EMPLOYEES' RIGHT TO PRIVACY IN THE WORKPLACE

Sharen Litwin, Esq.
Kotin, Crabtree and Strong, LLP, Boston [1]

Massachusetts Continuing Legal Education
December, 2006

I. INTRODUCTION

The primary source of private sector employees' right to privacy in Massachusetts is the Massachusetts Right of Privacy Act, G.L. 214 §1B (the "Privacy Act" or "Massachusetts Privacy Act"). The Privacy Act provides that:

> A person shall have a right against unreasonable, substantial or serious interference with his privacy. G.L. 214 §1B.

The Privacy Act does not specifically reference the workplace, but has been interpreted by Massachusetts courts to apply to a wide range of workplace issues. Massachusetts courts have used a balancing test when interpreting the Privacy Act where the employer's legitimate business interests are balanced against the employee's reasonable expectation of privacy. *See Bratt v. International Business Machines Corp.*, 392 Mass. 508, 520-521 (1984).

Employees in the public sector have also brought claims for invasion of privacy under the Fourth Amendment to the United States Constitution pursuant to 42 U.S.C. §1983.

This article will address three selected topics in the area of employees' right to privacy: use of e-mail and the Internet in the workplace, drug testing and video surveillance.

II. EMPLOYEES' RIGHT TO PRIVACY IN THEIR USE OF E-MAIL AND THE INTERNET IN THE WORKPLACE

A. Massachusetts Cases Under the Privacy Act

The issue of employees' right to be protected against the invasion of their privacy has come to center stage with the widespread use of the Internet and e-mail in the workplace. Most employees who file claims for invasion of privacy under the Massachusetts Privacy Act, or under similar privacy statutes or

---

[1] I want to thank Amy C. Mainelli Burke of Kotin, Crabtree and Strong, LLP for her valuable contribution to the preparation of this article.

common law in other states, in connection with their use of e-mail and the Internet in the workplace do not prevail. This is especially true when the employer has policies in place notifying its employees that the computer systems belong to the employer and that the employer has the right to monitor its employees' use of the Internet and transmission of e-mails on the employer's computer system. Even when an employer does not have specific computer use policies, the employer often still prevails on its employees' invasion of privacy claims. The courts in Massachusetts and elsewhere balance the employer's legitimate business interests against the employee's reasonable expectation of privacy under the privacy statutes and usually find that the employee did not have a reasonable expectation of privacy. [2]

Since the widespread use of the Internet and e-mail in the workplace is relatively recent, there has not been an abundance of caselaw under the Massachusetts Privacy Act relating to employees' use of e-mail or the Internet.

In *Restuccia v. Burk Technology, Inc*., 1996 WL 1329386 (Mass. Super. 1996), the employer had an e-mail system where each employee had a password that they were instructed to change periodically to ensure confidentiality. There was no company policy against using e-mail for personal messages. There was only a policy against excessive "chatting." Supervisors were able to access employees' computer files by using supervisory passwords. The company's e-mail system stored everything on back up files that management could access. Employees, however, were not informed that all e-mail on the company system was saved or that their supervisors had access to all stored e-mail.

After the president of the company was informed by a manager that plaintiff Neil S. LoRe ("LoRe") spent a lot of time utilizing e-mail, the president accessed the back up files using his supervisory password and read LoRe's and co-plaintiff Laurie M. Restuccia's ("Restuccia") e-mails. After reading LoRe's e-mail to Restuccia, which contained nicknames for the president and referenced his affair with another employee, both employees were fired. The reason given for the termination was excessive use of e-mail, not the contents of their e-mails.

---

[2] This article will discuss the Massachusetts Privacy Act, cases brought under similar privacy statutes in other states and, as to public employees, privacy rights stemming from the Fourth Amendment to the United State Constitution. It will not discuss other statutory sources for employees' claims for invasion of privacy in connection with their use of the Internet and e-mail at work such as the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§2510 – 2522, 2701 – 2712, which prohibits the interception and monitoring of electronic communications, and the Massachusetts Eavesdropping Act, G.L. c. 272 §99, because my co-presenter will be concentrating on these statutes in his article. However, employees rarely prevail on their claims for invasion of privacy in connection with their use of the Internet or e-mail in the workplace pursuant to these electronic interception statutes.

The employees filed claims against the company and its president, *inter alia*, under the Massachusetts Privacy Act and the Massachusetts Eavesdropping statute. The court granted the defendants' summary judgment motion on the Massachusetts Eavesdropping Statute claim, but denied the defendants summary judgment on the Privacy Act claim, holding that there was a genuine issue of material fact as to whether the president's reading of the e-mails constituted an unreasonable, substantial or serious interference with the employees' privacy.

Notably, the employees were likely able to avoid summary judgment on the Privacy Act claim only because the employer lacked appropriate written e-mail and Internet use policies. In a jury trial in Middlesex Superior Court on November 22, 1999, however, a jury found for the employer and its president. *See* Massachusetts Lawyer's Weekly, 28 M.L.W. (Jan. 17, 2000) and 29 M.L.W. (Jan. 10, 2000). Although the employer lacked a written policy on e-mail use, it claimed that it had an established practice about employees' use of e-mail. The employer also presented evidence that the plaintiffs were very familiar with the company's computer system and should have known that their e-mails were not private.

In *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 WL 974676 (D. Mass. 2002), employees received sexually explicit e-mails from the Internet and other third parties, which they then forwarded to co-employees. A fellow employee complained after receiving one of these e-mails. The company, therefore, investigated the employees' e-mail folders as well as those of other employees they e-mailed on a regular basis.

The company terminated the employees for a violation of its e-mail policy, which prohibited messages that were obscene or sexually oriented, and stated that inappropriate use of e-mail was a violation of company policy and may result in disciplinary action. The policy also stated that all information stored in the company's e-mail system was the property of the company. It further said that although the company does not intentionally inspect employees' e-mail usage, there might be business or legal situations that necessitate company review of e-mails and that the company reserved the right to access all e-mail files.

The employees filed a claim, *inter alia*, under the Massachusetts Privacy Act.[3] The court held that while the plaintiffs believed their personal e-mail correspondence was private, their expectation of privacy was not reasonable.

---

[3] The employees also filed claims under the Massachusetts Eavesdropping Statute. In *Garrity*, the court cited to *Restuccia*, stating that the automatic e-mail back up system is protected under the "ordinary business exemption" of the Massachusetts Eavesdropping Statute and, therefore, does not constitute an "unlawful interception" in violation of the statute.

The plaintiffs testified that they assumed that the recipients of their e-mail messages might forward them to others. Plaintiffs, moreover, admitted that they knew the employer had the ability to review the e-mails on the company's system and knew that they had to be careful about sending e-mails. The plaintiffs argued, however, that the e-mails were private because the company had instructed them on how to create passwords and personal e-mail folders. The court noted that any e-mail messages stored in personal folders were still transmitted over the company network and at some point were accessible by a third party.

Although the company had specific policies regarding their employees' use of e-mail in the workplace, the court emphasized that other courts have held that employees have no reasonable expectation of privacy in their e-mail use even where the employer did not have specific e-mail usage policies. *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (Even in the absence of a company policy, plaintiffs would not have a reasonable expectation of privacy in work e-mail).

The *Garrity* court held that even if the plaintiffs had a reasonable expectation of privacy in work e-mail, the company's legitimate business interest in protecting employees from harassment at work would likely trump their privacy interest.

In *Battenfield v. Harvard University*, 1993 WL 818920 (Mass.Super. 1993), an employee brought a claim, *inter alia*, under the Massachusetts Privacy Act based on four allegedly unlawful disclosures, including Harvard's inspection of the employee's papers and computer files while she was on sick leave. The plaintiff's privacy claim was dismissed. The court determined that the material was not highly personal and was reasonably related to the employer's legitimate business interest of ensuring the plaintiff's fitness for the job and the masters' program. The court concluded there was little or no privacy interest in the employee's work files because they were Harvard's property.

B. Non-Massachusetts Cases On Employees' Right To Privacy In Their Computer Use

Plaintiffs filing privacy claims under other states' privacy laws or common law also rarely prevail, especially when the employer has an adequate e-mail and computer use policy.

In *Smyth v. Pillsbury Co*., 914 F.Supp. 97 (E.D.Pa. 1996), an at will employee brought a claim for wrongful termination in violation of public policy when he was terminated for transmitting inappropriate and unprofessional comments over his employer's e-mail system. The court held that the termination did not violate public policy, as there was no reasonable expectation of privacy under Pennsylvania law in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system. The court held that the

employer had the right to read employee e-mails transmitted over the company systems, even if the monitoring was done without the employee's knowledge, and even where the employer had repeatedly assured employees that all e-mail communications would remain confidential and privileged and could not be intercepted and used by the employer against its employees as grounds for termination or reprimand.

In *Thygeson v. U.S. Bancorp*, 2004 WL 2066746 (D.Or. 2004), an employee brought a state law claim for invasion of privacy based on the employer's monitoring and search of his computer at work. The employer compiled a report of all the websites the employee had visited during a particular period, but not their actual contents. The report was compiled using the network drive and no one entered the employee's office.

The court determined that no court precedents supported the employee's argument that he had a reasonable expectation of privacy in the e-mails saved in his personal folder. The court stated that on the contrary, other courts have held that when an employer accesses its own computer network, and like U.S. Bancorp, has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy.

In *Kelleher v. City of Reading*, 2002 WL 1067442 (E.D.Pa. 2002), an employee sued her employer for, *inter alia*, invasion of privacy under Pennsylvania law for the publicizing of e-mails and other purportedly private information relating to her suspension. The court held she had no reasonable expectation of privacy in workplace e-mail where the employer's guidelines explicitly informed employees that there was no such expectation of privacy.

C. Fourth Amendment Right To Privacy

Public employees have also utilized the Fourth Amendment to the United States Constitution, in addition to state privacy statutes, as a source of protection against an invasion of privacy in their use of their employer's computer system.[4] The Fourth Amendment guarantees, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…" U.S.C. Const. Amend. 4. The results have generally been unfavorable to employees where the employer had written policies warning employees of its right to monitor its computer systems, but more favorable to employees where the employer lacked such policies.

---

[4] Note that in bringing constitutional claims, state action is required, which raises issues of sovereign immunity, qualified immunity and common law immunity. These topics are outside the scope of this article, but practitioners should be aware of these doctrines, which shield state actors from liability under certain circumstances.

See e.g. U.S. v. Angevine, 281 F.3d 1130 (10th Cir. 2002) (Employee's motion to suppress materials from work computer denied where employer had written monitoring policy); *U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000) (Employee's motion to suppress denied in light of employer's Internet policy); *U.S. v. Bailey*, 272 F.Supp.2d 822 (D.Neb. 2003) (Employee's motion to suppress evidence from work computer denied where employer had written monitoring policy); *Wasson v. Sonoma County Jr. College Dist.*, 4 F.Supp.2d 893 (N.D.Cal. 1997) (Employee's claim denied because of the employer's written monitoring policy); *U. S. v. Thorn*, 375 F.3d 679 (8th Cir.2004) *cert. granted and judgment vacated on other grounds by* 543 U.S. 1112, 125 S.Ct. 1065 (2005) (Warrantless search of employee's computer did not violate the Fourth Amendment where employer had written monitoring policy); and *Leventhal v. Knapek*, 266 F.3d 64 (2nd Cir. 2001) (Employee had a reasonable expectation of privacy where the employer had no written policy governing computer usage and no general practice of monitoring, but summary judgment for the employer on §1983 claim was affirmed for other reasons.)

Notably, in *Haynes v. Office of Atty. Gen. Phill Kline*, 298 F.Supp.2d 1154 (D.Kan. 2003), the employee prevailed on a motion for a preliminary injunction where the underlying claim was based on Fourth and Fifth Amendment violations even though the employer's computer screen warned employees there was no expectation of privacy in using the employer's computer system. The court emphasized that the employees were allowed to use the computer for private communications, were advised that unauthorized access to users' e-mail was prohibited, were given passwords to prevent access by others, and no evidence was offered to show that the employer ever monitored private files or employee e-mails.

III. EMPLOYEES' E-MAIL COMMUNICATIONS WITH THEIR ATTORNEYS ON EMPLOYERS' COMPUTERS

National Economic Research Associates, Inc.("NERA") v. Evans, 21 Mass.L.Rptr. 337, 2006 WL 2440008 (Mass.Super. 2006), is the only reported Massachusetts decision on the issue of whether employees waive their attorney-client privilege when they communicate with their attorneys on their employer's computer system. The plaintiff employer NERA moved to compel defendant Evans, a former employee, to disclose e-mail communications between Evans and his private attorney that were transmitted on NERA's laptop computer. This case did not include a claim for invasion of privacy. Rather, Evans was seeking to prevent NERA from retaining otherwise privileged e-mail communications between him and his attorney that were retrieved by NERA from its computer.

Significantly, Evans e-mailed his attorney and received responses from his attorney utilizing his private Yahoo e-mail account, but the e-mails were transmitted on the employer issued laptop computer. NERA contended that Evans waived his attorney-client privilege because he should have realized that

the e-mails were stored on the laptop's hard disk and were subject to review by NERA.

When Evans resigned from NERA, he returned his laptop but first deleted his personal files. He did not, however, delete the e-mails from his Yahoo account because he did not know that these e-mails had been stored on the laptop's hard disk. After his resignation, NERA retained a computer forensic expert to search the hard disk on the NERA issued laptop and the expert was able to retrieve various communications between Evans and his attorney. Again, all of these communications were made via Evans' Yahoo account and not on NERA's Intranet. NERA instructed the expert to retain the e-mails, but not review them while NERA waited for the court decision on its motion to compel.

NERA argued that Evans had waived his attorney-client privilege because although his communications with his attorney were intended to be private, Evans should reasonably have understood from the circumstances of the communications that they were likely to be read by NERA.

The court determined that Evans did not waive his attorney-client privilege as to these e-mails on his Yahoo account.

The court stated that Evans could not reasonably have expected to communicate in confidence with his private attorney if he had e-mailed his attorney using his NERA e-mail address through the NERA Intranet because NERA's employee manual clearly warned employees that e-mails on the network could be read by NERA network administrators.

The court noted, however, that NERA's employee manual did not expressly state that NERA would monitor the *content* of Internet communications. Rather, it simply stated that NERA would monitor the Internet *sites* visited. More importantly, the employee manual did not expressly state, or even implicitly suggest, that NERA would monitor the content of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. NERA also did not warn its employees that the content of such Internet e-mail communications was stored on the hard disk of NERA-issued computers and was, therefore, capable of being reviewed by NERA.

In holding that Evans did not waive the attorney-client privilege, the court also emphasized that Evans attempted to maintain the confidentiality of his communications with his attorney by using his private Yahoo account and by deleting other personal files on his NERA-issued laptop before he returned it to NERA. He did not delete the e-mails on his Yahoo account to and from his attorney only because he did not know that they would be stored on the computer's hard drive.

The court's holding appears to be driven by the fact that these e-mails contained attorney-client communications and such communications are sacrosanct. Based on existing caselaw and the holding in this case, the e-mails may well not have been protected under the Massachusetts Privacy Act if the content of these e-mails were not otherwise privileged communications, even if they were sent on a personal e-mail account and even where employees were not warned that such e-mails could be reviewed.

The court, moreover, may well have ruled that the attorney-client privilege had been waived if NERA had a more explicit policy. The court stated:

> The bottom line is that, if an employer wishes to read an employee's attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet, the employer must plainly communicate to the employee that:
>
> 1. all such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and
>
> 2. the company expressly reserves the right to retrieve those temporary files and read them.
>
> Only after receiving such clear guidance can employees fairly be expected to understand that their reasonable expectation in the privacy of these attorney-client communications has been compromised by the employer. *Evans* at *5.

The court, however, raised the dilemma of the employee who wants to communicate with his attorney and is on a business trip. To maintain the attorney-client privilege, the employee would not be able to safely communicate with his attorney on his company issued laptop, but would have to bring a second laptop on his trip. The court noted that even communicating via the hotel's computer might not preserve the attorney-client privilege.

The *Evans* decision is problematic for attorneys because it signals that it is not safe for clients to communicate with their attorneys if they are using their employer's computer system, even if they are using a personal e-mail address. For example, if an attorney sends a client a redlined settlement agreement, the client cannot safely retrieve the agreement until he returns home from work each evening, thereby delaying the settlement process.

Curto v. Medical World Communications, Inc., 2006 WL 1318387 (E.D.N.Y. 2006), is similar to the *Evans* case. The court ruled that the plaintiff had not waived her right to assert her attorney-client and work-product privileges

concerning documents the employer retrieved from the laptop computer issued to the plaintiff. The court concluded that the plaintiff's conduct was not so careless as to suggest that she was not concerned with the protection of the attorney-client privilege. She deleted all personal files and written communications (notes and e-mails) with her attorney before she returned the laptop to the company. (The company was able to retrieve the plaintiff's deleted communications with her attorney only by retaining a forensic consultant.)

Notably, one of the factors the court considered was that the employer did not normally enforce its computer usage policy. The court also emphasized that the plaintiff in this case worked from her home office and her laptop was not connected to the employer's computer server. The employer, therefore, was not able to monitor her use of her home based laptop. In fact, it appears that this case may have been decided differently if the plaintiff had worked on the employer's premises.

The court noted that the standard used in analyzing whether the attorney-client privilege is waived is very different than the standard used to decide whether an employee has an expectation of privacy in workplace computer files where the employer has an explicit e-mail policy.

See also In re Asia Global Crossing, Ltd., 322 B.R. 247 (Bkrtcy. S.D.N.Y. 2005) (The court could not determine whether the attorney-client privilege was waived with respect to employee's e-mails without further record as to whether the employer had a policy of monitoring employees' e-mails.)

IV. DRUG TESTING

The outcome of claims by employees against their employers under the Massachusetts Privacy Act (or also under the Fourth Amendment if they are public employees) for mandatory drug testing usually depends on the nature of the employee's job responsibilities. Employees usually do not prevail on their claims if they are public safety officials or work in hazardous occupations. The courts also examine the drug testing procedure to ensure it is not overly intrusive and is reliable.

In *Folmsbee v. Tech Tool Grinding & Supply, Inc*., 417 Mass. 388 (1994), a former employee sued her employer for discharging her for refusing to submit to drug test. The court held the employer did not violate the employee's rights under the Privacy Act.

The company manufactured industrial cutting tools and the plaintiff was a tool grinder. The tools manufactured by the employee were razor sharp.

The drug testing at issue subjected the employees being tested to a brief visual inspection while dressed in a hospital gown to ensure that no employee brought

a vial of urine with him or her to the test. The court balanced the employer's legitimate business interest in determining the employees' effectiveness at their jobs against the seriousness of the intrusion on the employees' privacy. The court recognized that requiring an employee to submit to urine analysis involved a significant invasion of privacy, but the court found that the balancing test tilted in favor of the employer in light of the dangerous nature of the work, the substantial evidence that drug use had occurred in the workplace, and the procedural safeguards utilized by the employer in the testing process to maximize privacy. The drug testing procedure, moreover, was not unnecessarily intrusive because vials of urine for purpose of frustrating drug testing were commercially available.

In *Webster v. Motorola, Inc*., 418 Mass. 425 (1994), two employees of an electronic equipment manufacturer, an account executive and a technical editor, sued the employer under the Massachusetts Privacy Act and the Massachusetts Civil Rights Act (MCRA), challenging the employer's drug testing program. The court affirmed the Superior Court's grant of summary judgment to the employer as to the technical editor and the denial of summary judgment as to the account executive.

The court determined the technical editor's interests under the Privacy Act outweighed the employer's interests in conducting a random drug testing program. The employer was engaged in the design, manufacture, and sale of electronic and communications equipment to federal and state agencies, and the editor's job duties were such that errors could possibility result in harm to human health and safety or to national security. The editor, however, edited technical texts, he was not a principal writer, his work was checked by others before release, he did not have security clearance, and he did not work directly on matters of national security. The employer conceded that it was unable to predict whether the manuals the editor edited were likely to affect national security or human health and safety. Accordingly, the court concluded that the nexus between the editor's job duties and the harms feared were attenuated and that the employer's legitimate business interests in determining whether its employees are using drugs were outweighed by the editor's privacy interests.

The court held, however, that the employer's legitimate business interests justified its random drug testing of the account executive. The court stated that the account executive's responsibilities included sales of communications equipment to government agencies, and his position required him to drive a company-owned vehicle approximately 20,000 to 25,000 miles a year. The court held that an employer's general interest of ensuring employee safety and providing a drug-free work environment is insufficient by itself to justify a random drug testing program. This employer, however, had an interest in ensuring that its motor vehicle was not being operated by a person intoxicated by drugs.

The court also observed that the employer utilized a number of safeguards to ensure that the testing program was not unreasonably intrusive and that it was reliable. The employees tested were not observed while urinating or visually inspected during the procedure. The specimens were tested by an independent laboratory and if any specimens tested positive, the results were verified by an independent medical review officer. The laboratory, moreover, utilized a highly accurate, state of the art testing technique.

In *O'Connor v. Police Com'r of Boston*, 408 Mass. 324 (1990), a police cadet was discharged after testing positive for cocaine. He filed claims, *inter alia*, under the Fourth Amendment and the Privacy Act.

The court determined that unannounced, warrantless, and suspicionless urinalysis testing of all police cadets did not constitute an unreasonable invasion of police cadets' privacy. The court recognized the intrusiveness of collecting the urine sample and subjecting it to chemical analysis. The court noted, moreover, that the testing is capable of revealing not only recent drug use, but other personal information such as pregnancy. The court observed that this particular drug testing was especially intrusive because the cadets were being monitored in the act of urinating.

The court, however, concluded that the cadets had consented to the testing in pre-employment agreements, police officials had a compelling interest in determining whether cadets were using drugs and in deterring such use, and that those interests outweighed the cadets' privacy interests. The court concluded that any interference with the cadet's privacy rights was neither "substantial" nor "serious."

In *Byrne v. Massachusetts Bay Transp. Authority*, 196 F.Supp.2d 77 (D.Mass. 2002), police associations and police officers employed by the Massachusetts Bay Transportation Authority (MBTA) filed claims under the Privacy Act and the Fourth Amendment challenging a policy which required officers to submit to random urinalysis drug and alcohol screens under direct observation of collection employees in certain circumstances. The court rejected the plaintiffs' claims. The court cited to *Webster v. Motorola, Inc.*, and observed that the only time the Supreme Judicial Court has held that a drug testing procedure violated the Privacy Act was in a case where the employee being tested was not engaged in a dangerous or safety-sensitive occupation.

In *Harrison v. Eldim, Inc.*, 2000 WL 282446 (Mass.Super. 2000), the plaintiff filed suit against his employer alleging that defendants violated the Privacy Act by compelling him to provide a urine sample for drug analysis after he sought medical attention following a work-related accident. The court held that the employer's legitimate business interests justified the post-accident drug testing of an employee in the plaintiff's position to ensure that his work performance was not impaired by controlled substances, and that the procedures the employer

utilized did not invade the plaintiff's privacy any more than was inherent in drug testing itself. The court concluded that there was no unreasonable interference with the plaintiff's privacy.

V. VIDEO SURVEILLANCE OF EMPLOYEES

Claims by plaintiffs under the Massachusetts Privacy Act and/or the Fourth Amendment based on their employer's surveillance of employees have had mixed success depending on the type of surveillance and the particular factual circumstances. There is a dearth of cases in Massachusetts and elsewhere on this issue and the law is still unsettled.

In *Nelson v. Salem State College*, 446 Mass. 525 (2006), a state college employee who was videotaped by a hidden camera as she changed clothes and applied sunburn medication to her upper chest area and neck in an open area of her workplace brought claims under, *inter alia*, the Fourth Amendment pursuant to 42 U.S.C. §1983 and under the Privacy Act against the college and its public safety officers. She claimed that the defendants' 24 hour video surveillance of her workplace without a warrant violated her right to privacy.

The area in question was an office open to the public during the day, but locked at night. However, volunteers and employees had keys. The college began secret video surveillance of the office (but no audio surveillance) because they were concerned about unauthorized entry into the office after regular business hours. The college, however, chose to use 24 hour surveillance instead of surveillance only when the office was closed.

The court in *Nelson* emphasized that there is a dearth of cases involving video surveillance and there have been conflicting conclusions reached by different courts. The court concluded, therefore, that this area of the law is still unsettled.

The court determined that although the plaintiff had a subjective expectation of privacy there was no objectively reasonable expectation of privacy in the workplace against such surveillance and summary judgment was affirmed as to the Fourth Amendment claim. The court emphasized that the area under surveillance was open to the public.

The individual defendants in *Nelson* were sued under the Privacy Act in their individual capacities.[5] The court held that even assuming there was an invasion

[5] The plaintiff conceded that the Commonwealth, the college, the board of trustees and the individual defendants acting in their official capacities were immune from intentional tort claims and that the Massachusetts Tort Claims Act, G.L. c. 258, §10(c), specifically lists invasion of privacy as a type of intentional tort. She also conceded her claim under the Fourth Amendment as to these defendants.

of privacy, the individual defendants were shielded from liability for the Privacy Act claim by the doctrine of common law immunity.[6] They acted in good faith, engaging in activity that was within their discretion in monitoring the workplace, i.e., investigating criminal activity on the campus through surveillance.

The court in *Nelson* and in the other video surveillance cases cited by *Nelson* looked at a number of factors in evaluating whether plaintiffs have an objectively reasonable expectation of privacy. These factors include: whether the surveillance is secret, whether the area under surveillance is public, whether it an enclosed area, whether the surveillance is of a private office with a door, whether the office is locked, whether the employee has exclusive use of the area, whether there is audiotaping, whether there is adequate justification for the surveillance, whether the surveillance is conducted in the most restrictive manner possible, and whether the area under surveillance is a locker room where employees undress or a restroom. *Nelson* at 534-536.

In *Clement, et al v. Sheraton-Boston Corp*., Suffolk Super. Court Docket Nos. 93-0909F, 93-3450F and 94-4233F (Suffolk Super. Ct. Feb. 21, 1997), employees filed a Privacy Act claim based on secret videotaping by Sheraton of a remote area in the men's locker room. Sheraton argued it had been trying to discover whether employees were dealing cocaine. The tapes showed no illegal activity. The court held that the employees could seek emotional distress damages under the Privacy Act, even where no physical harm was suffered. Summary judgment was denied, but the case settled for $200,000 before trial. The settlement went to the five employees who were taped in the men's locker room. *See* Massachusetts Lawyer's Weekly, 26 M.L.W. 1068 (Jan. 19, 1998). *See also Clement v. Sheraton-Boston Corp.*, 1993 WL 818763 (Mass. Super. 1993) (Discussing the facts in denying defendants' motion for an injunction to prohibit parties from disseminating statements about the case by means of public communications.)

In *Vega-Rodriguez v. Puerto Rico Tel. Co*., 110 F.3d 174 (1st Cir. 1997), employees of a quasi-public telephone company filed a lawsuit against the company challenging videotaping of their workplace under the Fourth Amendment. The court emphasized that the law in this area was not established and stated that, "As employees gain access to increasingly sophisticated technology, new legal issues seem destined to suffice the workplace." *Id.* at 176.

---

[6] A public employee may be personally liable pursuant to G.L. c. 214 § 1B , but under the doctrine of common law immunity a public official, exercising judgment and discretion, is not liable for negligence or other error in making an official decision if the official acted in good faith, without malice and without corruption.

The court held the employer could engage in video surveillance monitoring of employees. It concluded that the employer was a "quasi public" company and there was no reasonable expectation of privacy in workplace. The employer had a legitimate interest in the efficient operation of the workplace and told employees in advance when cameras would operate. They did not record sound or invade any reasonable expectation of privacy.

The court noted that, "…the mere fact that the observation is accomplished by a video camera rather than the naked eye, and recorded on film rather than in the supervisor's memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one." The court observed that if the employer is constitutionally permitted to monitor the employees with the naked eye, it could instead choose to accomplish that goal by means of an unconcealed video camera not equipped with microphones. The court cautioned, however, that cases involving secret videotaping or electronically assisted eavesdropping would be viewed more critically.

VI. CONCLUSIONS

In conclusion, it is clear that an employee's right to privacy is circumscribed.

The computer use cases cited in this article make it abundantly clear that it is essential for employers to disseminate detailed and clear policies to their employees about their use of the employer's computer systems. The cases also make it clear that employees should generally assume that their use of the employer's computer system is never private and can be monitored or reviewed by their employers.

In the drug testing area, the courts generally look to see whether the employee is in a dangerous or safety sensitive position. The courts further consider whether the employer is utilizing the least intrusive means of testing and whether the employer is ensuring that the test results are accurate.

The video surveillance cases are very fact specific. The courts generally analyze whether there is a legitimate business purpose for the surveillance, and consider factors such as whether the video surveillance is concealed, whether there is also audio surveillance, whether the area under surveillance is public, whether the employee has the exclusive use of the area, and whether the surveillance is of a particularly sensitive area such as a locker room or a restroom. The results of these cases are not always consistent.

In short, although plaintiffs seeking redress for invasion of privacy have remedies under the Massachusetts Privacy Act and for public employees, under the Fourth Amendment to the United States Constitution, the courts afford the employer ample latitude in monitoring its employees.