Chapter 17

PRIVACY

LAWRENCE J. CASEY, ESQ.
Shilepsky Hartley Robb Casey Michon LLP, Boston

JOSHUA M. DAVIS, ESQ.
Goulston & Storrs, Boston

DEBORAH HESFORD DOSSANTOS, ESQ.
Lahey Health System, Burlington

NEIL V. MCKITTRICK, ESQ.
Ogletree, Deakins, Nash, Smoak & Stewart, PC, Boston

CLAIRE NEWTON, ESQ.
Shilepsky Hartley Robb Casey Michon LLP, Boston

Chapter 17, Part I
PRIVACY IN THE WORKPLACE: AN EMPLOYER PERSPECTIVE

JOSHUA M. DAVIS, ESQ.
Goulston & Storrs, Boston

DEBORAH HESFORD DOSSANTOS, ESQ.
Lahey Health System, Burlington

NEIL V. MCKITTRICK, ESQ.
Ogletree, Deakins, Nash, Smoak & Stewart, PC, Boston

Chapter 17, Part II
PRIVACY IN THE WORKPLACE: AN EMPLOYEE PERSPECTIVE

LAWRENCE J. CASEY, ESQ.
CLAIRE NEWTON, ESQ.
Shilepsky Hartley Robb Casey Michon LLP, Boston

Chapter 17, Part I

PRIVACY IN THE WORKPLACE: AN EMPLOYER PERSPECTIVE*

JOSHUA M. DAVIS, ESQ.
Goulston & Storrs, Boston

DEBORAH HESFORD DOSSANTOS, ESQ.
Lahey Health System, Burlington

NEIL V. MCKITTRICK, ESQ.
Ogletree, Deakins, Nash, Smoak & Stewart, PC, Boston

Scope Note

Part I provides an employer-side perspective on issues relating to privacy in the workplace. Applicable federal and state statutes are covered. Specific employer practices, including questionnaires, disclosures regarding an employee's discharge, employee medical and personnel records, drug testing, and access to employee credit reports and criminal records, and their limitations, are explained in detail. The extent to which employers may investigate employees via lie detector tests, physical searches, and surveillance is also discussed, along with limitations on employer interception of employee mail, e-mail, voice mail, and phone conversations. Part II provides an employee-side perspective. Limitations on employers' ability to disclose employees' medical information and facts regarding termination, conduct drug testing, maintain personnel files, access employees' criminal records, and intercept employees' mail are covered in detail, along with relevant case law. Employers' use of lie detector tests and physical searches during investigations are also discussed. Finally, the law regarding employer interception of employees' telephone and live conversations is presented.

* Updated for the 2013 Supplement by Neil V. McKittrick, Esq.

§ 17.1 INTRODUCTION

The principal source of privacy protection for employees in the private sector is the Massachusetts Right of Privacy statute, G.L. c. 214, § 1B. Courts have consistently recognized that an individual's right of privacy must be balanced against an employer's legitimate business objectives, which may involve obtaining or disclosing otherwise private information. Technology has made it possible to obtain considerable information, often without having to make direct requests to the persons involved or even to notify those people that the information is being collected. Some of this technology makes striking the right balance more complex for employers, employees, and courts. As our society continues to grapple with a changing global environment and the wide-reaching effects of technology, we will likely continue to redefine and refine the proper balance between an individual's right of privacy and an employer's legitimate need for information. Indeed, Massachusetts has recently seen the enactment of new data security laws that put in place safeguards to protect individuals' identifying information and the way in which it may be stored and disseminated, which further legislates an employee's right to privacy in the workplace. G.L. c. 93I; 201 C.M.R. § 17.

Massachusetts courts have addressed a variety of specific situations where an employer's business objective intersects or conflicts with an employee's right of privacy. Perhaps the most obvious example is drug testing, such as by urine sample. Serious privacy concerns are implicated by drug testing, but courts have consistently upheld such testing when the employer's business interest is sufficiently serious and related to the drug use information. While drug testing may not be a concern for every employer, such common practices as gathering information via employee questionnaires, disclosing the reasons for the termination of an employee to third parties, and recording employee phone calls also implicate privacy concerns. The Massachusetts case law on these topics, as well as certain other issues, is outlined below.

In addition to the Massachusetts Right of Privacy statute, there are at least three other sources of law that are potentially relevant in an analysis of an individual's right of privacy. First, the Massachusetts Civil Rights Act, G.L. c. 12, § 11I, establishes a cause of action for individuals whose rights, as secured by the federal and state constitutions and by the laws of the United States and the Commonwealth, have been interfered with by "threats, intimidation or coercion." Threats of adverse employment action or actual adverse employment action, in conjunction with a violation of an employee's privacy, may be actionable under the Civil Rights Act. In *Webster v. Motorola, Inc*., 418 Mass. 425 (1994), the Supreme Judicial Court held that an employer's threat to terminate an "at will" employee if he did not submit to an invasion of his privacy (in this case, random drug testing) was not actionable under the Civil Rights Act. *See also Carmack v.*

AMTRAK, 486 F. Supp. 2d 58, 80–81 (D. Mass. 2007) (reasonable for employer to terminate employee for failing to undergo fitness-for-duty examination where employee was perceived to pose threat to public using rail services, and, accordingly, examination not invasion of employee's privacy). However, in *Tuli v. Brigham & Women's Hospital*, 566 F. Supp. 2d 32 (D. Mass. 2008), the court

(Text continues on p. 17–3.)

held that an employer-required medical exam may be an invasion of the employee's privacy, especially "where a psychiatric or medical evaluation is used as a tool of harassment or discrimination." *Tuli v. Brigham & Women's Hosp.*, 566 F. Supp. 2d at 58. The Supreme Judicial Court has reaffirmed that in some situations economic pressure alone can satisfy the "threats, intimidation or coercion" requirement of the Massachusetts Civil Rights Act (MCRA). G.L. c. 12, §§ 11H, 11I; *Buster v. George W. Moore, Inc.*, 438 Mass. 635, 647 (2003).

Second, under the Fourth Amendment of the U.S. Constitution and Article 14 of the Massachusetts Declaration of Rights, public employees have greater rights of privacy than do those who are not employed in the public sector. Private companies may, however, be held to the standards of public employers if government involvement in, or control over, a private employer's activities is so great that the private employer is found to be a "state actor." The same is true for private employers that take on governmental roles. Courts usually decide whether the additional protections associated with government activities—protections that stem from federal and state laws and constitutions—apply to a private entity based on the degree to which the private entity has become a "state actor." *See, e.g., Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989). An employer that receives substantial government funding or whose activities are closely intertwined with a federal or state agency should be sensitive to the greater privacy protections that cover government employees and that may, in some cases, apply to the employer's own workers.

Cases decided under the state Civil Rights Act and cases in which federal and state constitutional rights are implicated are beyond the scope of this chapter; however, the authors will briefly survey a third type of authority—state and federal statutes that deal with issues related to privacy and that may confer certain protections on employees in the workplace. After addressing the cases concerning the Massachusetts right of privacy, the authors will address these additional statutes below.

§ 17.2 MASSACHUSETTS' RIGHT OF PRIVACY STATUTE

Massachusetts has enacted a fairly comprehensive statutory right of privacy. This privacy statute is considered analogous to the common law cause of action for public disclosure of private facts. *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. 508, 519 n.15 (1984). The statute, G.L. c. 214, § 1B, provides: "A person shall have a right against unreasonable, substantial or serious interference with his privacy." The statute specifies that a plaintiff whose privacy rights have been violated may seek an injunction against the intrusive practice, as well as money damages. *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. at 519 n.15.

Massachusetts courts have interpreted this statute to protect private facts of a "highly personal or intimate nature" relating to a matter not of legitimate concern to the public. *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. at 518. However, a person may surrender his expectation of privacy, even for facts that are highly personal or intimate in nature. As the Supreme Judicial Court has noted, "a person may relinquish a privacy right by engaging in certain activities, or by placing himself in certain contexts where his legitimate expectation of privacy is reduced." *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 409 Mass. 514, 521 (1991). The Supreme Judicial Court has held that an employer's otherwise impermissible disclosures about an employee involved in a highly public matter were not actionable under the statute because they "only provided further publicity on a matter that was already squarely in the public eye." *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. 367, 384 (2005), *cert. denied*, 126 S. Ct. 397 (2005). Whether the expectation of privacy has been relinquished is a question of fact, to be examined on a case-by-case basis. *Lemire v. Silva*, 104 F. Supp. 2d 80, 93 (D. Mass. 2000). Consent to the disclosure is an absolute defense to the claim for invasion of privacy because it eliminates any expectation of privacy. *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 409 Mass. at 520–21.

In determining whether a given practice violates the right of privacy, courts ask first whether the intrusion is unreasonable, and second whether the intrusion is also serious or substantial. *See Ball v. Wal-mart, Inc.*, 102 F. Supp. 2d 44, 50 (D. Mass. 2000). Courts have placed particular importance on the statute's use of the word "unreasonable" in assessing any alleged interference with privacy. As a result, there are few absolute prohibitions on an employer's methods of obtaining private information or using such information. Additionally, to violate the statute, an employer actually must "gather or disseminate" information. *Dasey v. Anderson*, 304 F.3d 148, 154 (1st Cir. 2002). Discharging an employee for failing to provide private information may contravene public policy as embodied in the Massachusetts Privacy Act and warrant the imposition of liability on the employer under the so-called public-policy exception to the rule of "at will" employment, but it is not an invasion of privacy. *Cort v. Bristol-Myers Co.*, 385 Mass. 300, 307 (1982).

Defining what is reasonable information-gathering or disclosure in the employment context means considering the employer's reasons and objectives for obtaining or sharing the information. The Supreme Judicial Court has instructed that courts must balance "the employer's legitimate business interest in obtaining and publishing the information against the substantiality of the intrusion on the employee's privacy resulting from the disclosure." *Bratt v. Int'l Bus. Machs. Corp*., 392 Mass. at 521. In practice, absent a statutory or judicial prohibition against certain conduct, an employer will be permitted to use reasonable means to obtain and disclose information for demonstrable and proper business purposes.

The reasonableness of an employer's practice will often be a fact-specific determination in individual cases, sometimes requiring the court to examine the policy as it applies to individual employees. *See Webster v. Motorola, Inc*., 418 Mass. 425, 432–33 (1994) (holding that drug testing was permissible as applied to employee who drove company car 20,000 miles per year, but not permissible for technical editor).

While one might assume that disclosure of private facts could be justified if limited to members of the company, and not available to the general public, the Supreme Judicial Court has found otherwise. The Supreme Judicial Court has instructed "that the disclosure of private facts about an employee among other employees in the same corporation can constitute sufficient publication under the Massachusetts Right of Privacy statute." *Bratt v. Int'l Bus. Machs. Corp*., 392 Mass. 508, 519 (1984); *see also Oropallo v. Brenner*, No. 06-0447, 2009 Mass. Super. LEXIS 13, at *15 (Mass. Super. Ct. Jan. 14, 2009).

§ 17.3 SPECIFIC PRACTICES

§ 17.3.1 Questionnaires

Employers are entitled to survey or question employees on matters that are "reasonably related to job performance." *Carney v. City of Springfield*, 403 Mass. 604, 610 (1988). Employers may also compel employees to answer job-performance-related questions under threat of discharge. *Carney v. City of Springfield*, 403 Mass. at 610.

Specifically, questions requesting information about business experience, education, family, home ownership, physical data, personal activities, and professional aims, including desired income, have been found not to violate an employee's privacy. *See Cort v. Bristol-Myers Co.*, 385 Mass. 300, 308–10 (1982). However, the information that a high-level or confidential employee may reasonably be expected to disclose is broader in scope and more personal in nature than what should be expected from lower-level employees. Therefore, a questionnaire that might be appropriate for a high-ranking executive might be unreasonably intrusive for a lower-level employee. In *Cort*, the Supreme Judicial Court held that the employer was permitted to ask the questions described above of drug salespersons whom the court viewed as holding positions close to upper-level managers. *Cort v. Bristol-Myers Co.*, 385 Mass. at 308. The Supreme Judicial Court noted, however, that the information requested about family, home ownership, and personal activities, although not highly personal, was also of little use to the employer, *Cort v. Bristol-Myers Co*, 385 Mass. at 310, and the court stated that if an employer had no right to ask a question, the employee could not properly

be discharged for failing to answer the improper question(s). *Cort v. Bristol-Myers Co.*, 385 Mass. at 307. Employers should therefore be careful to design questionnaires that relate to business objectives.

§ 17.3.2 Information About Another Employee's Termination

As noted above, the disclosure of private information need not be made to the general public to be actionable as a violation of privacy. Information about employees must be handled appropriately within the company to prevent violations of employee privacy. Perhaps the most common area where this issue arises is when one employee has been discharged, and the employer would like to make the reasons or circumstances known to other employees.

In *Mulgrew v. City of Taunton*, 410 Mass. 631, 637 (1991), the Supreme Judicial Court held that disclosures of the reasons for terminating an employee, including the facts that he was a "sick day abuser" and left under "a cloud of suspicion," did not violate the employee's privacy. However, *Mulgrew* involved a police officer, and the court viewed the disclosures as directly related to the strong interest of the employer-police department in ensuring the competency of the police force. *Mulgrew v. City of Taunton*, 410 Mass. at 637. Similar disclosures by a private employer may not be seen as equally necessary.

At least one Massachusetts court has recognized that "[i]nforming subordinates of a coworker's performance problems could constitute an unprivileged invasion of privacy . . . ." *Williams v. Commonwealth Limousine Serv., Inc.*, No. 98-4351, 1999 Mass. Super. LEXIS 17, at *3 (Mass. Super. Ct. Jan. 26, 1999). In *Williams*, the company had posted in a public area on its property the termination letter addressed to the plaintiff, which detailed his failures in the areas of grooming, driving, personal expenses, and following company policies. *Williams v. Commonwealth Limousine Serv., Inc.*, 1999 WL 1331281, at *1. The Superior Court determined that whether this posting unreasonably and substantially or seriously interfered with Williams' right of privacy was an issue for the jury and therefore denied the employer's motion to dismiss. *Williams v. Commonwealth Limousine Serv., Inc.*, 1999 WL 1331281, at *3. The First Circuit has addressed whether a terminated employee could prevail on a libel claim after a company executive disseminated an e-mail message containing the details of the terminated employee's conduct. *Noonan v. Staples*, 539 F.3d 1 (1st Cir. 2008). The court held that the e-mail message contained true information about the terminated employee, and that the executive had not acted with actual malice. The court specifically noted that even broad dissemination to 1,500 employees did not constitute actual malice. Thus, there was no basis for the former employee's libel claim. *Noonan v. Staples*, 539 F.3d at 6–10. While these cases do not offer

much guidance for employers on how to strike the appropriate balance in a privacy dispute, they assume that there could be a business purpose for making such information known and that this must be balanced against the employee's right of privacy. Companies should be mindful of that balance in determining how termination information is handled within the company.

§ 17.3.3 Medical Information

Employers often want or need medical information about employees. Medical and therapeutic information is protected by the same degree of privacy as other personal information, *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. 508, 522 (1984), by the additional protection of the physician-patient privilege, and by specific state and federal statutes and regulations. The Supreme Judicial Court has explicitly noted that "an employer may have a substantial and valid interest in aspects of an employee's health that could affect the employee's ability effectively to perform job duties." *Webster v. Motorola, Inc.*, 418 Mass. 425, 432 (1994) (quoting *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. at 524). Because of this recognized legitimate employer interest, an employer who obtains or discloses medical information regarding an employee is not necessarily liable for an invasion of privacy. Instead, the courts apply a slightly modified version of the balancing test in these situations. When an employer obtains from a physician or discloses medical information relating to an employee, the ultimate question is whether the degree of the intrusion into the employee's privacy and the public interest in preserving the confidentiality of the physician-patient relationship outweigh the employer's need for the medical information. *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. at 523.

One court has held that the disclosure to other employees, including managers and junior staff, of an employee's report that he or she has AIDS can constitute an invasion of the employee's privacy. *Cronan v. New Eng. Tel. & Tel. Co.*, No. 80332, 1986 Mass. Super. LEXIS 1, 41 Fair Empl. Prac. Cas. (BNA) 1273 (Mass. Super. Ct. Aug. 15, 1986). Similarly, an employee's claim survived summary judgment where the employer had distributed the employee's psychiatric evaluation to people not in a supervisory position over the employee, and had posted the employee's medical excuse note in a public location for other employees to see. *Wagner v. City of Holyoke*, 241 F. Supp. 2d 78, 100 (D. Mass. 2003), *aff'd*, 404 F.3d 504 (1st Cir. 2005), *cert. denied*, 126 S. Ct. 552 (2005).

It was not an invasion of privacy, however, for an employer to require that employees in safety-sensitive positions consult with the employer and disclose all prescription or over-the-counter medications that each employee was taking that could impair the abilities of the employees to perform their duties. *Byrne v. Mass. Bay Transp. Auth.*, 196 F. Supp. 2d 77, 85–86 (D. Mass. 2002).

Employers must also be careful about the way in which they collect and maintain employee health information obtained in the course of medical examinations performed on present or prospective employees. The Americans with Disabilities Act (ADA) and its accompanying regulations require such information to be maintained in separate medical files (i.e., not in employees' regular personnel files) and treated as confidential medical records. 42 U.S.C. § 12112(d)(3); 29 C.F.R. § 1630.14. Employers may only disclose such information as necessary to supervisors who need to know about an employee's restrictions or accommodation needs, safety personnel who may need to provide emergency treatment, or government officials monitoring compliance with the law. 42 U.S.C. § 12112(d)(3); 29 C.F.R. § 1630.14.

Many employers are not considered covered entities required to comply with the rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) prohibiting the wrongful disclosure of individually identifiable health information. 42 U.S.C. § 1320d-6. HIPAA imposes strict confidentiality requirements on "health plans," "health care clearinghouses," and "health care providers." 45 C.F.R. § 160.102. Only employers that provide self-insured medical benefits are covered entities under HIPAA; others are not covered entities, and, therefore, are not bound by the confidentiality requirements of the law. *See Brown v. Massachusetts Office on Disability*, No. 06-12029, 2008 U.S. Dist. LEXIS 19019, at *20 n.8 (D. Mass. Mar. 7, 2008). However, employers who receive private health information from a HIPAA-covered entity for the purposes of administering a health plan can use that information only for the designated purpose, and not for other personnel actions. Finally, HIPAA does not provide for a private right of action, providing recourse only through a complaint with the U.S. Secretary of Health and Human Services. 45 C.F.R. § 160.306; *see also Brown v. Massachusetts Office on Disability*, 2008 U.S. Dist. LEXIS 19019, at *20 n.8.

See also the discussion of statutes relating to medical records, below.

§ 17.3.4 Medical Information Held by an Employer-Retained Physician

Special issues arise where an employer hires or pays the physician or therapist examining the employee. The first issue is whether a physician-patient relationship exists and therefore cloaks information with the physician-patient privilege. The answer seems to be no. The Supreme Judicial Court, in dicta in *Bratt*, stated that "[w]hen an employer retains a physician to examine employees, generally no physician-patient relationship exists between the employee and the doctor." *Bratt v. Int'l Bus. Machs. Corp*., 392 Mass. at 523 n.21; *accord Hoesl v. United States*,

451 F. Supp. 1170, 1176 (N.D. Cal. 1978), *aff'd*, 629 F.2d 586 (9th Cir. 1980); *Jones v. Tri-State Tel & Tel. Co.*, 136 N.W. 741 (Minn. 1912).

To determine whether such a relationship was formed and therefore whether the privilege applies, courts usually look at whether the individual was examined for treatment or diagnosis on the one hand, or for a business-related evaluation (because the employer wants information for its own purposes) on the other hand. Where the examination was for business-evaluation purposes, one Massachusetts court has found that no physician-patient relationship was formed and no privilege applies, therefore permitting production of the psychotherapist's report. *Morgan v. Geran*, No. 99-2118H, 2001 Mass. Super. LEXIS 53, at *7–8 (Mass. Super. Ct. Jan. 25, 2001). Following this reasoning, employers likely can demonstrate that if the consultation or examination was sought for business purposes (such that a physician-patient relationship did not arise), those same business purposes might outweigh the employee's privacy interest in the information. This is still an undeveloped area of law, however, and there are few reported cases.

§ 17.3.5 Drug Testing

As mentioned above, an employer may demonstrate legitimate business purposes for drug testing. *Webster v. Motorola, Inc.*, 418 Mass. 425 (1994), continues to be the leading Massachusetts case on drug testing. In that case, Motorola had instituted a universal drug-testing program, where employees were randomly selected by a computer (over a three-year cycle) for testing. After notification, employees reported to a collection site and were given the opportunity to discuss medications that might affect the testing. Then employees gave a urine specimen, with a technician standing immediately outside a bathroom. *Webster v. Motorola, Inc.*, 418 Mass. at 426–27. Motorola had a complex procedure for dealing with positive results, including further consultation with the employee about medications and dietary issues, access to an employee assistance program, and a rehabilitation plan created by an outside provider. *Webster v. Motorola, Inc.*, 418 Mass. at 427–28. Two employees, a technical editor and an account executive, filed suit objecting to this policy. Applying the balancing test explained in *Bratt*, the Supreme Judicial Court noted that compulsory urinalysis "involves a significant invasion of privacy." *Webster v. Motorola, Inc.*, 418 Mass. at 431 (quoting *Folmsbee v. Tech Tool Grinding & Supply Co.*, 417 Mass. 388, 392 (1994)). Turning to the specific job duties of the two individuals, the Supreme Judicial Court concluded that, although all businesses "have a general interest in protecting the safety of their employees and in providing them a drug-free environment in which to work," this interest alone was not enough to outweigh the privacy interests of the technical editor. *Webster v. Motorola, Inc.*, 418 Mass. at 433. Because the account executive had a company-owned car and was required to drive 20,000 to 25,000 miles per year, the additional interest in ensuring

that he did not operate the car while intoxicated was sufficient to justify the "significant" invasion of the executive's privacy. *Webster v. Motorola, Inc.*, 418 Mass. at 433.

At least one court also has found that a policy requiring manufacturing employees to be tested for drugs following an on-duty accident with the machinery was permissible. *Harrison v. Eldim, Inc.*, No. 99-404-F, 2000 Mass. Super. LEXIS 33 (Mass. Super. Ct. Feb. 17, 2000). Further, direct observation of an employee urinating may be permissible in limited circumstances where there is reason to suspect tampering with the sample. *Byrne v. Mass. Bay Transp. Auth.*, 196 F. Supp. 2d 77 (D. Mass. 2002). Observation also may be permissible when the employee has agreed to urinalysis as a condition of employment. *O'Connor v. Police Comm'r of Boston*, 408 Mass. 324 (1990).

§ 17.4 OTHER AUTHORITY FOR PRIVACY CLAIMS

In addition to the generalized right of privacy discussed above, many other statutes may implicate privacy issues. These statutory limitations will supersede the privacy balancing test if they apply in any particular context. For example, certain statutes control an employer's preemployment inquiries and inquiries as part of an employer's investigation, and they limit an employer's ability to disclose any information that it acquires through the employment relationship. The laws of other countries may also apply to a business with offices and employees abroad. Lawyers must be familiar with these statutes when advising management in its handling of employee information.

§ 17.4.1 Credit Reports

Both G.L. c. 93, §§ 50–68 and the federal Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x, regulate the use of credit reports produced by private reporting companies on individuals. Both statutes permit employers to obtain these reports, but only for "employment purposes." G.L. c. 93, § 51; 15 U.S.C. § 1681a(d)(1)(B). The FCRA defines employment purposes as "evaluating a consumer for employment, promotion, reassignment or retention as an employee." 15 U.S.C. § 1681a(h).

Under the FCRA, an employer requesting an employee's or an applicant's credit report must (1) make a separate written disclosure to the employee or applicant that a credit report may be obtained for employment purposes; and (2) obtain the employee or applicant's written authorization. 15 U.S.C. § 1681b(b)(2)(A). If an

employer seeks a report that contains not only credit information, but also information on the individual's character and reputation obtained through personal interviews (an "investigative consumer report"), G.L. c. 93, § 53 requires the employer to (1) disclose to the employee or prospective employee, in writing, its intention to request a report; (2) disclose the precise nature and scope of the investigation requested; (3) disclose the employee's or applicant's right to have a copy of the report provided on request; and (4) obtain the employee's or applicant's written permission prior to making the request for the report. The Massachusetts requirements on this point are more stringent than the FCRA requirements. Because they are not preempted by the FCRA, they are controlling upon Massachusetts employers. *Cf.* 15 U.S.C. § 1681d.

If the employer subsequently decides to take adverse action against the employee or applicant based on the information in the report, it must comply with the FCRA by providing the employee or applicant with a copy of the report and a Summary of Consumer Rights form prior to taking the adverse action. 15 U.S.C. § 1681b(3)(A). There are two limited exceptions to this requirement: (1) U.S. government agencies taking adverse employment action in the context of a national security investigation, and (2) employers that are interstate motor carriers or regulated by a state transportation agency and receive applications remotely. 15 U.S.C. § 1681b(3), (4). The Massachusetts statute providing different requirements for taking adverse action on the basis of a credit report, G.L. c. 93 § 62, is explicitly preempted by the FCRA, and thus is not controlling. 15 U.S.C. § 1681t(b)(1)(C); *see also* Philip H. Myers, Annotation, "Construction and Application of Fair Credit Reporting Act (15 U.S.C.A. §§ 1681 et seq.)," 17 *A.L.R. Fed.* 675 (1973–2005).

In 1999, a staff attorney of the Federal Trade Commission (FTC), which enforces the FCRA, issued a written opinion (the "Vail Letter") asserting that employment-related investigations conducted for clients by outside counsel were "consumer credit reports" for purposes of the FCRA. Therefore, the staff attorney opinion stated, prior approval of such investigations would be required from the employee involved, and a copy of the report should be provided to that employee. Federal Trade Commission, Staff Opinion Letter, Apr. 5, 1999, available at http://www.ftc.gov/os/statutes/fcra/vail.htm (last visited Aug. 10, 2009). Various courts considered and rejected the FTC's position. Subsequently, Congress passed the Fair and Accurate Credit Transactions (FACT) Act of 2003 in response to the controversy. Pub. L. No. 108-59, 117 Stat. 1952 (codified at 15 U.S.C. § 1681).

The FACT Act excluded certain types of third-party reports from the definition of "consumer credit reports," overturning the Vail Letter. Investigations of "suspected misconduct relating to employment" or "compliance with Federal, State, or local laws and regulations, the rules of a self-regulatory organization, or any

preexisting written policies of the employer" are not credit reports under the FCRA if they are reported to the employer or its agents only. 15 U.S.C. § 1681a(x)(1)(B), (D). This provision releases employers using third parties to investigate suspected misconduct from having to secure the employee's consent before investigating, and from having to give the employee a copy of the report.

However, the FACT Act imposes different requirements on these reports. After taking adverse action based on this type of report, the employer must provide the employee with a "summary containing the nature and substance" of the report, which may exclude, at the very least, the sources of the information. 15 U.S.C. § 1681a(x)(2). It is not clear whether this summary must be in writing, and the time given the employer to provide the summary, once the adverse action has been taken, is not specified.

Further, because the report only may be given to the employer or its agents (or other listed entities, such as law enforcement) for it to qualify under the FACT, employers must be cautious in sharing such reports too broadly, as such action could subject the report to the stricter notice and disclosure requirements of the FCRA. This limitation on sharing the report raises a potential conflict with the victim's right to know the results of an investigation of his or her accused harasser as defined by the EEOC. To follow both the FACT and the EEOC requirements as closely as possible, employers should provide only the summary of the report—and not the report itself—to the victim. For further guidance, see Rod M. Fliegel & Ronald D. Arena, "The Impact of the FACT Act on Employee Misconduct Investigations and Implications for FCRA and Title VII Compliance," 20 *Lab. Law.* 97 (2004).

§ 17.4.2 Personnel Records

General Laws c. 149, § 52C gives employees a right of access to their personnel records maintained by either present or former employers. The employer must respond to an employee's written request for his or her personnel records within five business days. However, the statute does not address whether and under what circumstances an employer may disclose information contained in an employee's personnel file to individuals other than the employee. The legality of such a disclosure would thus be determined under the general privacy statute by balancing the employer's business interest in disclosing the information contained in the records against the employee's interest in maintaining his or her confidentiality. In addition, the disclosure of personnel file information may implicate the Massachusetts data security laws, the ADA, or HIPAA, and employers should be mindful of those laws when deciding whether to disclose to a third party information contained in a present or former employee's personnel file.

In 2010, the legislature amended G.L. c. 149, § 52C to, among other things, require employers to notify employees within ten days of placing in their personnel records any information that has been used or may be used negatively to affect the employee's qualification for employment, promotion, transfer, or additional compensation, or the possibility that the employee will be subject to disciplinary action. In the privacy context, this amendment expedites the need for employers to assess the privacy implications of placing information in an employee's personnel file, even when it may contain private information about a third person.

§ 17.4.3 Criminal Records

Under G.L. c. 151B, § 4(9), employers may not ask about, make a record of, or discriminate against any person for failing to furnish information regarding

- an arrest record or a detention that did not result in a conviction;
- convictions for certain minor misdemeanors; or
- convictions for any misdemeanors dating back more than five years from the date of the employment application.

The Massachusetts Criminal Offender Record Information Reform Act (the CORI Reform Act), enacted in 2010 and fully implemented in 2012, significantly limits an employer's use of criminal record information in making employment decisions.

In accordance with the act, most employers are now prohibited from asking about applicants' criminal histories on their initial written employment applications. The interpretive guidance issued about the amended law states that "initial written application" means any preinterview applicant inquiry, so that an employer (excluding certain employers whom the statute exempts, *see* G.L. c. 151B, § 4(9½)) may not ask about an applicant's criminal history before conducting an interview. At the interview stage, an employer is permitted to ask employees or prospective employees if they have a felony record and to ask about misdemeanors not included in the prohibition under G.L. c. 151B, § 4(9). If an employer requests this information, however, it must expressly inform the employee that he or she is permitted to respond "no record" if his or her criminal records have been sealed pursuant to G.L. c. 276, § 100A. If an employer requests information regarding an applicant's prior convictions, the employer must, under G.L. c. 276, § 100A, include the following statement on the form requesting the information:

> An applicant for employment with a sealed record on file with the commissioner of probation may answer "no record" with respect to an inquiry herein relative to prior arrests, criminal court appearances or convictions. An applicant for employment with a sealed record on file with the commissioner of probation may answer "no record" to an inquiry herein relative to prior arrests or criminal court appearances. In addition, any applicant for employment may answer "no record" with respect to any inquiry relative to prior arrests, court appearances and adjudications in all cases of delinquency or as a child in need of services which did not result in a complaint transferred to the superior court for criminal prosecution.

Moreover, under G.L. c. 6, § 172, employers may not ask an individual to "provide a copy of [his or her] criminal offender record information." However, employers may seek and obtain certain specified criminal history information from the state's Department of Criminal Justice Information Services pursuant to G.L. c. 6, § 172, but felony information is limited to the previous ten years, and misdemeanor information is limited to the previous five years. Additionally, employers must obtain a signed acknowledgment form from the applicant before requesting the information, and they must retain that form for at least one year.

Other changes under the CORI Reform Act include the following:

- prior to questioning an individual about his or her criminal history in connection with an employment decision, employers in possession of the individual's criminal record information must provide a copy of the record to the individual;

- if an employer makes an adverse decision on the basis of an individual's criminal history, the employer must provide a copy of the criminal record information in the employer's possession, regardless of the source from which it was obtained;

- employers that annually conduct five or more criminal background checks must maintain a written CORI policy and include in the policy that the employer will

  – notify the applicant of the potential adverse decision based on criminal record information,

  - provide a copy of the individual's criminal history information and the employer's policy to the applicant, and
  - provide information concerning the process for correcting a criminal record;

- CORI may only be shared with individuals within the employer's business who a need to know the information;
- employers must maintain a dissemination log for one year following the dissemination of an individual's CORI; and
- employers may not keep records of the information obtained for more than seven years from the last date of employment.

§ 17.4.4 Medical Records

Numerous statutes protect the confidentiality of an individual's medical records and communications and thus preclude an employer's access to such information. Under the Massachusetts Patients' Rights Statute (G.L. c. 111, § 70E), G.L. c. 111, § 70, and G.L. c. 111E, § 18, all medical records held by licensed facilities, such as hospitals, clinics, and nursing homes, including records relating to treatment for drug and alcohol dependency, are confidential. Under statutory and common law privileges, communications between an individual and a physician, a psychotherapist (G.L. c. 233, § 20B), and a social worker (G.L. c. 112, § 135A), are confidential.

Moreover, under G.L. c. 151B, §§ 4(9A), 4(16) and the ADA, 42 U.S.C. § 12112(d)(2), employers are prohibited from making preemployment inquiries into whether a prospective employee has been treated for mental illness or drug or alcohol dependency. Under 42 U.S.C. § 12112(d)(3), employers may not conduct "medical examinations" of prospective employees until after a conditional offer of employment is made, and 42 U.S.C. § 12112(d)(4)(A) subjects employers to greater restrictions when conducting medical examinations of current employees. The Seventh Circuit has held that a test that measured personality traits and could be used to help diagnose certain psychiatric disorders (the Minnesota Multiphasic Personality Inventory, or MMPI) was a prohibited "medical exam" under the ADA. *Karraker v. Rent-a-Center, Inc.*, 411 F.3d 831, 836–37 (7th Cir. 2005).

As discussed above, even where employers are permitted to conduct medical examinations, the ADA requires employers to maintain the gathered information in a separate, confidential medical file, *not* in the employee's personnel file, and

the information may only be shared with specific individuals under certain circumstances. 42 U.S.C. § 12112(d)(3); 29 C.F.R. § 1630.14. Most employers do not need to follow the strict requirements under HIPAA, as discussed above, but employers who do provide self-insured health benefits or are otherwise covered under the law must follow HIPAA's stringent confidentiality requirements. 42 U.S.C. § 1320d-6; 45 C.F.R. § 160.102. Moreover, employers who receive private health information from a HIPAA-covered entity for the purposes of administering a health plan can use that information only for the designated purpose, and not for other personnel actions.

§ 17.4.5 Use of Employee Names or Images for Commercial Purposes

General Laws c. 214, § 3A prohibits use of an individual's name, portrait, or picture for advertising or other commercial purposes without the individual's written consent. The statute also provides a private right of action and allows courts to award treble damages for knowing violations. As a result, an employer who plans to use an employee's name or any form of an employee's image in furtherance of its commercial goals must obtain the employee's written consent. Employers should consider the impact of this statute when designing promotional materials such as websites, mailings, publications, or press releases.

§ 17.4.6 Protection of Employee Personal Information

In 2007, Massachusetts enacted a new set of laws protecting individuals' personal information from identity theft by requiring holders of such information, including employers, to take certain precautionary steps. G.L. c. 93H, 93I. Chapters 93H and 93I, as well as the accompanying regulations (201 C.M.R. § 17.00), set forth minimum standards for proper maintenance and disposal of paper or electronic records containing personal information, put in place steps for businesses to follow in the event of a security breach, and require businesses to put in place an information security plan in order to protect individuals' personal information, including employees' identifying information.

In both chapters, "personal information" is defined to include a Massachusetts resident's first and last name (or first initial and last name) in combination with any one or more of the following: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without access codes. *See* G.L. c. 93H, 93I. "A financial account is an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result. Examples of a finan-

cial account are: checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account." Massachusetts Office of Consumer Affairs and Business Regulation, "Frequently Asked Question Regarding 201 CMR 17.00," *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf.

In the case of records disposal, "biometric indicators" are also covered. *See* G.L. c. 93I. Employers should take reasonable precautions to protect employee personal information and must dispose of records containing such information so that the information cannot practicably be read or reconstructed. In the event that an employer's systems are compromised under circumstances that raise a substantial risk of identity theft, the employer must give the prescribed forms of notice set forth in the statute.

§ 17.4.7 Employers with Offices in the European Union

Privacy protection in many countries outside the United States is more systematic and strict. The European Union, for example, has adopted a Directive on Privacy Protection, 95/46/EC, which took effect on October 25, 1998. The directive treats privacy as a fundamental human right and requires member states to adopt national legislation insuring the protection of privacy, if they wish to participate in the free flow of information within the European Union. Both member states and nonmember states doing business with them are required to adhere to undefined "minimum standards" in processing "personal data," broadly defined as "any information relating to an identified or identifiable natural person." After lengthy negotiations, the United States reached an accord with the European Union known as the Safe Harbor Principles. The Safe Harbor Principles went into effect on November 1, 2000. Participation in the safe harbor creates a presumption that the organization provides an adequate level of privacy protection and qualifies the company to receive data from EU member states. Companies with European employees, as well as companies doing business with European customers, which need to share personal data about citizens of EU member states, must become familiar with the Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000), and the Issuance of Principles and Transmission to European Commission: Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (Sept. 19, 2000). The U.S. Department of Commerce's Web site provides further guidance on the safe harbor principles at http://www.export.gov/safeharbor.

As an alternative to participating in the safe harbor, U.S. companies may also use preapproved contract clauses to receive data from the European Union. See European Commission, Data Protection Web site, Model Contracts, for the

transfer of personal data to third countries, at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.html.

§ 17.5 LIMITS ON EMPLOYER INVESTIGATION

In addition to the cases and statutes discussed above, other laws limit the means available to an employer investigating an applicant or employee. These statutes and cases, both federal and state, address more extreme types of investigation—intercepting mail, conducting lie detector tests, or searching the workspace or person of an employee.

§ 17.5.1 Intercepting Mail

A federal statute, 18 U.S.C. § 1702, prohibits the interception or obstruction of another person's postal mail and imposes criminal penalties for such conduct. This is a criminal statute, enforced by the federal government. There is no comparable state statute, and any private challenges to the interception and obstruction of personal correspondence would have to be made under the Commonwealth's general right of privacy statute. An employer would have an uphill battle to justify opening mail that is clearly personal even though it was received at the workplace, but it should be permitted to open mail reasonably believed to be business correspondence and to open correspondence to check whether it is business related.

(Text continues on p. 17–17.)

§ 17.5.2 Lie Detector Tests

General Laws c. 149, § 19B prohibits employers from requesting or requiring their employees or prospective employees to take any form of lie detector test, and it further prohibits any retaliatory action against employees for asserting rights secured by the statute. The statute also requires that all employers notify employees and prospective employees that it is unlawful to ask them to take a lie detector test. The statute states that all employment applications must contain the following statement: "It is unlawful in Massachusetts to require or administer a lie detector test as a condition of employment or continued employment. An employer who violates this law shall be subject to criminal penalties and civil liability." G.L. c. 149, § 19B(2)(b).

The statute, however, creates an exception for lie detector tests administered to an employee by law enforcement authorities as permitted in criminal investigations. Under this exception, if an employee is asked by authorities to take a lie detector test for suspected criminal conduct and the employee refuses, the employer may then request that the employee take the test under the threat of losing his or her job. Moreover, the employer may terminate the employee if he or she fails the test. *Bellin v. Kelley*, 435 Mass. 261 (2001); *Baker v. City of Lawrence*, 379 Mass. 322 (1979).

A federal statute, 29 U.S.C. § 2002, provides even broader prohibitions on the use of lie detector tests by employers, although the statute exempts government employers from the prohibition.

§ 17.5.3 Physical Searches

Most of the cases dealing with challenges to the lawfulness of physical searches of employee work areas, such as desks and file cabinets, have arisen in the context of public employment and therefore involve state or federal constitutional prohibitions against "unreasonable" searches and seizures. In these cases, the courts have used the test balancing an employer's legitimate business interest against the seriousness of the intrusion into an employee's privacy. Generally, the search of a public employee's office will be justified if there are reasonable grounds for suspecting that the search will reveal evidence that the employee engaged in work-related misconduct, or unlawful conduct while at work, or if the search is necessary for a noninvestigatory work-related purpose. *O'Connor v. Ortega*, 480 U.S. 709 (1987), *aff'd*, 146 F.3d 1149 (9th Cir. 1998).

There are no statutes and little case law dealing expressly with physical searches in the private employment context. The lawfulness of searches of the offices of private employees would be evaluated under the general privacy statute and the

applicable balancing test. A search warrant would, of course, make a search lawful. Less protection should arguably be afforded to the employee's privacy interests in work areas of private employers than to those in the public employment context, because there are stronger constraints against intrusions by the state in the public employer context.

Courts are likely to scrutinize more closely searches of property that is related to, but outside, the immediate work environment, such as a motel room rented by the employer for the employee. *Sowards v. Norbar, Inc.*, 605 N.E.2d 468 (Ohio Ct. App. 1992). Searches of the employee's personal property implicate strong privacy interests, which would weigh heavily in favor of the employee under the balancing test. However, if the employer shows a compelling need for the information or provides the employee with notice that such searches are conducted in the ordinary course of business, the balance may swing in favor of the employer. As in many cases, a well-designed policy, included in a workplace handbook, can help the employer provide notice to employees of the search policy and define the applicable "zone of privacy."

§ 17.6 TECHNOLOGY ISSUES

Modern technology allows employers to engage in extremely sophisticated monitoring of an employee's workplace conduct and communications. This is especially true with electronic communication—telephones, voice mail, text messaging, electronic mail systems, and the Internet. These systems may "warehouse" deleted messages, enabling employers to discover and review communications the employee believed that he or she had erased. Not surprisingly, there are many unsettled legal issues raised by the proliferation of new technology.

§ 17.6.1 Intercepting Phone and Live Conversations

General Laws c. 272, § 99 prohibits the secret interception of "oral communications" and "wire communications" and imposes substantial criminal penalties for violations of the statute. As the Supreme Judicial Court has reaffirmed, the wiretapping statute "strictly prohibits the secret electronic sound recording by a private individual of any oral communication," including one made by a public official in the course of his or her duties. *Commonwealth v. Hyde*, 434 Mass. 594, 595 (2001). There are four exceptions to this prohibition that are relevant in the employment context.

First, an interception is not prohibited if the

- intercepting equipment is furnished to the employer by "a communications common carrier"; and
- equipment is used in the "ordinary course of business."

The "ordinary course of business" element is generally construed to require the employer to demonstrate a legitimate business purpose justifying the interception. Intercepting the personal phone calls of employees, for example, almost never can be justified except to the extent necessary to determine that the calls are, in fact, personal. The equipment element is explained in more detail below.

The second exception permits the interception of communications if the interception is done by a law enforcement officer who has been given authority by one party to the conversation to intercept it, and who is investigating one of the offenses enumerated in the statute.

The third exception allows for an interception where all the parties to the conversation have consented to it.

Finally, an interception is permitted in connection with the use of an office intercommunication system in the ordinary course of business.

The Supreme Judicial Court has stated that "the general rule is that monitoring business calls is legal, but eavesdropping on private calls is illegal unless there 'is a legitimate business purpose' for the employer to monitor an employee's conversation." *O'Sullivan v. Nynex Corp.*, 426 Mass. 261, 266 (1997). In a footnote in *O'Sullivan*, the Supreme Judicial Court opined that "employers may record private conversations of employees when they suspect that an employee is using the telephone in an unauthorized manner, or engaged in defrauding the employer." *O'Sullivan v. Nynex Corp.*, 426 Mass. at 266 (citing *Deal v. Spears*, 980 F.2d 1153, 1158 (8th Cir. 1992)). Therefore, an employer "may monitor by extension phone an employee's business-related calls as long as the employer offers a legitimate business reason that justifies such monitoring." *O'Sullivan v. Nynex Corp.*, 426 Mass. at 266.

Employers should be cautious, however, and ensure that the proffered legitimate business reason is tailored to the nature of the intrusion, because monitoring may not be within the boundaries of the ordinary course of business if the employer's suspicions do not justify the scope and intensity of the intrusion. *O'Sullivan v. Nynex Corp.*, 426 Mass. at 266.

The Supreme Judicial Court has also cited with approval *James v. Newspaper Agency Corp.*, 591 F.2d 579, 581 (10th Cir. 1979), which involved an employer

who had a telephone company install a monitoring and recording device on the business line so that a manager could monitor business calls made by employees to obtain information about abusive language from customers directed at employees. In *James*, however, the court noted that the employees making the calls were aware that their calls were monitored. *James v. Newspaper Agency Corp.*, 591 F.2d at 581. Their knowledge and lack of objection can be taken as implied consent to such monitoring.

The telephone equipment clause, on its face, applies only to equipment furnished by communications common carriers. An Appeals Court decision allowed the Massachusetts Bay Transportation Authority (MBTA), in a very limited circumstance, to record conversations on almost all telephone lines that are connected to its major operational centers. *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 310 (2000). The court noted specifically that the MBTA's policy of recording telephone calls was intended to improve efficiency, ensure public safety, and oversee employee compliance with applicable law such as providing a record of procedures followed during emergencies, aiding accident investigations, and preserving records of, reports of, and responses to problems with equipment and facilities.

In *Dillon*, MBTA employees sued the MBTA for violation of the wiretapping statute and argued that the telephone equipment exception did not apply because the equipment used by the MBTA had not been supplied by a communications common carrier. The Appeals Court held that the equipment used by the MBTA was the functional equivalent of equipment supplied by a communications common carrier, noting that telephone equipment, as it is generally understood, has become available from many vendors other than telephone companies themselves following deregulation of the industry. *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. at 314–16. The Appeals Court departed from the express wording of the statute, but did so cautiously and emphasized the unique circumstances of the case. *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. at 315–16. The court specifically noted that the MBTA devices were "commercially designed, were purchased by the defendant for routine business, were directly integrated into phone lines on which they depended in order to function, and recorded conversations for possible future listening." *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. at 317.

The federal Wiretap Act, 18 U.S.C. §§ 2510–2522, contains similar provisions. Under the federal law, however, only one party to the conversation is required to consent to the interception to make it legal.

Congress has authorized a civil action for the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §§ 2510, 2520. The third-party claimant

can seek equitable relief, compensatory and punitive damages, and reasonable litigation costs. If the claimant has suffered no actual damages, the court may award minimum statutory damages—the greater of $10,000 or $100 per day of the violation. 18 U.S.C. § 2520(c)(2)(B). Courts are split on whether the judge has discretion to deny this "minimum" statutory amount, with the majority holding that the minimum amount may be denied. *See DirecTV, Inc. v. Griffin*, 290 F. Supp. 2d 1340, 1347 (M.D. Fla. 2003).

Massachusetts has authorized a similar private cause of action for the interception of "contents of any wire or oral communication through the use of any intercepting device." G.L. c. 272, § 99(B), (Q). This private cause of action is not preempted by the federal statute. Russell G. Donaldson, Annotation, *Construction and Application of State Statutes Authorizing Civil Cause of Action by Person whose Wire or Oral Communication is Intercepted, Disclosed, or Used in Violation of Statutes*, 33 A.L.R. 4th 506 n.l (1993–2005). Again, the third-party claimant can seek compensatory damages, punitive damages, and reasonable attorney fees. If he or she suffered no actual damages, he or she is entitled to the greater of $100 per day for each day of the violation or $1,000. G.L. c. 272, § 99(Q)(1). Finally, the third-party claimant is unlikely to obtain punitive damages as they are generally disfavored, require a showing of actual harm, *see Pine v. Rust*, 404 Mass. 411, 415–16 (1989), and likely require a showing of wanton, reckless, or malicious intent. The federal statute applies such a malice standard. The Massachusetts statute was modeled on the federal statute, and both are generally read in accordance with the construction given by federal courts to the federal statute. *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 314 (2000).

The applicable federal statute of limitations is two years, which starts to run when the third party has had a reasonable opportunity to discover the violation. If he or she was prevented from discovering the violation, the statute of limitations is tolled. Kristine C. Karnezis, Annotation, "Construction and Application of Provision of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. § 2520) Authorizing Civil Course of Action by Person Whose Wire, Oral or Electronic Communications is Intercepted, Disclosed, or Used In Violation of Act," 164 *A.L.R. Fed.* 139 (2000–2005). In Massachusetts, tort actions are generally barred after three years. G.L. c. 260, § 2A. If the cause of action is fraudulently concealed, the statute of limitations tolls. G.L. c. 260, § 12.

§ 17.6.2 Monitoring E-mail, Instant Messages, Voice Mail, Text Messages, and Computer Files

Congress has enacted the Electronic Communications Privacy Act (ECPA). ECPA includes Title I, which amended the federal Wiretap Act, codified at 18 U.S.C. §§ 2510–2522; and Title II, also known as the Stored Communications

Act (SCA), codified at 18 U.S.C. §§ 2701–11. The amended Wiretap Act prohibits "interception" of oral, wire, or electronic communications. The SCA prohibits "unauthorized access" to stored wire or electronic communications. The ECPA provides for civil and criminal penalties, as well as a private cause of action. The ECPA reaches beyond common carriers to include private communication systems operated or subscribed to by major companies.

Employers monitoring employee e-mail usage are governed by the SCA or the Wiretap Act, depending on the point in time at which the e-mail is intercepted or accessed. Section 2511 of the Wiretap Act governs the unlawful interception of communications and has been interpreted to mean that an e-mail message must be in transit to be intercepted. *See United States v. Simons*, 29 F. Supp. 2d 324, 329–30 (E.D. Va. 1998), *aff'd in relevant part*, 206 F.3d 392 (4th Cir. 2000) (government agents did not violate the ECPA provisions regarding interception of electronic communications where they copied the defendant's e-mail messages that were in storage). The distinction between transit and storage, however, is not a bright line. The First Circuit has criticized such thinking, holding that e-mail in temporary, transient storage during the transmission process can be considered to be in transit for purposes of the Wiretap Act. *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005); *see also Blumofe v. Pharmatrak, Inc.* (*In re Pharmatrak Privacy Litig.*), 329 F.3d 9, 21 (1st Cir. 2003) (criticizing the storage-transit dichotomy as "less than apt to address current problems" that are raised by applying the ECPA to new technologies such as e-mail). Thus, if the employer intercepts e-mail messages before they are made available to their intended recipient, the Wiretap Act applies. In other cases, where the e-mail already is available for the recipient and is in some form of storage, the SCA applies.

If the e-mail is not yet available for the recipient when it is intercepted, the Wiretap Act applies, and the employer's actions must fall under one of two exceptions to be permissible. The provider of electronic communication services may lawfully intercept electronic communications "while engaged in any activity which is a necessary incident to the rendition of his service" or to protect the provider's rights or property (the "service provider exception"), 18 U.S.C. § 2511(2)(a)(i); and interceptions may be made when the employee has given implied or express consent (the "consent exception"), 18 U.S.C. § 2511(2)(c). If, instead, the e-mail already has been delivered and is in storage, then the SCA applies. In these cases, an employer accessing stored e-mail on the employer's network is exempted under the SCA's similar service provider exception. 18 U.S.C. 2701(c).

Under the service provider exceptions, employers may monitor their own proprietary e-mail systems, either during transmission or postdelivery storage, without violating the Wiretap Act or the SCA. It is unclear whether employees

using Webmail accounts (such as Yahoo or Hotmail) through the employer's computer network could be monitored using this exception. *See* Kevin W. Chapman, Comment, "I Spy Something Read! Employer Monitoring of Personal Employee Webmail Accounts," 5 *N.C.J.L. & Tech.* 121 (2003).

In a rare case where an employee's claim was allowed to proceed under the SCA, the employer had accessed the employee's password-protected Web site, which was hosted by a different service provider. Thus, the service provider exception of the SCA was not available to the employer. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

Employers may require employees to give written consent to monitoring so that the consent exception of the Wiretap Act will apply. Consent under the ECPA also includes implied consent, which may be achieved by the employer's prior notice to its employees that it will monitor its employees' communications. However, implied consent is not constructive consent. *Griggs-Ryan v. Smith*, 904 F.2d 112, 116–17 (1st Cir. 1990). Consent will not be judged by what a reasonable employee should have realized or should have known, but only by what reasonable notice an employee actually had. Additionally, at least one court has held that consent will not be implied where the employer notified the employees that it "might" monitor employee electronic communications, without advising employees that it was actually doing so. *See Deal v. Spears*, 980 F.2d 1153, 1157 (8th Cir. 1992). The First Circuit has refused to construe implied consent broadly. *Blumofe v. Pharmatrak, Inc. (In re Pharmatrak Privacy Litig.)*, 329 F.3d 9 (1st Cir. 2003).

The Massachusetts wiretap statute also applies to e-mail interceptions, and contains a similar service provider exception, allowing interceptions on the employer's own system made in the ordinary course of business using equipment furnished by a common carrier. G.L. c. 272, § 99. See § 17.6.1, above. The state wiretap statute is interpreted in accordance with the federal Wiretap Act. See § 17.6.1.

In *Restuccia v. Burk Technology, Inc.*, No. 95-2125, 1996 Mass. Super. LEXIS 367, the employer terminated employees for excessive use of e-mail for personal purposes. (An employee's forwarding of obscene messages raises a host of legal questions, including the potential for harassment claims. These issues, although important, are beyond the scope of this chapter.) The plaintiffs in *Restuccia* brought a claim under the state wiretap statute. The court decided in favor of the employer, holding that the interception of e-mail messages by the computer's automatic systems was within the employer's "ordinary course of business," and thus did not violate the statute.

In *Garrity v. John Hancock Mutual Life Insurance Co.*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002), the court found for the employer on both a state wiretap claim and an invasion of privacy claim. The messages were accessed from storage, so the Massachusetts wiretap statute did not apply, based on the same storage-transit dichotomy used under the federal Wiretap Act. The court found that the employee did not have a reasonable expectation of privacy in e-mail on the employer's system, despite the use of personal passwords and e-mail folders, so there was no actionable invasion of privacy.

Employee use of employer-owned devices for sending instant messages and text messages is a developing area of the law. An important distinction between instant and text messages and e-mail is that instant and text messages are not stored like e-mail messages. Thus, employer monitoring likely falls under the Wiretap Act and not the SCA. *See* Ira David, Note, "Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?," 5 *Nev. L.J.* 319 (2004). This lack of storage capability is a consideration for employers who need records of their employees' communications. Employers should consider whether instant messaging should be allowed on their computer networks at all, given this issue. In *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), the Supreme Court held that the city's review of employees' text messages sent on city-owned devices did not constitute an unreasonable search or violate the Fourth Amendment.

Voice mail falls under the SCA. *See United States v. Councilman*, 418 F.3d 67, 78–79 (1st Cir. 2005) (dicta). Other computer files on the employer's system fall under the SCA as long as they are kept in storage of some kind.

Many businesses claim the right to monitor e-mail, voice mail, and other electronic resources regularly, typically to make sure that the systems are being used for business purposes. Computer files in the employer's computer may well be the employer's "property." At a minimum, they should be accessible to the employer for legitimate business purposes. If the employer wishes to take this approach, it should adopt a policy to that effect and distribute it to all employees. Employers also should consider that enforcement of a "business-use only" policy regarding electronic communications systems may infringe on concerted activity that is protected under Section 7 of the National Labor Relations Act in some situations. 29 U.S.C. § 157. Further, several cases have addressed the question of whether employees who communicate with their attorneys using their employers' electronic systems have waived the attorney-client privilege with regard to such communications. *See, e.g.*, *National Economic Research Associates, Inc. v. Evans*, No. 04-2618-BLS2, 2006 Mass. Super. LEXIS 371 (Mass. Super. Ct. 2006); *Curto v. Medical World Communications, Inc.*,

No. 03CV6327, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. 2006). These issues, however, are beyond the scope of this chapter.

§ 17.6.3 Photography and Video Surveillance

There are no state or federal statutes specifically governing the use of still or video cameras to monitor the conduct of employees. (In one of the ironies in this developing area of the law, however, video surveillance with sound is regulated by the statutes prohibiting the interception of oral communications.) Employee challenges to the use of such cameras are therefore made under the general privacy law and the applicable balancing test, weighing the employer's legitimate business interest in the use of the surveillance equipment against the reasonable privacy interest of the employees. Courts that have addressed this issue have noted the importance of tailoring the scope of the surveillance to the precise business interest asserted. As the First Circuit stated in *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174, 180 (1st Cir. 1997), "[t]he precise extent of an employee's expectation of privacy often turns on the nature of an intended intrusion." In *Vega-Rodriguez*, the First Circuit held that even employees of a quasi-public company subject to the strictures of the Fourth Amendment had no reasonable expectation of privacy against disclosed, soundless video surveillance in an open work area. *Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d at 182. The Supreme Judicial Court recently held that undisclosed, silent video surveillance in an open, public work area was permissible because an employee had no objectively reasonable expectation of privacy under such circumstances. *Nelson v. Salem State College*, 446 Mass. 525, 534–36 (2006). *See also Acosta v. Scott Labor, LLC*, 377 F. Supp. 2d 647 (N.D. Ill. 2005).

A Massachusetts statute prohibits secret electronic, photo, or video surveillance of nude or partially nude people and provides for criminal penalties. G.L. c. 272, § 104 (added by 2004 Mass. Acts c. 395, § 6). The statute excludes certain limited categories of surveillance from its coverage, such as a merchant's surveillance of a customer changing room where conspicuous notice is given. It does not, however, exclude employer surveillance of areas in which employees can be expected to change clothing. Thus, employers should not place cameras in areas where employees may reasonably be expected to undress.

§ 17.7 CONCLUSION

Employee privacy is a developing area of law, and the law will respond, as our society does, to the new realities of the workplace. The latest challenge for Massachusetts employers in this area of the law will be compliance with the new data security laws. Massachusetts has a policy of protecting employee privacy

by requiring a fact-intensive inquiry into the scope of the intrusion and the business justification underpinning the employer's practice. As with many issues in the workplace, open and active communications between employers and employees, from well-prepared application procedures to a carefully written workplace handbook, can help establish the reasonable expectations of behavior for employees and employers.

Chapter 17, Part II

PRIVACY IN THE WORKPLACE: AN EMPLOYEE PERSPECTIVE*

LAWRENCE J. CASEY, ESQ.
CLAIRE NEWTON, ESQ.
Shilepsky Hartley Robb Casey Michon LLP, Boston

§ 17.8 THE EMPLOYEE'S PERSPECTIVE

An invasion of privacy under G.L. c. 214, § 1B, is actionable only where the violation is both unreasonable and substantial or serious. *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. 367, 382 (2005); *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 409 Mass. 514, 517 (1991). In the employment context, the courts have focused on the seriousness of the intrusion, the employer's legitimate need for the private information for demonstrable and proper business purposes, and the legitimate public interest. "When the subject matter of the publicity is of public concern . . . there is no invasion of privacy." *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. at 382 (citations omitted).

What constitutes demonstrable and proper business purposes will depend upon the facts. For example, a high-level employee or one who has access to sensitive or confidential information should reasonably be expected to disclose more private information than a low-level employee who does not have access to confidential information. The analysis centers on the need for the information in determining or assessing the employee's efficacy in his or her work.

Under the statute, private facts are not simply facts that are not public; they must also be facts of a highly personal or intimate nature. *French v. United Parcel Serv., Inc.*, 2 F. Supp. 2d 128, 131 (D. Mass. 1998). Intimate facts about a plaintiff's personal life may not be considered private if the employee discloses those facts to coworkers, even to a small circle of coworkers who are also close personal friends. Simply put, an employee who disseminates private information to coworkers in the workplace may relinquish a claim of privacy in that information under the statute. In addition, at least one Massachusetts Superior Court

* Updated for the 2013 Supplement by Claire Newton, Esq.

judge has ruled that an employee who is the subject of a legitimate workplace investigation and who discloses private facts to defend against allegations of wrongdoing may not bring a claim against the employer for an invasion of privacy. *Williams v. Brigham & Women's Hosp., Inc.*, 2002 Mass. Super. LEXIS 52 (Mass. Super. Ct. 2002). In *Williams*, the plaintiff was the subject of a criminal workplace investigation and was forced to reveal that she had an abortion to prove her whereabouts on the date in issue. The court in *Williams* ruled that the employer could not have been expected to know that her alibi would reveal private information. Since the investigation was reasonable and justified, the court concluded that the conduct did not violate G.L. c. 214, § 1B.

Disclosures about an employee's professional conduct that are not of an exceedingly personal or intimate nature do not automatically equate to an invasion of privacy, pursuant to G.L. c. 214, § 1B. *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. 367, 383–84 (2005). In *Ayash*, the plaintiff/employee was identified by the *Boston Globe* as a physician under investigation by Dana-Farber following the deaths of two patients who had been receiving chemotherapy. The *Globe* ultimately published nearly fifty articles on the subject, including materials based on confidential "peer-review committee" proceedings, which a jury could have found were leaked to the *Globe* by Dana-Farber. *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. at 375 n.12, 383–84.

While the Supreme Judicial Court noted that the disclosures were both "exceedingly distressing" and "embarrassing" to Ayash, the court entered summary judgment in favor of Dana-Farber on the invasion of privacy claim because the disclosures were a matter of intense public interest and were not exceedingly personal or intimate in nature. *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. at 383–85.

> This is a case where the plaintiff (unwillingly) achieved public figure status by reason of her status as chair and principal investigator of an experimental research protocol under which two patients at a prominent research institution received chemotherapy overdoses. . . . Accordingly, any dissemination of information regarding the plaintiff in connection with the overdoses, including documents which, under normal circumstances, would not be open to public inspection, only provided further publicity on a matter that was already squarely in the public eye.

Ayash v. Dana-Farber Cancer Inst., 443 Mass. at 384 (citations omitted).

Public-sector employees relinquish certain privacy rights by virtue of the public nature of their employment. The names, home addresses, payroll information, and disability pay of public-sector employees are generally not protected by G.L. c. 214, § 1B, as it has been determined that the public interest in the information outweighs the employee's right to privacy, and as a result, employers have been compelled to release this type of information. *Cape Cod Times v. Sheriff of Barnstable County*, 443 Mass. 587, 594–95 (2005); *Pottle v. Sch. Comm. of Braintree*, 395 Mass. 861, 863 (1985).

§ 17.8.1 Disclosure of Medical Facts

The courts apply the same balancing test—the legitimacy of the employer's interest in obtaining and disclosing the information against the substantiality of the intrusion on the employee's privacy—when medical information about an employee is disclosed by an employer. However, the balancing test is slightly modified where the disclosure is made by a physician employed by the employer. In those instances the court considers the degree of intrusion on privacy and the public interest in preserving the confidentiality of a physician-patient relationship balanced against the employer's need for the medical information. *Bratt v. Int'l Bus. Machs. Corp.*, 392 Mass. 508, 523 (1984).

§ 17.8.2 Disclosure of Facts Relating to Termination

An employer is not permitted to disclose private facts regarding a termination decision unless, on balance, the employer's need to disclose or the public interest in disclosure outweighs the privacy interest at stake. The balancing test applies to both existing and former employees.

The Supreme Judicial Court has refused to adopt the doctrine of "compelled self-publication defamation." *White v. Blue Cross & Blue Shield of Mass.*, 442 Mass. 64 (2004). In that case, Blue Cross and Blue Shield terminated White because he had allegedly disclosed the details of a confidential financial settlement. White denied knowing of the settlement and sued Blue Cross for defamation because he was "compelled" to disclose to prospective employers the reason for his discharge, which Blue Cross knew or should have known was false. *White v. Blue Cross & Blue Shield of Mass.*, 442 Mass. at 65–68. In denying relief to White, the court noted that the doctrine is "troubling conceptually," constitutes a "dramatic departure from the principles governing employment at will," and has the "potential to stifle communication in the workplace." *White v. Blue Cross & Blue Shield of Mass.*, 442 Mass. at 68–70.

§ 17.8.3 Drug Testing

The Massachusetts courts have recognized that drug testing can involve a significant invasion of privacy. See *Folmsbee v. Tech Tool Grinding & Supply, Inc.*, 417 Mass. 388 (1994), and cases cited therein. As a result, employees may be entitled to the least intrusive feasible testing methods available and to testing procedures that guarantee privacy and ensure accuracy. Drug testing that targets a single employee may pose more problems for an employer than testing that is applied universally. *Webster v. Motorola, Inc.*, 418 Mass. 425 (1994).

§ 17.8.4 Personnel Records

The Massachusetts legislature enacted sweeping revisions to the personnel records statute, G.L. c. 149, § 52C, in 2010. The amended statute requires employers to notify an employee within ten days of the employer placing in the employee's personnel record "any information to the extent the information is, has been used or may be used, to negatively affect the employee's qualification for employment, promotion, transfer, additional compensation or the possibility that the employee will be subject to disciplinary action." The amended statute also broadens the definition of "personnel record" to include documents that may not be maintained by an employer's typical personnel file. The statute defines a "personnel record" as

> a record kept by an employer that identifies an employee, to the extent that the record is used or has been used, or may affect or be used relative to that employee's qualifications for employment, promotion, transfer, additional compensation or disciplinary action. A personnel record shall include a record in the possession of a person, corporation, partnership or other association that has a contractual agreement with the employer to keep or supply a personnel record as provided in this section. A personnel record shall not include information of a personal nature about a person other than the employee if disclosure of the information would constitute a clearly unwarranted invasion of such other person's privacy. Without limiting the applicability or generality of the foregoing, all of the following written information or documents to the extent prepared by an employer of twenty or more employees regarding an employee shall be included in the personnel record for that employee: the name, address, date of birth, job title and

> description; rate of pay and any other compensation paid to the employee; starting date of employment; the job application of the employee; resumes or other forms of employment inquiry submitted to the employer in response to his advertisement by the employee; all employee performance evaluations, including but not limited to, employee evaluation documents; written warnings of substandard performance; lists of probationary periods; waivers signed by the employee; copies of dated termination notices; any other documents relating to disciplinary action regarding the employee. A personnel record shall be maintained in typewritten or printed form or may be handwritten in indelible ink.

G.L. c. 149, § 52C.

An employer must provide an employee with the opportunity to review his or her personnel record within five days of receiving a written request. An employee is authorized to review his or her personnel record twice per year. However, a review requested after the employee is notified that negative information has been placed in the employee's personnel record does not count against the employee's two statutorily permitted reviews. The statute also requires employers with twenty or more employees to maintain employees' personnel records for three years after the employees' date of termination.

The amended statute became effective August 1, 2010. The attorney general is authorized to enforce the statute and may impose fines between $500 and $2,500 for each violation. Note, however, that the Massachusetts Appeals Court previously held that employees did not have a claim for damages under the statute. Rather, their only remedy was "the opportunity to comment, correct or expunge incorrect or false information contained in personnel files that pertain to them." *Kessler v. Cambridge Health Alliance*, 62 Mass. App. Ct. 589, 597 (2004). Implicit in that remedy is the right to seek judicial review of documents to determine whether they constitute "personnel records" under the statute and therefore must be physically included in the personnel file. *Kessler v. Cambridge Health Alliance*, 62 Mass. App. Ct. at 597.

For public employees, G.L. c. 4, § 7, cl. 26(c) exempts from disclosure under the public records statute, personnel files, and "other materials . . . the disclosure of which may constitute an unwarranted invasion of personal privacy."

In *Wakefield Teachers Association v. School Committee of Wakefield*, 431 Mass. 792 (2000), the Supreme Judicial Court held that a disciplinary report concerning

the performance of a teacher is "personnel" information under G.L. c. 4, § 7 and therefore exempt from disclosure. In so holding, the court stated that what constitutes a personnel file or information may require a case-by-case determination but includes, "at a minimum, employment applications, employee work evaluations, disciplinary documentation, and promotion, demotion, or termination information pertaining to a particular employee." *Wakefield Teachers Ass'n v. Sch. Comm. of Wakefield*, 431 Mass. at 798.

In *Worcester Telegram & Gazette Corp. v. Chief of Police of Worcester*, 436 Mass. 378 (2002), the court declined to apply a "blanket exemption" to prevent disclosure of records relating to an internal affairs investigation, concluding that the records must be reviewed by the trial court to determine whether they are of the "nature or character" of a personnel record.

In *Boston v. Labor Relations Committee*, 61 Mass. App. Ct. 397 (2004), the Appeals Court addressed a labor union's access to information pertaining to a nonunion supervisor who was the subject of a grievance. The city retained a management consultant to aid the manager in dealing with the union employees. *Boston v. Labor Relations Comm.*, 61 Mass. App. Ct. at 398. The court denied the union's request to review the consultant's report. While the union was able to prove that the report was relevant and reasonably necessary to prosecute the union's grievance, the court held that the city was not required to turn over such information if there is a great likelihood that harm would flow from such disclosure. *Boston v. Labor Relations Comm.*, 61 Mass. App. Ct. at 399–401. Examples of such harm include invading the manager's privacy interest, undermining the manager's authority, and discouraging employers from providing staff members with opportunities aimed at improving their personal skills and management style. *Boston v. Labor Relations Comm.*, 61 Mass. App. Ct. at 402–03.

§ 17.8.5 Criminal Records

The Massachusetts Criminal Offenders Record Information Act (CORI), G.L. c. 6, §§ 167–178B, places strict limits on the information most employers may obtain concerning an existing or prospective employee. Any employer who obtains criminal offender information in violation of Section 172 may not collect, store, disseminate, or use the information in any manner for any purpose. The nature of the information available to an employer under Section 172 will depend on the nature of the employment. Law enforcement agencies, elder and disabled services agencies, IV-D Agencies, and long-term care facilities are but a few examples of employers that are entitled to enhanced information under Section 172.

Effective November 4, 2010, the CORI reform law prohibits employers covered by G.L. c. 151B from seeking disclosure of a job applicant's criminal record

information on an "initial written application form." The Massachusetts Commission Against Discrimination has issued guidelines under the new law. Other amendments to the CORI reform law are effective in May 2012. *See* 2010 Mass. Acts c. 256.

§ 17.8.6 Intercepting Mail

An employee does not relinquish his or her right to privacy in personal mail simply because it is delivered to the workplace. Whether an employer is justified in opening correspondence to determine if it is business related will depend on the facts and circumstances. Employees should take the position that absent a compelling business necessity an employer should be prohibited from opening questionable mail. Where possible the employee should be given the opportunity to sort through mail that is not clearly business related before the mail is examined. There may be circumstances wherein an employee's expectation of privacy in personal mail may be reduced. If, for example, an employee is aware that it is the business practice of the employer to open all mail, unless clearly personal, before it reaches the employee, the employer may argue that the employee has assumed the risk that personal mail will be opened. Of course, an employer who disseminates private information about an employee taken from the employee's personal mail is at risk of violating the employee's right of privacy under G.L. c. 214, § 1B.

§ 17.8.7 Lie Detector Tests

Both the state and federal lie detector test statutes (G.L. c. 149, § 19B, and 29 U.S.C. § 2002 et seq.) provide for significant civil penalties. Under the state statute, a prevailing plaintiff is entitled to minimum damages in the amount of $500.00 as well as treble damages, lost wages and benefits, costs, and attorney fees. Injunctive relief is also available under state law. The consent of an employee is not a defense under Section 19B.

Under G.L. c. 149, § 19B an employer may not request or require an employee or prospective employee to take a polygraph examination. The statute also requires that employment applications contain the statement set forth in the statute notifying prospective employees of the prohibition.

The statute contains an exemption for law enforcement and does not protect an employee where the polygraph examination is requested and administered by law enforcement as permitted in the conduct of a criminal investigation. In *Bellin v. Kelley*, 435 Mass. 261 (2001), the Supreme Judicial Court affirmed an order granting summary judgment where a plaintiff employee alleged that the defendant employer violated G.L. c. 149, § 19B(2) when it threatened to fire him

for refusing to take a polygraph examination requested by police investigating a break-in at the employer's place of business. Since the polygraph examination was both requested and to be administered by law enforcement, the court in *Bellin* held that the exception for tests conducted by law enforcement as part of a criminal investigation applied. In *Bellin*, the court declined to determine the "outer boundaries" of the exception in G.L. c. 149, § 19B(2) and thus "express[ed] no opinion as to whether a particular connection with the employee's work must be shown before the exception is applicable." *Bellin v. Kelley*, 435 Mass. at. 271.

An employee who prevails under the federal statute in a private civil action is entitled to appropriate legal and equitable relief, including but not limited to employment, reinstatement, promotion, and the payment of lost wages and benefits. The recovery of attorney fees and costs is discretionary under the federal statute. An employee may not waive rights under the federal statute other than in settlement of a claim brought as a result of a violation thereof.

§ 17.8.8 Physical Searches

The Fourth Amendment, applicable to the states through the Fourteenth Amendment, protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . . ." The Fourth Amendment applies to searches of the personal work areas and effects of public employees if there exists a reasonable expectation of privacy in the items searched. The reasonableness of a public employee's expectation of privacy will be addressed on a case-by-case basis and assessed in the context of the workplace environment. *O'Connor v. Ortega*, 480 U.S. 709 (1987). In those instances where a reasonable expectation of privacy is found to exist, the court will balance the invasion of the expectation against the government's need for supervision, control, and the efficient operation of the workplace. *O'Connor v. Ortega*, 480 U.S. 709 (1987). A warrant is generally not required unless the search is not work related.

§ 17.8.9 Technology Issues

(a) *Intercepting Telephone and Live Conversations*

The Massachusetts wiretap statute, G.L. c. 272, § 99, criminalizes the surreptitious recording of any oral or wire communications and provides for civil penalties for violations of privacy that occur as a result of an unlawful interception. The statute exempts interceptions made using equipment furnished to the employer by "a common communications carrier" if made in the ordinary course of business. Interceptions using internal office communications systems in the ordinary course of business are also exempt. In *Heffernan v. Hashampour*, No.

09-cv-2060, 26 Mass. L. Rptr. 541 (Mass. Super. Ct. Dec. 19, 2009), the Superior Court (Curran, D.) ruled that the wiretap statute applies when a party outside of Massachusetts secretly records a call to a party in Massachusetts.

An employer is permitted to monitor an employee's business related calls by extension phone if legitimate business reasons justify the intrusion. *O'Sullivan v. NYNEX Corp.*, 426 Mass. 261, 266 (1997). However, an employer's suspicions of illegal or inappropriate activity must justify the extent of the intrusion or monitoring. Eavesdropping on private calls will violate the wiretap statute in the absence of consent of all parties or a legitimate business purpose. The wiretap statute is also violated where an employer discloses, attempts to disclose, uses, or attempts to use, the contents of a wire or oral communication obtained through interception.

In *Commonwealth v. Hyde*, 434 Mass. 594 (2001), the court held that G.L. c. 272, § 99 applied to a recording a motorist made of his conversation with police officers during a routine traffic stop. In *Commonwealth v. Hanedanian*, 51 Mass. App. Ct. 64 (2001), the appeals court applied the statute to an unconsented recording made by a client of his conversations with his attorneys. Although neither of these cases arose in the employment context, they both signal a broad reading of the protections afforded by the statute.

The courts have yet to decide whether a recording made of a message left on company voice mail would violate the express provisions of the statute. These recordings are occasionally made by employees to prevent the spoliation of evidence of discrimination and by employers to preserve evidence to either refute a claim of discrimination or to impeach a plaintiff's credibility. The statute does not expressly prohibit recordings of recorded messages and does not address the extent to which a claim of privacy might be lost by one who leaves a message on another person's voice mail. An employer who makes the recording using the system supplied by the common carrier would not violate the statute, provided that the recording is made in the ordinary course of business, but the dissemination of the recording may violate the statute.

(b) *Intercepting E-Mail, Voice Mail, and Computer Files*

The monitoring of voice mail without the use of intercepting equipment is not a violation of the state wiretap statute. Intrusions into e-mail and other computer files will likely require a balancing of the employer's legitimate business interest against the degree of intrusion and the reasonableness of the employee's expectation of privacy in such files. An employee who is on notice that his or her e-mail, voice mail, and computer files are subject to inspection by an employer will not have a legitimate expectation of privacy in those files. *See City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (city's review of employees' text messages sent on city-owned devices did not constitute an unreasonable search or violate

Fourth Amendment). The burden is on the employee under the privacy statute to demonstrate that an intrusion into e-mail, voice mail, and computer files is both unreasonable and substantial or serious. Absent a legitimate business need, an employer should not disclose or disseminate information it obtains about an employee's private affairs through interception of computer, e-mail, or voice-mail files.

(c) *Social Media*

Growing numbers of employees use social media networks (e.g., Facebook and Twitter) both at work and at home to discuss their employment. Increasingly, employers are monitoring social media networks and, in some circumstances, taking disciplinary action against employees for such postings. To date, employee privacy rights on social networks have not been clearly defined by the Massachusetts courts or the legislature. Several recent decisions from the National Labor Relations Board (NLRB) suggest that posting on social media may constitute "concerted activity" and may be protected under the National Labor Relations Act (NLRA) if the postings address the terms and conditions of the employee's employment, including his or her wages, hours, or working conditions. *See Triple Play Sports Bar*, Case No. 34-CA-12915 (ALJ, Jan. 3, 2012) (employer violated NRLA by terminating employees who complained about employer's method of withholding taxes on Facebook); *Hispanics United of Buffalo*, Case No. 3-CA-27872 (ALJ, Sept. 2, 2011) (violation of NRLA to terminate employees for complaining about their jobs and/or manager on Facebook). Employees should be aware, however, that the disclosure of confidential employer information, including trade secrets, will not likely be afforded the same protection under the NLRA. *See* "Office of General Counsel, Division of Operations-Management," Memorandum OM 12-59 (May 30, 2012) (advising in sample social media policy that employees must "[m]aintain the confidentiality of [employer] trade secrets and private and confidential information").

§ 17.9 CONCLUSION

Employees must recognize that the right to privacy in the workplace is a limited one. Employment policies pertaining to the privacy of voice mail, e-mail, computer file information, and social media use should be read with care. There are many circumstances where an employer's legitimate need to obtain or disseminate information will prevail over an employee's desire to keep certain information private. As a result, a violation of privacy alone will not necessarily sustain a cause of action. The nature of the intrusion, the legitimacy of the employer's business purpose, and the reasonableness of the employee's expectation of privacy must all be considered in reaching a determination whether, under state or federal statutes or common law, an actionable invasion of privacy has occurred.

EXHIBIT 17A—Certain Definitions from G.L. c. 272, § 99

As used in this section

1. The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.

2. The term "oral communication" means speech, except such speech as is transmitted over the public air waves by radio or other similar device.

3. The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.

4. The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein.

5. The term "contents", when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.

EXHIBIT 17B—Example Electronic Systems Policy*

ELECTRONIC SYSTEMS

Personal Use

Network, Internet, phonemail and any other electronic systems provided to employees by [Company] are for Company business use only. These electronic communications systems and any mail messages transmitted on them are the property of the Company. As such, use of these systems for personal purposes is strongly discouraged. Any personal use of the Company's electronic systems should be kept to a minimum and must not interfere with any Company work. Employees who are found to violate this rule regarding personal use of electronic systems will be subject to disciplinary action, up to and including termination.

No Privacy Right

Use of the Company's electronic systems constitutes an acknowledgment by each employee that he or she does not have a personal right of confidentiality or privacy in anything that he or she places or receives on these systems, and such use constitutes an express waiver of any right to confidentiality or privacy in the systems.

The Company has the ability to monitor employees' usage of the Company's electronic systems, including Internet access, and will do so as necessary. If non-business usage of the Internet is deemed to be excessive, an employee will be subjected to disciplinary action, up to and including termination. This disciplinary action may include terminating the employee's access to the Internet on a temporary or permanent basis.

Network And Internet Use

The Company Network is a business network belonging to the Company. It is not a private place to create, send or keep emails, documents or other files that are personal or otherwise inappropriate for a business computer network. Accordingly, please note that:

Anything on the Company Network can be monitored and viewed by authorized members of the Company's staff or Company consultants, as and when required. Such access may occur without prior notice and at any time, consistent with the policies and needs of the Company, and/or as otherwise determined by the Man-

*

agement. This includes accessing documents, internal e-mails and other files located on the Company Network or anything that travels via the Internet, in order to perform maintenance or other work on the systems or for other reasons determined in the Company's sole discretion.

Employees should refrain from communicating threats, vulgarities, obscenities, sarcasm or other improper language in electronic mail or voice-mail messages. The communication of threats or use of foul or abusive language may be grounds for disciplinary action, up to and including termination.

Furthermore, except as is otherwise required in order to conduct business, the Company Network, including but not limited to the Internet feature, is not to be used to access, view, download, send, copy, print or in any way communicate or see harassing or otherwise offensive material or messages, documents or files that include intimidating, hostile, or offensive material on the basis of race, color, religion, national origin, sex, age, disability, family status or sexual orientation.

Electronic Mail

The Company Network is a business network. Consistent with this fact, the Company's electronic mail addresses are intended for business use only. In addition, so as to avoid an inappropriately high volume of email that could degrade the Network's performance, discretion should be used with respect to subscriptions to listservs, newsgroups, and other mail delivery services of the Internet. No one should ever subscribe to any such service that is not clearly reputable without first determining how to un-subscribe. It is also highly advisable that employees make every attempt to prevent the services from sharing their email addresses with third parties.

Furthermore, chain email letters and the use of Company email addresses to subscribe to or send electronic greeting cards are not part of the business of the Company. Such uses can degrade the Network's performance and, as such, are expressly prohibited.

Employees are also prohibited from sending mass internal emails for personal reasons, such as, for example, to solicit money or volunteers for private causes, to sell items, or to seek referrals for private services. The Company provides email bulletin boards that employees are required to use for these reasons.

Installation of Programs

The introduction of any program or other executables to the Company Network is expressly prohibited without specific permission from the IT Department. This includes downloading of program files or other executables from the Inter-

net, floppy disk, CD-ROM, or other access. Materially adverse consequences, including a complete disruption of service or virus infection, can ensue if files are introduced to the Network by anyone other than the IT staff. The IT staff will work with employees who need such files for business purposes. Any questions regarding the need for such files should be directed in the first instance to the IT Department.