I. Introduction: Can Privacy and the Information Age Co-exist?

Computers, e-mail and Internet access are an integral part of doing business in the twenty first century. If used correctly, technology enhances business productivity and efficiency. If abused, technology can distract employees from their work, expose employer trade secrets or create liability for employers by preserving evidence that support claims of discrimination or harassment or lead to expensive compliance with discovery obligations. As employers search for solutions to the issues raised by technology, perhaps by monitoring employee computer use or by enforcing e-mail and Internet policies, they may inadvertently expose themselves to conflict and liability in ways they did not anticipate.

The instantaneous transferability of data and the omnipresence of technology in the workplace have heightened the sensitivity of employees, the legislature and the judiciary to issues regarding the privacy of personal information. Additionally, employees and privacy advocates often criticize the surveillance of employee e-mail and Internet use for legitimate business purposes as unnecessarily invasive and occasionally illegal. Many of the questions about the intersection of individual privacy and technology as they relate to the workplace remain unresolved. The result is added pressure on employers to consider how best to balance privacy concerns and their need to run effective businesses.

This paper covers some of the most recent legal and management issues raised by concerns
about privacy and technology’s increasingly central role in the workplace. Further, it provides advice to employers about how to address these issues, given current legal thinking.

II. May Employers Monitor Employee Technology Use?

By now most employers should have adopted policies governing employee Internet and e-mail use. Implementing such policies makes good common sense. A well written policy alerts employees that employer owned computers and networks exist primarily, if not exclusively, for business purposes. To the extent that employers choose to tolerate a certain amount of extracurricular use, a good policy makes clear that all use must be in keeping with generally accepted professional standards. Namely, these policies should prohibit employees from visiting gambling, pornographic or hate group web sites. They should also prohibit employees from downloading sexually explicit images or copyrighted music to their work computer. Further, an e-mail policy should note that e-mail is not the appropriate forum to circulate off-color jokes, or to send abusive, profane or threatening messages.

In order to enforce these policies, employers may wish to inspect hardware issued to employees and monitor employee e-mail or Internet use from time to time. Additionally, many employers are taking advantage of software that blocks access to certain categories of web sites from their system. Other software can identify when prohibited language is used in e-mail correspondence.

According to a recent Washington Internet Daily release, more than eighty percent of major U.S. companies review the e-mail that employees write and the web sites they visit. Sixty seven percent of employers have disciplined or terminated at least one employee for improper or excessive use of e-mail or Internet access.
As a rule, disciplining or terminating employees in the twenty first century always creates risk of litigation. Termination or discipline resulting from abuse of workplace technology is no exception.

In deciding claims of wrongful termination arising from surveillance on the part of employers, courts typically have held that employees have no reasonable expectation of privacy in employer provided technology, period. Garrity v. John Hancock Mutual Life Insurance Company, Civ. Act. No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (holding that employees had no reasonable expectation of privacy in e-mail folders marked personal); Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (plaintiff had no reasonable expectation of privacy in his work e-mail); McClaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 (Tx. Ct. App May 28, 1999) (holding that there is no reasonable expectation of privacy in an employer owned e-mail system).

However, pertinent precedent is still limited in most jurisdictions. As a result, employees continue to bring suit against their employers when the decision to terminate or discipline them was based upon review of files or online activity they considered “private.” Such suits are filed on a number of grounds, including that their employer acted in violation of: the federal Electronic Communications Privacy Act, the federal Electronic Communications Storage Act, a state constitutional provision or privacy statute, the Fourth Amendment (if they worked for a public entity) or their right to privacy as derived from common law.

In Garrity v. John Hancock Mutual Life Insurance Company, Civ. Act. No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) plaintiffs were terminated for forwarding sexually explicit e-mails to their coworkers. A co-worker lodged a complaint with the plaintiffs’ supervisor that plaintiffs were sending harassing e-mail. Consequently, the supervisor launched an investigation into the matter, accessing the e-mails archived in each plaintiff’s personal folders. The investigation was in keeping with the employer’s e-mail policy, which explicitly stated
that “management reserves the right to access all e-mail files.”

Nonetheless, plaintiffs sued alleging that their privacy had been invaded. They asserted that their employer’s e-mail policy was “impossible to locate” on their employer’s Intranet and that it was too difficult to understand. Further, they suggested that their employer led them to believe that their personal e-mail was private by allowing them to store e-mail in folders marked personal and by granting them passwords for guarding against unauthorized access to their computers. While the Massachusetts district court agreed that the employees clearly had a subjective belief that their e-mails were private, it held that their belief was not objectively reasonable. Employees knew that management could view any e-mail in any folder without using their particular computer and that the company actively sought to prevent its e-mail system from being used to disseminate sexually explicit e-mails because its e-mail policy clearly stated that employees were subject to discipline for sending messages with sexual content.

The outcome of Garrity provides a clear basis for promulgating strongly worded policies regarding Internet and e-mail use to reduce employees’ expectation of privacy. Still, some of the first cases to address monitoring suggested that an employer could conduct any type of surveillance it liked of the computer, e-mail and Internet access it provided to employees whether or not it had a policy to that effect. See Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that even in the absence of a company e-mail policy, plaintiff did not have a reasonable expectation of privacy in his work e-mail); McClaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 (Tx. Ct. App May 28, 1999) (holding that there can be no reasonable expectation of privacy in an employer owned e-mail system). Garrity also expressed strong support for employer surveillance of e-mail and Internet use. There, the court noted that an employer’s legitimate business interest in protecting its employees from harassment in the work place would trump a plaintiff’s privacy claims even if the plaintiff could