

THE MANAGEMENT JOURNAL FOR CORPORATE GROWTH

SmartBusiness[®]

a SMART BUSINESS NETWORK[®] publication

DALLAS

SMART LEADERS

Why The Levenson Group's Stan Levenson focuses on the benefits of people and products, not their attributes

FAST LANE

Informatics' Ed Burke: You have to have that 'big hairy audacious goal' mentality

Doing it right

How Daniel Son helped build Penson Worldwide into a powerhouse securities service firm

What's on your screen?

Dealing with employee use of the computer **Interviewed by Curt Harler**

Electronic communications and computers are supposed to make everyone's job easier. However, there is great tension in the workplace between firms that want to protect themselves by limiting employee use of the Internet and e-mail and workers' expectation of privacy.

Smart Business asked Audrey E. Mross of the Dallas law firm of Munck Butrus Carter, P.C. where the lines should be drawn.

What aspects of employee computer usage are most troubling to employers?

The most common worry is 'cyberslackers' whose workplace productivity has an inverse relationship to the amount of time they spend visiting Web sites and sending e-mails. Go to www.bored.com for an eye-opening list of ways to waste time on a computer, including virtual Bubble Wrap to pop. Less frequent but more serious offenses include transfer of trade secrets, violation of copyrights, trading in child porn and other illegal activities.

Can a firm prohibit all personal use of its computers?

In most cases, no. Selective enforcement of a 'no nonbusiness use' policy will set the company up for an unfair labor practice (ULP) charge under the National Labor Relations Act when the employer attempts to stop protected activity. For most companies, it's not realistic to prohibit all personal use of e-mail.

What kinds of limits do make sense?

A good policy should expressly incorporate the company's equal employment opportunity and harassment policies to make clear that images, voice and text that are intimidating, offensive, profane or hostile based upon gender, race, color, national origin, religion, disability, age or any other protected status are off limits. The employer's systems should not be used to conduct a personal business enterprise, to spam others, to threaten violence or to express views that could be seen as the view of the company.



Audrey E. Mross
Shareholder
Munck Butrus Carter, P.C.

The systems should be used in ways that are consistent with security measures, which may include prohibiting employees' access to their personal ISPs (e.g., Yahoo, AOL) from employer-provided systems, where such access would thwart firewalls and similar protective measures. Excessive personal use that monopolizes bandwidth or affects employee productivity is another act that could result in corrective action, up to and including discharge from employment.

Can the company be held responsible for its employees' bad acts?

Yes. The doctrine of respondeat superior ('let the master answer') is frequently used to hold employers responsible for the misdeeds of employees while in the course and scope of their employment. Negligence theories are used in cases where the misconduct took place outside of the employees' normal duties.

For example, where an employer had knowledge that a worker was receiving and sending nude and seminude images of his 10-year-old stepdaughter on his workplace computer in order to gain access to child porn sites, the court found negligence and stated that the company had a duty to

further investigate and take prompt and effective action to stop the employee by terminating his employment, reporting him to law enforcement or both (*Doe v. XYZ Corp.*). The court remanded on the issue of whether the child could prove harm from the transmitted photos, but the employer withdrew its petition and the parties settled.

Is there any privacy protection for employees using a company system?

This is an area where unrealistic expectations collide. Employers often think there is no privacy, since the equipment used is theirs. Employees often think that there is privacy, especially where they have a secret password to access the system.

A few years ago, the Texas Supreme Court found an employee did have a reasonable expectation of privacy where the employer provided lockers for storing personal items but allowed the employees to bring their own locks (and not provide the combination or a spare key to the employer). The analogy to company-provided computers and employee-provided passwords is not much of a stretch. Employers must advise employees, in writing, that there is no reasonable expectation of privacy in use of the employers' systems and employers should have written consent. This is normally accomplished by having an electronic communications policy in the employee handbook and securing a signed acknowledgment from each employee. As additional proof of consent (which is an absolute defense to a claim of invasion of privacy), some employers add a 'no privacy' reminder to the log-on screen on computers so the consent refreshes on a daily basis. Employers should also ask for and keep records of employee passwords to undercut privacy arguments and for practical reasons, such as accessing needed information when the employee is absent or has quit.

AUDREY E. MROSS is a shareholder at Munck Butrus Carter, P.C. leading the labor and employment group. She combines prior experience as a human resources professional with the current practice of law to provide preventive measures and practical solutions to employers. She authors a monthly e-newsletter, *Legal Briefs for HR*, which is available on request at amross@munckbutrus.com.

Insights Legal Affairs is brought to you by Munck Butrus Carter, P.C.