WILMERHALE

Do Employees Have a Legitimate Expectation of Privacy in Their E-Mail and Voicemail Communications?

DECEMBER 1, 1999

Today, employees are more and more reliant and knowledgeable about the use of the world wide web, e-mail and voicemail systems for conducting their day-to-day tasks. Employees are using these technologies to communicate with customers, suppliers and colleagues. But, along with business use comes personal use. Employees usage of computers and telephones for personal business can range from chatting with friends and relatives to cyber-shopping. The employer of today must be cognizant of the risks and benefits of the use and misuse of these ever-expanding technologies.

The usefulness of these technologies is well-known for employee access, use and dissemination of business information. Likewise, misuse of communication technologies can just as easily waste company time and resources as a result of employees:

- spending too much time on personal e-mail messages;
- taking part in extensive "chat room" dialogues;
- misappropriating and disseminating company trade secrets;
- improperly posting company information on "bulletin boards;"
- copying and distributing intellectual property without authorization; and
- sending or downloading inappropriate, sexually hostile or harassing messages or graphic pictures which can expose companies to liability.

By establishing policies stating the company's expectations regarding e-mail and Internet access and use, employers can prevent misunderstandings and possible claims before they develop.

Do Employers Have A Right To Monitor E-Mail And Internet Use By Employees?

The federal law on employee privacy rights and e-mail is still developing. Congress enacted the Electronic Communications Privacy Act Of 1986 (ECPA) [1], which prohibits the interception of "electronic communications" including e-mail, to update older federal wire-tapping laws used to combat organized crime. ECPA protects e-mail messages from interception and disclosure to third parties. Section 201 of ECPA provides that a person who "intentionally accesses without authorization a facility through which an electronic communication is provided . . . and thereby

obtains access to an . . . electronic communication while it is in electronic storage . . . shall be punished as provided in subsection (b) of this section." [2] E-mail is considered stored electronic communications under ECPA. Exceptions within ECPA, however, appear to exempt employers who monitor employee e-mail.

First, ECPA only applies to electronic communications that "affect interstate or foreign commerce." As such, intracompany e-mail communications likely will not fall within the Act. Second, ECPA allows for the interception of electronic communications where one of the parties to the communication has given prior consent. In theory, employees could consent to the interception of communications sent or received on their employer's e-mail system. The final exception employers could utilize is the "business exception." For the business exception to apply, an employer would likely need to show that its reason for monitoring is credible and not excessive. In such circumstances, the employer would argue that the interception or monitoring is necessary to prevent misconduct in the work environment, or that it justifiably suspects disclosure of confidential information.

Even if exempted from ECPA, employers still must be wary of the possible common law claims that irate employees may bring upon discovering that their e-mail was intercepted and read by their employers. Likewise, many states already have statutes creating a tort for invasion of privacy and several states are considering enacting statutes [3] . For a list of states that have enacted privacy laws, click here. Employees may claim under existing state laws that their privacy has been improperly invaded when their employers review or monitor what the employees deem to be their "private," "non-business related" communications. Massachusetts, for example, has a statute which protects every person in the Commonwealth from unreasonable, substantial or serious interference with his or her privacy [4] .

In *Smyth v. Pillsbury Co.*[5], a federal court interpreting Pennsylvania common law on privacy concluded that an employee has no reasonable expectation of privacy in his e-mail5. The court stated that a reasonable person would not consider an employer's interception of e-mail communications to be a substantial and highly offensive invasion of privacy. The employer's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail was found to outweigh any privacy interest that the employee may have had.

Employee access to the Internet can also lead to potential employer liability. For example, employees who use an employer's internal access usually disclose the employer's name as the originator of the message. Thus, if the employee accesses or downloads copyrighted materials or engages in any other inappropriate conduct, a third party could argue that the employer had a duty to stop such conduct. Likewise, if during employment the employee downloads and utilizes copyrighted information, the company likely will be liable for copyright infringement. Companies also need to make sure that employees are not improperly accessing and sending confidential information or trade secrets of the company over the Internet.

Don't Forget - E-Mail Is Evidence.

E-mail also is becoming the proverbial "smoking gun" in litigation. Today, smart attorneys are routinely requesting e-mail records as part of their general discovery requests. Prominent recent

examples include the Microsoft antitrust trial and the Clinton impeachment proceedings.

Employers and employees must understand that e-mail is not a one-time, whispered exchange. E-mail messages can be retrieved, recreated and used as evidence, even if the sender or recipient believes they have been deleted.

What Should Employers Do?

Every employer who provides e-mail and Internet access to its employees should create e-mail and Internet policies that explain the company's expectations and state that the company's e-mail, voicemail and computer systems are monitored. Policies should state that employees' e-mail and Internet access are the company's property. Employees should also be cautioned to only commit to e-mail what they would commit to paper because e-mail continues to exist even after the delete button is pushed. To prevent e-mail from being recreated, companies should also implement electronic deletion procedures which will destroy all e-mail files on a regular basis. By doing so, companies may prevent embarrassing or damaging messages from being restored after deletion.

Lisa S. Burton
lisa.burton@haledorr.com

---

[1] 18 U.S.C. ' 2510 *et seq*.

[2] Civil penalties for violation of ECPA include preliminary and other declaratory and equitable relief, monetary damages, punitive damages, attorneys' fees and costs. 18 U.S.C. ' 2520(b). Criminal penalties include maximum imprisonment for not more than five years, fines, or both. 18 U.S.C. ' 2511(4)(c).

[3] For example, the California legislature is currently considering a law requiring employers to notify employees if they are monitoring an employee's e-mail. S.B. 1016, 1999-2000 Reg. Sess. (Ca.1999). The California bill on monitoring can be viewed here.

[4] The Massachusetts Privacy Statute, M.G.L. c. 214, ' 1B.

[5] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996).