Monitoring Workplace Computer Activity Can Protect Your Business

Employee access to proprietary business information through office computers and networks is no less of a risk than the threat from outsiders, which can be more easily addressed with a barbed-wire fence.

By Catherine P. Wells, Esq., and Denise J. Pipersburgh, Esq.
Wolff & Samson

THERE IS LITTLE DOUBT THAT THE ADVANCE OF technology has significantly enhanced business efficiency, including the ability to manage customer relationships and deliver products and services in an expeditious and cost-effective manner. Although there are significant benefits associated with the use of e-mail and the Internet in the workplace—allowing for instantaneous, interactive communications that ensure business demands are met with speed and efficiency—this same technology also poses considerable risks for employers.

Significantly, allowing employees access to company-owned computer equipment and software without restriction not only can potentially impact employee productivity, but could create a minefield for litigation. As a consequence of employee misuse of these systems, employers should monitor employee's e-mail and Internet usage to protect their legitimate business interests.

Indeed, there are a multitude of legitimate reasons for an employer to monitor employee e-mail and Internet use. For example, every employer must guard against the unauthorized dissemination of confidential business information or trade secrets by employees to competitors and others. Likewise, employers should be concerned that there is the potential that web surfing by employees could cause downloads of dangerous computer viruses that could crash an entire computer system if appropriate precautions are not taken.

Monitoring employees' e-mail and Internet usage may also demonstrate an employee's lack of productivity by revealing that employees are exchanging jokes, conducting personal business during work hours, or viewing pornography. Indeed, monitoring e-mail may demonstrate that an employee is sending messages to others within the workforce that constitute unlawful harassment and discrimination.

Despite the legitimate business reasons justifying such monitoring, unwary employers often overstep the legal boundaries, resulting in unnecessary, costly litigation from disgruntled employees who are disciplined or discharged as a result of the abuse of their employer's computer system. Typically, these employees institute lawsuits asserting claims for invasion of privacy or alleged violations of the federal and state wiretapping laws, which limit an employer's right to intercept employee e-mail communications.

To balance the employee's right to privacy with the employer's legitimate business needs, while simultaneously avoiding liability, employers must be proactive from the outset. All employers should implement a clear and unequivocal policy providing employees with written notice that the computer system, the software and all information stored on those systems are property of the company. Moreover, the policy must provide that both e-mail and the Internet are designed for business use only, that employees have no expectation of privacy in any communications transmitted through the company's computer system, and that the employer reserves the right to randomly and periodically monitor an individual employee's e-mail and Internet usage. A carefully tailored policy will also prohibit an employee from accessing personal e-mail accounts from a work computer, and require the employee to sign the policy acknowledging receipt of it.

The dissemination of such a policy will not only eradicate an employee's invasion of privacy claim, but it is also sufficient to constitute implied consent to any monitoring conducted by the employer so as to avoid potential liability under the various federal and state laws. Many employers also have implemented additional protective measures, such as the installation of software programs designed to block access to undesirable Web sites, including personal e-mail Web sites. Appropriate blockers can, in some instances, prevent the unauthorized disclosures of confidential information, excessive downloading and employee non-productivity.

Although employer monitoring of e-mail and Internet use can create risks, there is a substantially greater threat posed by failing to take any action. If properly implemented, an e-mail and Internet monitoring policy can reduce any risks associated with reviewing an employee's use of company-owned computers, while simultaneously protecting an employer's business interests. As technology continues to advance, it is critical for employers to take appropriate steps to protect their business interests by regulating employee use of their equipment, including their computers. ■

Catherine Wells is the chair of the Employment Law Group at Wolff & Samson PC in West Orange; Denise Pipersburgh is an associate in the Group.