

First Wednesday — A Monthly Discussion of Employment Law Issues and Other Hot Topics for Management



By Jeffrey A. Snyder - Issue No. 7: February 5, 2003

Jeff is a Shareholder of Thoits, Love, Hershberger & McLean, specializing in employment law and commercial litigation. He can be reached at (650) 327-4200 or jsnyder@thoits.com.

E-Mail and the Need for a Company Monitoring Policy

The widespread use of e-mail has led to a real need for companies to adopt specific policies to monitor and control its use in the workplace. Any company that is concerned about limiting its liability, protecting corporate assets and generally reducing exposure to various risks, should immediately put in place an e-mail monitoring policy. The reason has much less to do with the idea that “Big Brother” is watching, but has everything to do with protecting the company and its property.

After reviewing the issues and concerns posed by e-mail use, I will list the elements to include in a sample e-mail monitoring policy.

An E-mail Policy Fits Well with Other Established Company Policies

Most companies already have specific policies forbidding sexual harassment and disclosure of confidential information. Yet with the huge growth in the use of e-mail, and the ease by which e-mail can be used to forward such things as obscene jokes, derogatory and discriminatory material, and company trade secrets, an effective e-mail policy is crucial to enforcing the company’s established policies.

Some Examples of How E-mail is Being Used as Evidence in Litigation

The use of e-mail as evidence in civil lawsuits has grown dramatically. In a sexual harassment case, jokes and pictures sent by company employees may tend to prove allegations of a hostile working environment. In a defamation case, slanderous material posted on the company's intranet or electronic bulletin board may become Trial Exhibit A. In an age discrimination case, offhand or joking remarks that would not have been said in a formal letter or memo, will be found in someone's "deleted" e-mail. In a patent infringement case, premature public disclosure, shown to destroy patent protection, might be proven by the careless and simple act of clipping proprietary data as an attachment to an e-mail sent externally. In a case for misappropriation of trade secrets, one of the elements of proof is that the company has made "reasonable efforts" to keep its information protected; but without an effective e-mail policy in place, arguably, this element cannot be proven. These are just a few examples of the many situations in which e-mail can be used against companies in litigation.

Why is E-mail Such a Valuable Source of Evidence?

Aside from the near-total reliance on e-mail, people tend to be overly casual in their style of communicating by e-mail. Things are written in e-mail that would not be written in a formal letter. Things are said that would not be said in a face-to-face conversation. Moreover, e-mail is never truly deleted, but is always recoverable, sometimes by data recovery experts specializing in the gathering of forensic evidence. E-mail creates a permanent record. Because e-mail is such a rich source of evidence, it is essential to monitor and control its use.

An E-mail Policy Will Help Defeat Claims for Invasion of Privacy

Another reason to have an e-mail monitoring policy is to protect against employee claims for "invasion of privacy." Each individual has a right of privacy that extends to the workplace. The issue in a case of workplace privacy invasion is whether the individual had a "reasonable expectation of privacy" based on all the facts and circumstances. For example, the fact that an employee may choose a "private"

password, or may access the company's computer system from home, tends to create a presumption of privacy. Therefore, as to all company property and systems (including e-mail, voicemail, Internet use and corporate servers and databases), the company needs to have a clear policy such that, while the company respects individual privacy, it must reserve the right to monitor and control all of its systems – as set out below.

The Minimum Components of an Effective E-mail Policy:

- The company has the right to monitor web surfing and read e-mail without notice, as needed for administrative and investigative purposes, and to ensure that all company property and systems are being used for legitimate business purposes.
- Employees have no right or expectation of privacy when using company property and systems, including, but not limited to, e-mail, voicemail and Internet access. There is no expectation of privacy even though passwords are chosen and even when company-owned laptops are used, or systems are accessed from home.
- All passwords belong to the company, and the company may also use an overriding IT-password to access its computers and systems.
- E-mail and the Internet are primarily for business use; while some personal use may be permitted in the company's discretion, this privilege cannot be abused or cause interference with the timely performance of anyone's job duties.
- The company does not tolerate unlawful harassment or discrimination of any kind. There shall be no obscene, harassing or discriminatory content in e-mails sent or received, including attachments and links.
- The company owns valuable intellectual property and other confidential information. Nobody can send trade secret, confidential or proprietary

information to anyone other than those with a genuine business need to know. Be careful about overusing the “cc” and “bcc” buttons.

- Always proofread and contemplate your e-mail before sending it, checking for spelling, grammar, tone, style and potential double meanings. Do not use e-mail casually. Remember, e-mail creates a permanent record.
- Any violation of the company e-mail policy may result in discipline up to and including immediate termination.
- Any questions about this policy should be directed to Human Resources or the Legal Department. The company reserves the right to change its policies at any time without prior notice, but will make reasonable efforts to post notice of the changes.

Effect of Federal Law

A final cautionary note relates to the Electronic Communications Privacy Act, or ECPA. This federal law prohibits unauthorized access to, or retrieval of, a wire or electronic communication while in electronic storage or transit without the consent of a party to the communication. To defend against potential violations of the ECPA, therefore, companies should have their employees specifically consent to the e-mail monitoring policy. Even if consent is obtained, any monitoring should only occur on a limited and necessary basis. (Since the “provider” of the communications service is exempted from liability under the ECPA, employers who own their systems may also have an additional defense.)

Summary

Employers should (1) adopt a formal e-mail policy including the minimum elements listed above; and (2) access and monitor their employees’ e-mail and Internet habits only as needed for administrative, investigative or necessary business purposes.

(© Jeffrey A. Snyder and Thoits, Love, Hershberger & McLean)

First Wednesday Distribution List:

- If you are not receiving this newsletter directly, please send me your e-mail address and I will add you to the First Wednesday Distribution List.
- If you no longer want to receive this newsletter, please send me an e-mail with "Remove" in the subject line.
- If you would like this newsletter redirected to others within your organization, please send me their e-mail addresses.
- First Wednesday is a publication of general applicability and not specific to any set of facts. Thus, it should not be relied upon for any specific case or matter without further discussion. No attorney-client relationship is formed as a result of your reading or replying to this newsletter, which is not intended to provide legal advice on any specific matter, but rather to provide insight into current developments and issues.

Jeffrey A. Snyder
Thoits, Love, Hershberger & McLean
245 Lytton Avenue, Suite 300
Palo Alto, California 94301-1426
Telephone: (650) 327-4200
Facsimile: (650) 325-5572
E-mail: jsnyder@thoits.com

