

AN EMPLOYER'S E-MAIL PRIMER

Much has been written about the rights and responsibilities of employers and its employees relating to the use of the company provided e-mail service. Employers have the right, if not in fact the duty, to monitor and audit the e-mail traffic to insure that their system is not being used for unlawful purposes, and should be monitoring the e-mail to be sure that it is not being used for any purpose not in the employer's best interest. Monitoring and auditing includes the right to review randomly, or any particular employee's e-mail specifically, as the company sees fit.

Because this area is changing so rapidly, we have created this link to the most recent version of 18 U.S.C. Sections 2702 *et seq.*-- STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS law. An important section of the Act is Section 2701(c)(1) which states that it is not a violation of the Act for the person or entity providing a wire or electronic communication service to access electronic communications (e-mails) while they are in electronic storage on the employer's system. If the employer owns and runs the e-mail service and stores the electronic messages on its own servers, under the Act, it is free to access any of the messages stored there.

Cited below are three (3) typical cases dealing with these issues. Unfortunately, there does not seem to be one case which covers all possible aspects of the e-mail problem. However, the three cases do seem to make the important points worth considering.

The employer should first promulgate an e-mail and internet policy for the company at large, if one does not already exist. The case of *U.S. v. Simons*, decided February 28, 2000, gives a fairly detailed explanation of what such a policy should say, content of which was approved by one appellate court. Although addressing the subjects in a criminal context, *Simons* clearly stands for the proposition that no one has a reasonable expectation of privacy in a company e-mail service, and even if they did, that expectation would not be legitimate in light of a published e-mail/internet policy stating that it was the company's intention to audit, inspect and/or monitor internet and e-mail usage.

In *Bohach v. Reno*, decided July 23, 1996, a district court in Nevada engaged the same issue and reached substantially the same conclusion. The *Bohach* court however, also addressed the statutory claims related to 18 U.S.C. § 2701 *et seq.* The court concluded that once the emails in *Bohach* were remitted to the city's electronic

storage, “the City, as the system provider, was free to access the stored messages as it pleased.” While not addressed as yet in any district court in all districts, this appears to be a well reasoned opinion and that many courts will reach a similar result in similar circumstances.

Finally, Smyth v. The Pillsbury Company, decided January 23, 1996, is an action by a private employee against a private employer. The claim made by the employee was that the employer had violated the employee’s privacy right by reading the employee’s e-mail without his consent or without notice. This employer had gone so far as to guarantee that e-mail messages would never be used as a basis for termination or reprimand. Ultimately, the employer used plaintiff’s e-mails as a basis for termination, alleging that the e-mails transmitted inappropriate and unprofessional comments. Disposing of plaintiff’s claims for violation of the employee’s right to privacy as embodied in the common law, the court held that there was no such violation because the employee could not have a reasonable expectation of privacy in an e-mail system used by the entire company. The court went on to state that even if the employee did have a reasonable expectation of privacy in his e-mail communications, the companies interception of those e-mails was insubstantial and not a highly offensive invasion of the employee’s privacy, and therefore the company’s interest in preventing inappropriate and unprofessional conduct or comments over the company e-mail system outweighed any privacy interest that the plaintiff may have had in those e-mails. While there is no way to predict with any certainty what a specific court might do under similar circumstances, this result seems a reasonable one.

We have assembled some basic guidelines for the formulation of policy that might be of interest to an employer:

1. Any internet or electronic mail policy should make clear that the system is owned by the employer and that it is a company resource and is not there for private use.
2. The employees should be advised that they should have no expectation of any privacy regarding anything on the company computer system. Such a statement should be made in the context of an announcement by the company that they will audit, monitor and/or inspect e-mail and internet usage on the company system at will.
3. Employees should be cautioned to treat company e-mail as they would any business or professional communication and that all e-mail should

be written with an expectation that it will be read by a third party, and with the certain understanding that it is subject to review by the company at will.

4. The firm should set up some specific procedure to permit e-mails containing unprofessional, unbusinesslike, and unlawful material to be reported to the company. In particular, laws such as Title VII require that employers have procedures in place for reporting discriminatory conduct and preventing retaliation for such reporting. The e-mail policy should be set up in such a way as to permit an employee who believes they have been the subject of discriminatory treatment as reflected in e-mail message(s) to bring that to management's attention consistent with the requirements of Title VII. There are any number of other laws and instances where such a reporting procedure needs to be put into place if the company is to protect itself against claims that it did not work hard enough to protect its employees from prohibited conduct perpetrated through the employer's e-mail or internet system.

There are those in the legal community who believe that the policy should be signed off on by each and every employee. In a large company, this may be impractical. It seems that the policy could be made part of the employee manual, or as some firms have done, every time an e-mail message is written, forwarded, or replied to, a short message is displayed, together with the e-mail being composed, which alerts the employee to the core features of the company policy. Obviously requiring a signed statement will have a greater impact on the employees.