WILMER, CUTLER & PICKERING

e-commerce news

January 25, 1999

E-Mail Policies

The growing use of electronic mail ("e-mail") by companies and its overwhelming popularity among employees present new concerns for corporate counsel. The current Microsoft antitrust trial provides an extreme example. Despite being a leader in the computer industry, Microsoft never had an e-mail policy governing retention of messages. The government was able to obtain thousands of e-mail messages dating from more than five years ago, some of which were used to impeach Chairman Bill Gates's videotaped testimony.

Here are three steps you may want to consider taking:

1. Establish an E-Mail Usage Policy for Employees. Any usage policy should be in writing, and employers should consider having employees sign an acknowledgment form to verify that they have read the policy and will comply with it. Among other things, a usage policy should:

- warn employees not to use language that can tarnish the company's image or subject it to liability;
- remind employees that e-mail messages may be retrievable—by the company or by opposing parties to a litigation—long after employees delete them from their computers; and
- provide clear guidance as to the employer's policy on access to e-mail by those other than the reader or recipient and on use of e-mail for other than company purposes.

2. Establish a Retention and Elimination Policy. Counsel should identify the relevant laws and regulations governing the company's retention of documents or records. This exercise is particularly important in heavily regulated industries. In the securities industry, for example, SEC Rule 17-a-4 requires brokers and dealers to retain for three years "[o]riginals of all communications received and copies of all communications sent by such member, broker or dealer (including inter-office memoranda and communications) relating to his business as such." A company's e-mail retention policy should specify the routine deletion of e-mail so that its e-mail is archived for the shortest period necessary for its regulatory or business needs. Keep in mind that in some cases business uses for e-mail include recording transactions or communications with clients or associates. In such cases, business needs may dictate a relatively lengthy retention period. An e-mail retention/elimination policy may include:

- A statement specifying the routine, automatic deletion of e-mail from the company server and back-up tapes;
- A statement requiring employees to discard

inactive e-mail regularly. (Note that this policy may not be desirable where employees use e-mail to organize their activities/ projects);

- A statement that automatic deletion of e-records will be suspended and steps taken to preserve these records once litigation or investigation commences; and
- Compliance measures, such as requiring employees to sign acknowledgment forms, holding regular training sessions, and re-circulating the written policy as a reminder to employees.

3. Consider Using E-mail Archiving/ Monitoring Software. Archiving software can help a company protect privileged e-mail from disclosure, respond appropriately and efficiently to discovery requests, and comply with laws and regulations regarding document retention. Monitoring software can protect a company from liability to its employees for harassment or discrimination, prevent employees from disseminating defamatory statements or confidential information, and identify e-mail records that must be maintained in compliance with document retention laws and regulations. Although employer monitoring of e-mail has prompted privacy suits by employees, screening software can actually preserve some level of employee privacy since e-mail is simply scanned by the software for "red flag" terms and is not read by a person unless such terms are detected.

E-Mail Risks

- **E-mail is Informal and May Provide a Basis For Litigation.** Because e-mail has an informal "feel," employees sometimes use language that is inappropriate for formal written communications and can tarnish the company's image or even subject it to liability. For this reason, e-mail messages provide a powerful tool for litigants. Whereas cases in the past were difficult to prove because much of the conduct at issue was oral, e-mail messages can provide a hard copy—and hard proof—of harassing or discriminatory conduct. Also, employees who send sexually explicit e-mail to co-workers can create a hostile work environment, exposing the company to sexual harassment claims. In 1995, Chevron Corporation paid $2.2 million to settle a lawsuit brought by four female employees who contended that sexist jokes circulated via e-mail were part of a pattern of sexual harassment. Companies may be held indirectly liable for failing to address behavior that creates a hostile work environment. To prevent the harassing use of e-mail, a company should establish an acceptable-use policy, spelling out approved e-mail usage and making misuse grounds for termination.

- **Employees Believe (Inaccurately) in the Effectiveness of Deletion.** There is a widespread problem of "perceived impermanence": an employee may mistakenly believe that once he or she deletes a message from her inbox, it can no longer be retrieved. E-mail is not truly gone until it is overwritten by other information in each place that it is stored. Computer forensics experts can retrieve e-mail files even if they have been partially overwritten.

- **Use of E-Mail May Increase Security Risks.** Whether done intentionally or unintentionally, employee e-mail usage can result in the loss of confidential company information. Although the Economic Espionage Act of 1996 makes it a crime to intentionally steal a trade secret, such criminal liability may not redress the harm done when an employee leaks confidential information. In cases where particularly sensitive information must be guarded, companies may want to consider using filtering and monitoring software to prevent and detect the leaking of confidential information. Programs such as Assentor and MIMEsweeper can screen outgoing e-mail for terms that indicate corporate espionage, insider trading, and inadvertent revealing of trade secrets. So-called "sniffer" programs

divert the messages containing such terms to a manager or supervisor for review before they are transmitted to the outside world.

- **Use of Encryption Raises Special Problems.** Some employees may use encryption programs to encrypt their e-mail and other files, and companies may find that such programs are valuable for some purposes. Employers may want to require that employees encrypt their e-mail only with the use of software approved by the company. This software may provide for retention by the company of a key necessary to access encrypted messages, or may otherwise limit the degree of protection provided by such encryption. Alternatively, companies should consider whether and how they could retrieve computer records if an employee's encryption key were not available. Note that the federal government has restricted the export of programs containing encryption technology. Consequently, companies that decide to distribute encryption programs should inform employees of these restrictions to prevent liability for violating the export restrictions.

- **Employees Believe E-Mail is Private.** There is a common misperception among employees, perhaps created in part by the use of confidential passwords, that e-mail is private. Nonetheless, most courts hold that because the company owns the e-mail system, management has the right to read anything on it. Generally, employees have no reasonable expectation of privacy in their e-mail messages. However, any e-mail usage policy should put employees on notice as to the level of privacy that he or she can expect. A company can build trust with its employees by providing that it will access e-mail only when it has a business reason to do so and that it will use procedures that assure responsible monitoring practices. The policy may reduce the risk that an employee will bring a privacy action and may reduce costs of litigation if an employee does bring suit.

- **Employees Receive Spam, Inappropriate Materials, and Large Files.** Corporate systems administrators may reasonably become concerned that incoming e-mail files contain inappropriate materials, unsolicited commercial e-mail ("spam"), or large files (e.g., animated greeting cards) that use up too much of the firm's storage capacities. Companies may be able to delete such messages at the gateway. Although the Electronic Privacy Communications Act of 1986, 18 U.S.C. § 2510 et seq. (1986), generally prohibits the interception (access to contents) of electronic communications, it allows a "provider" of electronic communications to intercept and monitor messages on its system. Companies providing e-mail to their employees would likely fall within the definition of a "provider" because they own the equipment being used. The Act also provides an exception to liability where one of the parties to the electronic communication has consented to the interception. A written policy providing that the company has a right to monitor e-mail, particularly if signed by the employee, may be evidence that the employee has consented to interception of his or her messages. (If e-mail accounts are company accounts, it also may be able to argue that the company is the intended recipient, via its agent.) Or, a company may elect to use a filtering program (such as MIMEsweeper by Content Technologies) that automatically deletes specified categories of messages. Programs of this type also can control inappropriate web surfing, which uses corporate time and resources.

David R. Johnson djohnson@wilmer.com 202/663-6868
Susan P. Crawford scrawford@wilmer.com 202/663-6479
Jennifer E. Grishkin jgrishkin@wilmer.com 202/663-6048

This memorandum is for general purposes only and does not represent our legal advice as to any particular set of facts, nor does this memorandum represent any undertaking to keep recipients advised as to all relevant legal developments.