

Web of Intrigue

Employers Face Potential Liability for Employees' Internet and E-mail Use

By *KEVIN V. MALTBY*

Recent case law suggests that employers may be liable for the conduct of their employees when they use the company's E-mail and Internet connection. For example, you may be liable for an employee disseminating pornographic material by E-mail because it was generated from your location. Before you slide down a slippery legal slope, you might want to consider a few safeguards.

Over the past two decades, employers have witnessed a technological evolution in the workplace environment. Computers replaced typewriters, electronic data storage has replaced filing cabinets, electronic mail and scanning have replaced faxes, and the Internet has replaced libraries. Most recently, instant messaging is beginning to replace electronic mail. While employers seem focused on integrating technology with business, they often overlook revising employment policies and procedures to match technology. In addition, employees seem willing to help themselves to your Internet and E-mail while conducting personal business.

When you consider updating your office equipment, software, and computers, you should also upgrade your employee handbook and other policies and procedures associated with technology. The following are suggested topics that you should assess regarding your employees' use of technology.

Employee Handbook

First, update your employee handbook to include a compre-

hensive E-mail and Internet use policy. Recent case law suggests that courts are balancing whether an employee has a reasonable expectation of privacy against the realities of the workplace environment. The Supreme Court has acknowledged that employees may have a reasonable expectation of privacy with regard to a

Inform employees whether personal use of the Internet or E-mail is permitted. It is advisable to prohibit all personal use of the Internet and electronic mail on company time and equipment.

file cabinet or desk; however, the court also noted that the privacy expectations of an employee "may be reduced by virtue of actual office practices and procedures."

While it is clear from the Supreme Court that there are no absolutes regarding this issue, it is also apparent that you can reduce an employee's expectation of privacy by adopting an unambiguous written policy regarding the use of the Internet, E-mail, and instant messaging. Such a policy should be included in your company's employee handbook, and you should alert your employees that they should have no expectation of privacy relative to E-mail, Internet use, or instant messaging. You should warn your employees that you reserve the right to inspect files on the network and their desktops to assure compliance with company policies and procedures.

Electronic Mail and Internet Use Policy

You should develop a comprehensive E-mail and Internet use policy in concert with revising your employee handbook. Once the policy has been developed, the next step is to communicate it

whether personal use of the Internet or E-mail is permitted. It is advisable to prohibit all personal use of the Internet and electronic mail on company time and equipment.

Monitoring rights: Advise employees that their Internet and E-mail activity is monitored.

Prohibited uses: Inform employees what uses of Internet and E-mail are permitted or prohibited.

Report violations: Develop an easy process for employees to report mistakes or violations.

Consequences: Provide employees with information regarding the consequences of violating the E-mail and Internet use policy.

Technological Restrictions

You might also invest in a firewall or Internet restriction program. This is a proactive approach to enforcing your E-mail and Internet use policy by blocking certain Internet sites or E-mail content. Recent case law has suggested that employers may be liable for the conduct of their employees when using the company's electronic mail and Internet connection. By implementing a strict firewall or Internet restriction program, you reduce the chances of liability by preventing certain content from reaching your employees or letting them send it out of your company.

For example, you could have a firewall that prevents employees from accessing certain Web sites such as pornographic, sports, or Internet gaming sites. Especially important here is the ability to

to your employees. Work with your network administrator to include an advisory each time an employee signs into the company system. As previously mentioned, the E-mail and Internet use policy should be documented in your employee handbook, and when you hire a new employee, it's a good idea to have him or her sign an orientation statement acknowledging receipt of the policy.

You might also want to consider conducting a training session regarding your E-mail and Internet use policy so employees have the opportunity to ask questions and alleviate fears about it.

Electronic Mail and Internet Use Policy Quick Tips

Make sure that everyone is familiar with the personal use policy: Inform employees

restrict access to hack sites that offer free, illegal software. Such software is typically full of viruses, spyware, and keystroke loggers that allow a hacker to get into employees' systems and obtain passwords. While employees would be able to enter a restricted URL into their Internet browsers, they would be unable to access that prohibited site.

In addition, there are programs available that scan electronic mail, preventing viruses and attachments from landing in the employee's inbox. Some monitor only incoming E-mail, and some monitor both incoming and outgoing E-mail. It is often overkill to monitor outgoing E-

mail because this could cause a severe delay to E-mail delivery that could inconvenience regular business activity. Monitoring incoming E-mail only requires someone within your company to regularly scan the blocked E-mail logs to make sure that no legitimate E-mail got caught in the filter. While it may be costly to purchase and maintain these programs, the potential liability for not doing so is staggering.

Back It Up

Another technological tool at your disposal is the backing up of all data created, received, sent, and stored by the E-mail system and Internet usage history. This

information becomes invaluable when investigating the conduct of a current or former employee. Imagine a scenario where a current employee is using your company's information, technology, or data to create his or her own business.

By virtue of saving and backing up electronic usage information, your employees' conduct is memorialized, and your company may have a cause of action against an employee for usurping a trade secret.

Employers need to balance the need for technology to enhance their business and productivity with the possible liabilities associated with its use.

By taking a proactive, preventative approach, employers can minimize liability with a revised employee handbook, E-mail and Internet use policy, and restrictions on the use of the technology within the company.❖

Kevin V. Maltby, Esq., is an associate with Bacon & Wilson, P.C. He is a former prosecutor for the Northwestern District Attorney's Office with extensive jury trial and courtroom experience. His practice concentrates on litigation, employment, and family matters. He also handles personal injury and product liability; (413) 781-0560; kmaltby@bacon-wilson.com