Employee Abuse of Technology The Ever-Changing Workplace Challenge
By Carolyn G. Burnette

Technology gone wild! Blogging, instant messages, text messages, e-mail, digital camera phones ... the list just keeps growing. With more employees using electronic communications devices, employers are constantly bombarded with new legal risks and efficiency challenges in their workplaces. Here are some tips on how to protect your organization from legal exposure and reduce the drain on resources.

How is Technology Affecting Workplace Efficiency?
The statistics are stunning. At least one source has reported the following about technology-related issues in today’s workplace:

1. 85.6 percent of employees use office e-mail for personal reasons;
2. 65 percent of Internet usage in the workplace is not work-related;
3. 64 percent of employees have received politically incorrect or offensive emails at work;
4. 20 percent of employees surf the Internet at least 10 times daily; and,
5. 67 percent of employers are using their information technology staff to monitor one or more forms of their employees’ electronic communications.

There is no escaping the obvious conclusion—a substantial amount of employer resources, including work hours and company equipment, are allocated to non-productive efforts each and every workday.

What Are My Employees Doing with Technology?
Some of today’s employees use technology in non-productive ways. One area of concern is ‘blogging.’ The word ‘blog’ is a combination of two words: web and log. A ‘blog’ is a Web site that generally provides informal commentary on subjects such as local news, politics, and entertainment.

Many blogs take on a form similar to a diary with daily, weekly, or monthly entries enlightening the blog visitor on a variety of topics. In addition to comments by readers, many blogs have pictures and links to other Web sites and blogs. Anyone can create a blog, and more and more people are taking advantage of the opportunity to speak their minds and share information. The workplace is not exempt—employees now use the Internet, both from work and at home, to ‘blog’ about their co-workers and employers.

Because blogs can be created and maintained by just about anyone, an employer may find that its employees have their own blogs or visit blogs maintained by their co-workers. These postings are very capable of negatively affecting the workplace, and can lead to legal liability or profit loss. For example, an employee may post trade secrets or other proprietary information, harassing or derogatory remarks about co-workers, or inappropriate or lewd material adjacent to a listing of a company’s name or logo. Certainly, this kind of activity will be immediately disturbing to employers.

Employers also may be concerned when discovering that employees are using blogs to discuss union organizing. Employers should be aware, however, that under the National Labor Relations Act (‘Act’) employees have a right to engage in ‘concerted activity’ for the purpose of collective bargaining or other ‘mutual aid’ or protection. Such activity may be conducted through blogging or other electronic communications. To the extent an employer takes adverse action against employees for such conduct, a retaliation claim under the Act may result.

Another example of how today’s employees are using their employer’s technology in non-productive ways is through e-mail and the Internet. On the one hand, e-mail provides efficiency and convenience, and is inexpensive and instantaneous method of communication. On the other hand, as with blogs, unrestricted e-mail, Internet access and text messaging can negatively impact production and create potential liability. At least one study found that 78 percent of all users accessed the Internet while at work for personal use and entertainment. Accessed sites cover topics such as shopping, sports, chat rooms, job searches and games.

Not surprisingly, some employees use in-house Internet services to access pornographic and other inappropriate sites. Once accessed, these materials sometimes are distributed through company e-mail to other employees in the workplace, resulting in claims of harassment. E-mails also can be detrimental to lawsuits when, for example, former employees are able to produce e-mails from managers or supervisors containing inappropriate content, or communicating a dislike of, or derogatory statements about, a former employee who is suing.

Can Employers Monitor Technology Use in the Workplace to Deter Abuse?
Some employers monitor employee use of technology, both on and off the
job, to stay abreast of abuse, and potential legal exposure. Monitoring, unfortunately, comes with its own set of risks and may result in invasion of privacy and related claims. Moreover, if disciplinary action such as termination results, the termination also may be actionable under various laws.

With respect to monitoring external activity, even when an employer learns through monitoring that its employees are regularly posting harmful information about the company on public Web sites, it can be very difficult for the employer to take any action to stop such postings.

Many states afford employees a constitutional right to privacy or preclude employers from regulating conduct away from work to protect the personal freedom of employees. For example, California Labor Code sections 96(k) and 98.6 preclude employers from discharging or discriminating against employees for lawful conduct occurring during nonworking hours away from an employer’s premises. This protection extends to electronic activity.

Privacy laws may not preclude employers from taking legal action against employees who post trade secrets on public Internet sites or unauthorized use of company logos, particularly if an employee has signed a non-disclosure/confidentiality agreement. Employees who engage in such conduct likely are violating the duty of loyalty and can be sued under these torts. They also may be sued for violating a nondisclosure confidentiality agreement or copyright infringement. In extreme cases where irreparable harm may be imminent to the company, it may be necessary to consider an injunction as an option. Obviously, when disclosure of trade secrets is at issue, the offending employee likely should be terminated.

With respect to internal activity, employers have a greater right to restrict employee use of technology because companies own their equipment, and it is generally understood that the intended use of company equipment is business purposes. These circumstances generally can establish that employees do not have a right to privacy when using an assigned computer or any other technology tool—including e-mail. These principles were affirmed by the Tenth and Ninth Circuits in U.S. v. Barrows and U.S. v. Ziegler, respectively.

When determining whether the plaintiff in Ziegler had a protected expectation of privacy as to pornographic material discovered on an assigned work computer, the Ninth held the employee did not have privacy interest by relying on: (1) the employers’ computer use policy prohibiting personal use of the systems; (2) a policy giving notice that work computers would be monitored; and (3) the fact that the equipment was owned by the company. The court acknowledged, however, that the employee did establish a subjective expectation of privacy as evidenced by password protections and a locked office door. This subjective expectation of privacy was not sufficient to afford a protected privacy interest.

In Barrows, the Tenth Circuit similarly found that, if the computer at issue is personally owned by an employee, this will be an important factor in determining privacy interests as to the electronic content. However, once a personally-owned computer is connected to a company-owned network and the equipment is placed in a publicly-accessible area without any password protection, any privacy interests can be negated.

To avoid any doubt about an employer’s right to monitor and inspect company equipment, employers must take heed of the lesson in Ziegler and adopt clear written policies addressing the use of technology in the workplace.

What Are the Key Elements of an Effective Electronics Communications Policy?

Developing a comprehensive electronics communications policy is perhaps the best tool for avoiding potential risks associated with the Internet, blogs, text messages, e-mail, and other electronic media. Employers should include a number of provisions to ensure the policy is comprehensive and binding.

First, the policy should apply equally to all forms of electronic communications. It should include a provision that use of company computers, Internet access, e-mail and other electronic devices is primarily for business purposes. Given the practicality that some personal use of the Internet for convenience is inevitable, and to avoid a claim of discrimination that could result from “cherry-picking” which employee violations are enforced, it may be best to include some limited provision for occasional personal use. This is also required by recent decisions of the National Labor Relations Board.

Second, the policy should advise employees that the technology is owned by the company, and that computer and e-mail use will be regularly monitored. The policy should clearly advise employees that they should not have any expectation of privacy with respect to any personal or business use of assigned equipment. To avoid giving a litigant the opportunity to show the policy is a pretext, the company should comply with the policy and monitor computer use on a regularly scheduled basis and company-wide.

Third, the policy should include provisions prohibiting discriminatory, lewd, defamatory or other offensive communications about the company, superiors, coworkers or competitors. Employers should be reminded that, when using company technology, they must comply with all other company policies, such as policies against sexual harassment and discrimination.

Fourth, a comprehensive electronic communications policy should
additionally employees that they can be disciplined or terminated for violating the policy. Employers should then have employees acknowledge in writing they have received, read and understand the policy. To avoid litigation, employers also should keep in mind that an electronic communications policy—like all company policies—must be equally and consistently administered and enforced among all employees and across all types of electronic communications.

Finally, to address at least some of the concerns about employees posting negative blogs about the organization from their homes, employers should require that employees sign non-disclosure/confidentiality agreements. Doing so will at least protect against and discourage employees from posting trade secrets and other proprietary information.

Employers also should adopt a “blogging policy.” The policy should suggest that employees specify in their blogs that the views expressed are their own, not the employer’s. The policy also may include that the organization will not indemnify employees who are sued for at-home Internet activity. These small steps could be worth their weight in legal protection.

Carolyn G. Burnette is a partner at Shaw Valenza LLP, a boutique employment law firm with offices in California. Her practice is focused on representing corporate and other employers in state and federal court litigation, conducting workplace investigations and advising clients on a spectrum of workplace issues.