



Doing Business Since 1926

October 2005

CHAMBER NEWS

The Greater Bethesda-Chevy Chase Chamber of Commerce

Privacy Rules in the Workplace

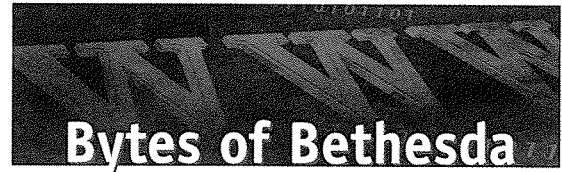
by Eric Von Vorys, Shulman, Rogers, Gandal, Pordy & Ecker, PA

There is a conflict in the workplace between employers who want to make sure their employees are working efficiently and employees who do not want their every move monitored. So far, the employees are losing the battle.

Courts generally recognize an individual's right to privacy in places where the individual has an expectation of privacy, such as the individual's home. This historically does not cover the individual's workplace because the employer owns the phone, the computer, and the building where the individual works. What's more, new technologies make it possible for an employer to monitor virtually every aspect of the workplace. According to the 2005 Electronic Monitoring and Surveillance Survey, conducted by the American Management Association and the ePolicy Institute, 76 percent of employers monitor workers' Web connections, while 50 percent store and monitor employees' computer files. The Electronic Communications Privacy Act (ECPA) of 1986, which was intended to provide individuals with some privacy protection in their electronic communications, has several exceptions that limit an individual's privacy in the workplace.

Without notice, employers are generally free to monitor (i) computer keyboard keystrokes, (ii) review and store employee e-mails and instant messages, and (iii) the time spent on the phone and phone numbers called. The only exception is under Maryland's wire tapping laws, which prevent an employer from recording an employee's telephone calls without notifying the parties that the call may be monitored. Notwithstanding, employers may still run into legal trouble under ECPA if their monitoring practices trespass into areas where an employee has an expectation of privacy.

Consequently, from a "best practices" standpoint, before monitoring electronic communications, an employer should adopt a written electronic communications policy. The policy should clearly state that there is no expectation of privacy in the workplace, that all computer activities will be monitored, as well as email traffic and Internet use, and that all data on the company's electronic communications system belongs to the company even if it is password protected. The policy should also provide notice to the employees as to what use is considered unacceptable by the company with respect to the Internet or when communicating via email (e.g., receiving, sending, or downloading offensive material). Once adopted, the policy should be distributed to all employees.



"Bytes of Bethesda" is a service of the Chamber's Technology Resources Committee, which invites members with an interest in current technology trends to join and participate in the committee, which meets the first Thursday of every month in the Chamber's Board Room. Members are also invited to write technology-related articles for the *ChamberNews*' "Bytes of Bethesda" column.