with French that imposed some obligation of confidentiality. Indeed, as French's superior, Clark may even have owed UPS a duty to report, sua sponte, what he had observed. Be that as it may, it is surely unlikely that the Massachusetts courts would interpret § 1B to give French a right to prohibit Clark (or any one else who was present, including DeButts) from voluntarily disclosing what he had personally observed

© The McGraw-Hill Companies, 2009

Chapter Thirteen The Employee's Right to Privacy and Management of Personal Information 721

or done in connection with the incident. In short, the incident was simply not a "private" affair of French alone.

In addition, there are circumstances in which it is legitimate for an employer to know some "personal" information about its employees, so long as the information reasonably bears upon the employees' fitness for, or discharge of, their employment responsibilities. In the employment context "the employer's legitimate interest in determining the employees' effectiveness in their jobs [is] balanced against the seriousness of the intrusion on the employees' privacy." UPS has articulated legitimate business reasons for seeking information about the DeButts incident, including concerns about the soundness of judgment exercised by its supervisory employees in regard to alcohol abuse generally as well as in a particular setting where all participants were UPS employees. In light of these legitimate concerns, the company's questioning him about facts known to several other employees amounted, at most, to a de minimis intrusion into French's privacy, not actionable under the statute.

(B) Attempted Contact of Mental Health Care Providers

French also alleges that UPS "repeatedly contacted the mental health professionals who were treating the Plaintiff to determine his condition and prognosis for recovery. UPS made these contacts without the prior consent of the Plaintiff." The complaint does not allege that any private information was actually obtained by UPS. "Whatever unlawful invasion of privacy might have arisen if

the defendant[] had obtained some of the information sought..., the short answer is that...[t]he defendant['s] attempted invasion of privacy... failed." The Supreme Judicial Court has twice declined to decide whether the Privacy Act "reaches attempted interference with a person's privacy." The court has suggested that the statute may not reach attempts. Thus, [prior court rulings'] rejection of the "failed" invasion as a basis for liability apparently continues to express the law of Massachusetts on this question.

(C) Suspension and Demotion

The employment actions UPS took against French—putting him on involuntary leave and then demoting him—were not themselves an invasion of his privacy within the scope of the statutory cause of action. If these actions were wrongful, it would have to have been for some other reason.

Therefore, French's claim for invasion of privacy must be DISMISSED.

Case Questions

- 1. Do you agree with the court's decision? Why or why not?
- 2. Why do you think the court determined the employer had a right to inquire about the incident that occurred off-duty?
- 3. Why do you think UPS was so concerned about an incident that occurred off-duty?