

REGULATING E-MAIL AND INTERNET USE IN THE WORKPLACE

Just as employers gain tremendous business advantages from their employees' use of e-mail and the Internet, an employee's inappropriate use of these tools can create varied and potentially serious risks for employers. This ELA addresses the legal risks involved in today's workplace technology and the steps employers can take to reduce those risks.

SOME OF THE RISKS

Inappropriate e-mail and Internet use by employees, such as the downloading and forwarding of sexually explicit, racist or copyrighted material, can expose an employer to lawsuits for unlawful harassment or copyright infringement. Other risks include the public disclosure of confidential information or trade secrets and the infection of the employer's information systems by computer viruses. Employees also may use the Internet to engage in "cybersmear" campaigns against their employers by posting false information about the company on Internet message boards. And, of course, employers may justifiably be concerned about the loss of employee productivity from personal e-mail and Internet use during working hours.

THE IMPORTANCE OF POLICIES AND TRAINING

Effective risk-management for employers in this area includes issuing a written policy addressing employee e-mail and Internet use, communicating that policy to employees, and conducting training on the policy. An effective policy, combined with regular training, will help to educate employees about the risks created by their inappropriate use and the consequences to them should they violate the policy. Perhaps more importantly, however, having an effective policy that has been communicated to employees will go a long way in preserving an employer's right to monitor employee e-mail and Internet use when the employer chooses to do so. As discussed below, without an effective policy in place, a court could potentially determine that such monitoring violates employee privacy rights.

We recommend that e-mail and Internet use policies be featured prominently in employee handbooks and covered in periodic training sessions, and that employees acknowledge in writing that they have read and understand the employer's policy.

CURRENT LAWS ALLOW EMPLOYER MONITORING

Generally, employers enjoy substantial freedom to monitor their employees' workplace use of e-mail and the Internet. Federal privacy laws such as the Electronic Communications Privacy Act of 1986 ("ECPA") provide several exceptions for employers and have been interpreted by courts to allow employer searches of

employee e-mails after they have been sent or received. For example, employers who maintain their own networks on which e-mails are stored fall within an exception under the ECPA for "system providers." Similarly, courts have found that state wiretap statutes, which prohibit the surreptitious interception of wire and oral communications during transmission, generally do not reach the reading of e-mails by employers after they have been sent or received by employees.

NO COMMON-LAW INVASION OF PRIVACY

Although there have been recent lawsuits in which plaintiffs have claimed that their privacy rights were violated by employer searches of their personal e-mails and computer files, courts generally have rejected such employee claims. These lawsuits generally have turned on whether the employee had a "reasonable expectation of privacy" in e-mails and personal files stored on the employer's computer systems. Historically, courts have held that no reasonable expectation of privacy exists for employees using company-owned computers. Courts have also recognized that employers have legitimate business interests, such as the protection of other employees from harassment, that justify monitoring. Employer e-mail and Internet use policies that put employees on notice that their stored e-mails, computer files, and internet habits are not personal or confidential have been cited by courts to show that an employee's asserted expectation of privacy was not reasonable.

KEY ELEMENTS OF AN EFFECTIVE E-MAIL AND INTERNET USE POLICY

As a threshold matter, an e-mail and Internet use policy should clearly state whether the employer's e-mail system and Internet access are to be used only for business purposes. Although lawful, many employers find it unrealistic or counterproductive to completely prohibit the personal use of computers by employees, opting instead for a middle-of-the-road approach that: (1) encourages primarily business use and (2) specifically prohibits inappropriate or potentially harmful personal use.

Whether or not the employer's policy specifically allows personal use, however, the most important element of any policy is that it clearly puts the employee on notice that his or her use of e-mail and the Internet in the workplace is neither private nor confidential. For example, a good policy should begin with a general discussion of policies relating to the use of the employer's computers including the following:

- The Company's computer hardware and all of the information stored on that hardware, or on any equipment connected with it through a network, are the property of the Company.
- The Company makes back-up copies of information

stored on its computer equipment, monitors files stored on its equipment, and examines such files from time to time.

- The Company cannot and does not ensure the privacy, security or confidentiality of personal information stored on its computer equipment.

A good policy will then reiterate this “no privacy” principle in the specific context of e-mail and Internet use by including more specific statements such as:

- E-mail and Internet access are business tools provided to employees primarily for business purposes.
- All e-mail messages or other communications sent internally or externally using the Company’s computers or communications systems are the property of the Company and are also subject to backup or other form of electronic storage or reproduction. Therefore, employees should not expect that any message transmitted using these systems is private.
- The Company reserves the right to access and review employee’s e-mail messages and Internet activity.
- The contents of e-mail messages and/or employees’ Internet activities may be disclosed when the Company determines that there is a business or other appropriate reason to do so.

As noted, a policy should give employees clear guidance concerning the permitted uses of e-mail and the Internet. The following is a non-exhaustive list of typical policy provisions:

- E-mail is to be used principally to transmit routine business information to assist employees in performing their day-to-day functions.
- Material transmitted by e-mail (internally or externally) or the Internet or posted to an Internet website from a Company PC must follow employer policies, good business practice and common sense with respect to communications with the public.
- In composing and sending e-mail, employees should take into consideration that e-mail messages are considered documents, just like any other writing, and could be subject to discovery in any litigation involving the Company. Although an e-mail may seem fleeting, messages may continue to exist in the Company’s electronic backup or storage files long after they are “deleted” by the employee.

The policy should also list examples of prohibited conduct. A

non-exhaustive list of prohibited activities includes:

- Solicitation for political, religious or other personal causes or personal business ventures (not including reasonable charitable solicitation)
- Transmission of material that is false, derogatory, profane, vulgar or sexually explicit, or any other material that would be offensive or harassing to the average person (*e.g.*, a racial or ethnic slur)
- Downloading from the Internet of sexually explicit or other offensive materials, software programs, or any copyrighted or trademarked materials
- Viewing or posting messages to web sites that contain sexually explicit, racist or other offensive material
- Engaging in any criminal activity
- Accessing the e-mail of any other employee without the approval of that employee or the approval of a supervisor or manager
- Disclosing online any confidential, proprietary, personal or business information related to the Company or to other employees

SPECIFY CONSEQUENCES FOR POLICY VIOLATIONS

An employer’s policy should clearly state that violations of policy may result in disciplinary action up to and including termination of employment.

PROVIDE OPEN CHANNELS OF COMMUNICATION

An employer’s policy should encourage employees who have questions about e-mail and Internet use in the workplace to call the information systems department or speak to their supervisor. The policy should also encourage employees who believe that they are receiving inappropriate e-mail to promptly bring the matter to the attention of management.

A FINAL NOTE ON PASSWORDS

Some plaintiffs have argued that personalized computer passwords give rise to a reasonable expectation of privacy. Generally, courts have rejected this argument on the grounds that e-mail is transmitted over the employer’s network and, therefore, is accessible to review by third parties at many points. Nevertheless, a good policy should include the following language as a defense against password-related privacy arguments: “The Company reserves the right to bypass personal passwords and access computer systems in its sole discretion.”

The MORSE, BARNES-BROWN & PENDLETON EMPLOYMENT & LABOR PRACTICE GROUP provides sophisticated legal services and practical advice to employers of all sizes, ranging from technology start-ups to Fortune 500 companies.

Robert M. Shea – rms@mbbp.com ♦ Mark H. Burak – mhb@mbbp.com

Donald W. Parker – dwp@mbbp.com ♦ Sandra E. Kahn – sek@mbbp.com ♦ Scott J. Connolly – sjc@mbbp.com

BUSINESS | SECURITIES | M&A | TECHNOLOGY + IP | TAX | EMPLOYMENT + IMMIGRATION

Reservoir Place ♦ 1601 Trapelo Road ♦ Waltham, MA 02451 ♦ (p)781-622-5930 ♦ (f)781-622-5933 ♦ www.mbbp.com