I. INTRODUCTION

This article will address employees’ right to privacy in their use of e-mail and the Internet in the workplace.

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. c. 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). Other states have similar privacy statutes or common law.

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.

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 pursuant to the Massachusetts Privacy Act, similar privacy statutes or common law in other states, or the Fourth Amendment in connection with their use of e-mail and the Internet in the workplace do not prevail when the employer has adequate policies in place notifying its employees that the employer’s computer systems and employer issued computers 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 computers. Even when an employer does not have adequate computer use policies, the employer sometimes still prevails on invasion of privacy claims by its employees. In general, the courts in

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.
Massachusetts and elsewhere balance the employer’s legitimate business interests against the employee’s reasonable expectation of privacy under the privacy statutes and the Fourth Amendment and usually find that the employee did not have a reasonable expectation of privacy.\(^2\)

Significantly, courts are much more concerned about providing protection to employees who communicate with their attorneys on their employer’s computers when they utilize their personal, password protected e-mail accounts. The courts carefully scrutinize these cases because of the significance of the attorney-client privilege. Nonetheless, employers often prevail on these claims if the employer has adequate e-mail use policies, including warning employees that they have no right to privacy even in their personal password protected e-mails if they are transmitted on the employer’s computer. Some courts also consider whether the employee took reasonable steps to protect their communications with their attorneys, whether the employer normally reviews their employees’ e-mails and enforces their computer use policies and whether the dissemination of the computer use policy to employees was adequate. A significant departure is *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), which states that even if the employer’s policies were entirely adequate, it would find that the employee has a reasonable expectation of privacy in communications with her attorneys because of the important public policy concerns relating to the attorney-client privilege.

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

A. **Massachusetts Cases under the Privacy Act**

In *Restuccia v. Burk Technology, Inc.*, 5 Mass. L. Rep. 712, 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

---

\(^2\) This article will discuss the Massachusetts Privacy Act, cases brought under similar privacy statutes and common law 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, which prohibits the interception and monitoring of electronic communications, the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*, and the Massachusetts Eavesdropping Act, G.L. c. 272 §99. However, employees rarely prevail against their employers 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.
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.

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 U.S. Dist. LEXIS 8343, 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. The court held that while the plaintiffs believed their personal e-mail correspondence was private, their expectation of privacy was not reasonable. 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.

---

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.
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.

*See also Oropallo v. Brenner*, 25 Mass. L. Rep. 147, 2009 Mass. Super. LEXIS 13 (Mass.Super. 2009) where a former employee sued her former supervisor for, *inter alia*, invasion of privacy alleging that he improperly circulated confidential material from an internal investigation into job performance that alluded to her sexual affair with a fellow employee. In considering whether plaintiff had a reasonable expectation of privacy in her romantic relationship, the court considered her use of the Town of Northborough's e-mail server in personal banter and noted that some courts have suggested that there is no reasonable expectation of privacy in information transmitted via work e-mail where an employer's e-mail policy warns employees that their messages may be monitored, comparing *Garrity* and *Restuccia*. The court determined that the policy at issue, which purportedly warned employees that their e-mail accounts were subject to scrutiny, was not determinative of Oropallo's expectation of privacy in this particular case because it was not clear that Oropallo’s e-mail banter amounted to the type of voluntary exposure that would cast into the public domain the fact that she was involved in a sexual relationship. The court ultimately denied summary judgment because there existed a genuine issue of material fact as to whether Brenner had a legitimate interest in publishing the materials to Town employees and volunteers that outweighed Oropallo's interest in keeping aspects of her personal life from public view.

In *Battenfield v. Harvard University*, 1 Mass. L. Rep. 75, 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**

Employees filing privacy claims under other states’ privacy laws or common law also rarely prevail when the employer has an adequate e-mail and computer use policy, and sometimes even when the employer does not have any 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 U.S. Dist. LEXIS 18863, 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 U.S. Dist. LEXIS 9408, 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 that 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.

In *Sporer v. UAL Corporation*, 2009 U.S. Dist. LEXIS 76852, 2009 WL 2761329 (N.D. Cal. 2009), the company fired an employee because he sent an e-mail with a pornographic video attachment from his work account to his personal account. The court held that the company did not unreasonably invade the employee’s privacy because the company had disseminated a clear e-mail policy to employees, including statements that it reserved the right to monitor all e-mails on the company’s e-mail system and that employees were prohibited from transmitting obscene messages on the system. There was also a warning notice that appeared on employees’ computers every time they were turned on and employees had to click “ok” to clear the warning notice.

### 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. 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.

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. Gavegnano, 305 Fed. Appx. 954 (4th Cir. 2009) (No Fourth Amendment violation given the user agreement signed by employee consenting to monitoring of all activities on government issued information system); 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.

Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), rehearing en banc denied, 554 F.3d 769 (9th Cir. 2009), cert. granted sub nom. City of Ontario v. Quon, 130 S.Ct. 1011 (2009), is a significant case which is now on appeal at the United States Supreme Court. This case involved a police officer’s texting of sexually explicit personal messages utilizing the police department’s issued pager. The Ninth Circuit found that the police officer’s right to privacy pursuant to the Fourth Amendment and the California constitution was violated when the police department audited his personal text messages.

Although the police department had no specific policy regarding text messaging, it had a strong e-mail and internet use policy which warned that the use of the police department’s computers and all associated equipment, networks, Internet, e-mail and other systems operating on these

---

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.
computers is limited to police business. In its policy, the police department reserved the right to monitor and log all network activity without notice. Police officers also attended a meeting during which a police lieutenant informed the employees that pager messages were considered e-mails and that those messages would be covered by the police department’s computer use policy. The lieutenant also said that text messages constituted public information and were eligible for auditing.

What the court found persuasive, however, was that the police department had an informal unwritten policy governing the use of the pagers. The informal policy provided that if a police officer used more than the allocated monthly character limit for text messaging, the police department would not audit the police officer’s text messages to determine if they were work related as long as the police officer paid for the overage himself. In fact, the police officer exceeded his allocated monthly limit three or four times previously. He paid for the overage and his text messages were not audited. The court held that without this informal policy, the police officer would have no reasonable expectation of privacy in his personal text messages.

The court further held that even though the police officer had a reasonable expectation of privacy in his text messages because of the police department’s informal policy, the court’s decision still hinged on whether the police department’s search of his text messages was reasonable. There was a material dispute concerning the police department’s actual purpose or objective in auditing the text messages. The court held that if the purpose of the search was to determine whether the allocation of the monthly character limits was adequate to cover all work related messages and to prevent police officers from having to pay overage charges for work related text messages, the search was reasonable because the search was work related. On the other hand, if the purpose of the search was to uncover misconduct, the search would not be reasonable. However, a jury found that the police department’s purpose in conducting the audit was to ensure that police officers were not being required to pay for work-related expenses. The Ninth Circuit nonetheless found that the search was excessively intrusive because there were less intrusive ways of conducting the audit to achieve the objective of ensuring that police officers were not required to pay for work-related expenses.

[After this article was written, the Supreme Court of the United States reversed the Ninth Circuit decision in the case of City of Ontario, California v. Quon, 130 S.Ct. 2619 (2010). The Supreme Court held that the police department’s search of Quon’s text messages was reasonable. The Court noted that the search was justified at its inception because there were reasonable grounds for suspecting that the search was necessary for the non-investigatory work-related purpose of determining whether the character limit on the city’s contract was sufficient to meet the city’s needs. Additionally, the city and the police department had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work related expenses or, on the other hand, that the city was not paying for extensive personal communications. In short, the court held that the review of the text messages was reasonable because it was an efficient and expedient way to determine whether the employee’s overages were the result of work-related messaging or personal use. Accordingly, there was no violation of Quon’s Fourth Amendment rights.]
III. EMPLOYEES’ E-MAIL COMMUNICATIONS WITH THEIR ATTORNEYS ON EMPLOYERS’ COMPUTERS

In National Economic Research Associates, Inc. (“NERA”) v. Evans, 21 Mass.L.Rptr. 337, 2006 WL 2440008 (Mass.Super. 2006), Judge Gants discussed 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.
In another Judge Gants decision, *TransOcean Capital, Inc. v. Glen M. Fortin*, 21 Mass. L. Rep. 597, 2006 Mass. Super. LEXIS 504, 2006 WL 3246041 (Mass. Super. 2006), TransOcean filed a motion to compel the deposition testimony of a subsidiary’s board member and his attorney regarding their communications about the board member’s plan to find outside investors for an acquisition. The board member and the attorney argued that their e-mail communications were confidential because of the attorney-client privilege. TransOcean argued, however, that the attorney-client privilege was breached because the e-mail communications utilized TransOcean’s e-mail address and TransOcean’s computer system.

The pivotal issue was whether the board member received fair warning that TransOcean could read his e-mails, including otherwise privileged e-mails. Judge Gants held that the board member did not receive fair notice because TransOcean did not have its own policies or procedures manual or employment manual setting forth its policies on computer use and Transocean’s review of e-mails on its network. Instead, TransOcean retained an outside company, TriNet, to handle human resources issues for TransOcean.

TriNet maintained an Employee Handbook on its website which stated that all communications stored in TransOcean’s computer system belong to TransOcean and are to be used only for job-related purposes. It also warned that TransOcean, “may monitor use of any systems and equipment to ensure proper usage”. Judge Gants held, however, that TransOcean failed to expressly inform its board members and employees that it had adopted TriNet’s handbook. It also failed to provide its board members and employees with a copy of the handbook. There was also no evidence that the board member was aware of these computer use policies. Accordingly, Judge Gants held that the e-mail communications between the board member and his lawyer on TransOcean’s computer network utilizing TransOcean’s e-mail address did not breach the attorney-client privilege. (The court did rule, however, that the privilege was breached because the board member and his attorney’s communications were disclosed to an outside individual.)

Cases from other jurisdictions also focus on whether an employee has waived the attorney-client privilege in light of the employer’s e-mail policies. For example, *Curto v. Medical World Communications, Inc.*, 2006 U.S. Dist. LEXIS 29387, 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.

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

In *Long v. Marubeni America Corp.*, 2006 U.S. Dist. LEXIS 76594, 2006 WL 2998671 (S.D.N.Y. 2006), although two employees used their work computers to communicate with an attorney through private password protected e-mail accounts, such communications were not privileged where the company’s electronic communications policy stated that there was no right to privacy in employees’ e-mail and prohibited their use of company systems for personal use (and the company sent employees a reminder each year of this policy).

In *Kaufman v. SunGard Inv. System*, 2006 U.S. Dist. LEXIS 28149, 2006 WL 1307882 (D.N.J. 2006), the court held that the employee’s e-mail communications with her attorney sent and received from the company’s e-mail system were not privileged given the company’s policy that it could search and monitor e-mail communications at any time. *See also Leor Exploration & Prod. LLC v. Aguiar*, 2009 U.S. Dist. LEXIS 87323 (S.D. Fla. 2009)(no reasonable expectation of privacy regarding employee’s communications transmitted using company e-mail address and server in light of handbook that stated company owns all electronic communications and individuals using its e-mail system have no expectation of privacy) and *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866 (D.Oh. 2009) where the court held that e-mails sent from a work e-mail account were not privileged when the employer’s policy said it reserved the right and intended to exercise the right to review and intercept all messages created, received or sent over the e-mail system for any purpose. The court noted that the employee did not attempt to protect the confidentiality of the messages by using a personal web-based, password protected e-mail account.

In *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436 (N.Y.Sup.Ct. N.Y. 2007), the court held that e-mails that a physician received from an attorney through the hospital's e-mail system were not protected by the attorney-client or work product privileges where the hospital had a policy that e-mail could only be utilized for business purposes and it reserved the right to access emails. The court was not persuaded by the fact that the e-mails from the attorney contained a notice stating that the communication “may” be confidential and that the attorney should be notified if anyone other than intended recipient gained access to the e-mail message.

In *Current Med. Directions, LLC v. Salomone*, 2010 N.Y. Misc. LEXIS 388 (2010) the court granted a motion in limine holding that the attorney-client privilege did not apply to e-mails between the employee and his attorney. Notably, the employee did not object to the use of e-mails that were exchanged between him and his attorney after the employer was acquired because *Scott v. Beth Israel Medical Center, Inc.* is “clear authority” that such e-mails are not
privileged and that as an employee using the company e-mail system, the employee had no reasonable expectation of privacy in such communications. However, the employee objected to the use of pre-acquisition e-mails by the acquiring entity, which resided in the employer’s computer servers and along with other assets, were sold in the acquisition. The employee, however, made no effort to delete the e-mails from the servers prior to or after the acquisition and did not assert any privilege (or seek a protective order) with respect to these e-mails until the motion in limine, thus the court determined he did not take reasonable steps to prevent their disclosure.

In *Mason v. ILS Technologies, LLC*, 2008 U.S. Dist. LEXIS 28905, 2008 WL 731557 (W.D.N.C. 2008), the court held that the attorney-client privilege was not waived where the employer could not demonstrate that the employee was aware of the employer’s e-mail policy, which stated that e-mail was for business purposes only and that the employer reserved the right to review all e-mail sent over the employer’s systems, or agreed to abide by it, or that the policy was effectively communicated to employees.

In *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), the New Jersey Supreme Court held that although the employer’s policy stated that it had the ability to monitor an employee’s e-mail, the attorney-client privilege was not waived where the employee communicated with her attorney from a work issued laptop computer through a personal password-protected web-based e-mail site. The court noted that the employer’s policies did not explicitly state that the employer could monitor emails utilizing personal e-mail accounts. The policy also permitted occasional personal use of e-mail. The court further noted that the attorney’s e-mail had a standard warning about the attorney-client privilege, although it did not consider this a substantial factor.

Significantly, *Stengart* went beyond a mere analysis of the sufficiency of the employer’s computer use policy and held that even if the employer had a perfect policy, it still would find that the employee had a right to privacy in her communications with her attorney. The court stated,

> But employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual – that is a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee’s attorney-client communications, if accessed on a personal, password-protected e-mail account using the company’s computer system - - would not be enforceable. *Id.* at 665.

This latter holding is at variance with prior cases that simply analyze the sufficiency of the employer’s computer use policy to determine whether the attorney-client privilege remains intact when an employee communicates with her attorney on company issued computers. The court, however, said that employers have the right to discipline employees for violating a policy permitting only occasional personal use of the Internet if the employee spends significant parts of
the work day communicating with her lawyer or if the employee sends offensive material on e-mail.

See also U.S. v. Hatfield, 2009 U.S. Dist. LEXIS 106269 (E.D.N.Y. 2009) where in ruling on a motion to dismiss an indictment, or, in the alternative, to suppress certain evidence based on alleged violations of the attorney-client privilege and attorney work-product doctrine, the court noted that most courts seek to determine whether the employee, as a practical matter, had a reasonable expectation that the attorney-client communications would remain confidential despite being stored on a company's computer system and have considered the following factors: (1) does the corporation maintain a policy banning personal or other objectionable use; (2) does the company monitor the use of the employee's computer or e-mail; (3) do third parties have a right of access to the computer or e-mails; (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies and finally (5) how did the company interpret its computer usage policy? Based on these five factors, the court found that the employee did not waive privilege with respect to otherwise privileged or work-protected documents stored on his employer’s computer.

In Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441 (D.Conn. 2009), the court denied the defendant’s motion for summary judgment on the employee’s Fourth Amendment claim despite the school district’s computer use policy. The employee alleged that the superintendent accessed her e-mail account without her permission, accessing an e-mail containing a letter the employee sent to her attorney. The court determined that the employee had a reasonable expectation of privacy in her work e-mail because the school district's acceptable use policy stated that users had a limited privacy expectation in the contents of their personal files on the District system, only the employee and the computer system's administrators had the password to her e-mail account, and it was not the practice of the school district to routinely monitor e-mail accounts.

IV. EMPLOYEES’ CLAIMS AGAINST EMPLOYERS FOR MISCONDUCT IN THEIR ACCESSING AND USE OF EMPLOYEES’ E-MAILS.

It is important to distinguish between an employer’s general access to an employee’s e-mail and unauthorized access. For example, in Pure Power Boot Camp, Inc. v. Warner Fitness Boot Camp, LLC, 587 F.Supp.2d 548 (S.D.N.Y. 2008) the employer was found to have violated the federal Stored Communications Act because the employer illegally accessed e-mails that former employees sent on their personal, password protected e-mail accounts from the former employees’ own home computers. Some of the e-mails were sent to their attorneys.

The employer was able to access a former employee’s Hotmail account because the former employee had left his user name and password information stored on the employer’s computers. The employer did not examine its own computers to determine which e-mails the former employee accessed at work, but rather logged directly into Microsoft’s Hotmail system where the e-mails were stored and it printed the e-mails directly off the Hotmail system. There was no evidence that the e-mails in dispute were created on “or sent or received through, the employer’s computers or that they were viewed at work”. The court held that the employer was precluded from admitting e-mails it illegally accessed as evidence in its lawsuit against the former
employees for breach of their fiduciary duties and infringement of the employer’s trademarks and copyrights, but that the e-mails could be used for impeachment purposes if the former employees opened the door.

Employers must also enforce their e-mail monitoring policies consistently to avoid unlawful discrimination claims. For example, in Williams v. Wells Fargo Fin. Acceptance, 564 F.Supp. 2d 441 (E.D.Pa. 2008), the court denied summary judgment for an employer on an African American employee’s claims under state and federal discrimination laws. The employee was terminated for violating the employer’s e-mail usage policy and sexual harassment policy. The employee had sent an e-mail that contained sexually suggestive and otherwise inappropriate jokes and a picture attachment in violation of the employer’s policy. The employee claimed, however, that his termination, as well as that of 29 other African American employees who disseminated similar e-mails, was the result of racial discrimination. The employee alleged that in a previous similar situation, non-African American employees were treated less harshly for violating the same e-mail usage policy. The employee presented evidence that it was common for employees to send personal e-mails, including e-mails with pornographic or sexual content, during work hours and that the employer usually counseled or warned employees rather than firing them. The court concluded that a jury could reasonably infer that the employer selectively enforced its e-mail policies and utilized the most severe discipline available to result in the termination of a disproportionate number of African American employees.

V. CONCLUSIONS

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

The computer and e-mail 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 system and employer issued computers, including e-mail use. The employer’s policies need to be clear that e-mails sent on the employer’s computers are subject to review by the employer regardless of whether the employees use their personal or work e-mail accounts, and even if the e-mail is password protected. The cases also make it clear that employees should assume that their use of the employer’s computer system and employer issued computers is never private and can be monitored or reviewed by their employers.

In short, although plaintiffs seeking redress for invasion of privacy have remedies under the Massachusetts Privacy Act, similar invasion of privacy statutes and common law in other states, and for public employees, under the Fourth Amendment, the courts afford employers ample latitude in monitoring their employees’ computer use.

The recent New Jersey Supreme Court case of Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010), however, held that even if the employer had a perfect computer use policy, it still would find that the employee had a right to privacy in her communications with her attorney. It stated that employers have no need or basis to read the specific contents of personal, privileged attorney-client communications in order to enforce corporate policy. Please note, however, that even the Stengart court would not likely have reached this conclusion if the e-mails in question were not communications with an attorney.
Also, significant is *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892 (9th Cir. 2008), *rehearing en banc* denied, 554 F.3d 769 (9th Cir. 2009), *cert. granted sub nom.* *City of Ontario v. Quon*, 130 S.Ct. 1011 (2009), which held that an employee had a reasonable expectation of privacy in the contents of his personal text messages despite the employer’s strong computer use policy. The court based its decision on an informal unwritten policy that the employer would not audit the employee’s text messages as long as the employee paid overage charges.