TO SPY OR NOT TO SPY

David Walton

To spy or not to spy on your own employees? That is the question facing many employers today. And, increasing numbers of companies—facing concerns ranging from data security to trade secrets—are saying "yes" to employee surveillance. Here's a look at the current surveillance landscape, the case for watching your employees, and how you can protect yourself from claims of improper monitoring.

THE STATS

Every year since 2001, the American Management Association (AMA) has conducted a survey on electronic monitoring and surveillance. In the 2007 survey, 45% of the responding employers indicated they monitor employee Internet *and* computer activity, including keystroke monitoring. Of these companies, 60% conduct this monitoring on an ongoing or routine basis.

Monitoring the Internet is the most common form of surveillance, with 66% of the respondents saying they monitor employees' Web site access and Internet usage. Almost two-thirds of these employers use software to block an employee's access to specific sites. This is a 27% increase from 2001. About 40% of the employers store and monitor employee computer files; 46% of these employers characterize this type of monitoring as ongoing or routine.

Similarly, 43% of the employers in the survey monitor their employees' e-mail messages. Of these employers, 96% look at internal and external messages, and 58% check internal messages only.

What's more, the growth of software to conduct this type of monitoring has boomed over the past couple years: 73% of the employers said they use some type of software to monitor emails. But 40% of the employers eschew software and instead assign at least one individual to manually read and review e-mails. In a somewhat surprising revelation, 73% of the employers said that IT personnel conduct this surveillance, while only 34% indicate that their HR department did the surveillance. This last point raises a host of potential liability issues that will be discussed below.

Video surveillance is also still a popular form of monitoring. About half of the employers surveyed use video surveillance to prevent crime, violence, and sabotage. But only about 7% of those companies surveyed utilize video to monitor employee work performance.

With the growth of satellite technology, 11% of the employ-

Cozen O'Connor labor & employment attorney DAVID WALTON represents a broad range of clients, from large multinational corporations, to small companies—litigating matters involving non-competes, restrictive covenants, trade secrets, fiduciary duties, and discrimination claims, and assisting employers facing challenges posed by the information-age economy. Vice-chair of the firm's E-Discovery Task Force, Walton recently won a $7 million jury verdict on behalf of a U.S. company whose trade secrets were stolen by former employees. Contact him at dwalton@cozen.com or 610-832-7455.

ers use satellite-based systems to track their employees. Most of this monitoring is accomplished through GPS systems on company vehicles or employer-owned cell phones.

THE CASE FOR SURVEILLANCE

So, why is all of this monitoring going on? There are many perfectly legitimate reasons for employers to conduct surveillance on their employees.

False Claims for Workers' Compensation/Disability

For decades, employers have relied on surveillance to root out malingerers in workers' compensation cases. This typically involves the use of private investigators to take video of or record personal observations of an employee's off-duty but public activity. The purpose is to find out if an employee claiming an injury is really hurt or is trying to improperly collect workers compensation or disability benefits. This also has been used to investigate whether employees are engaging in improper moonlighting activity. In addition, it's not unusual for large corporations to have their own departments dedicated to monitoring their own employees. Sometimes these resources are used to ferret out employees who are improperly leaking information to the press or to your competition.

So long as the monitoring focuses on public conduct, it's generally legal, as individuals don't have an expectation of privacy here. An example of this is the recent opinion in *Vail v. Raybestos*.[1] There, an employee claimed that she needed intermittent FLMA leave for an injury. The employer suspected that the employee was actually using this time to help her husband run his lawn-mowing business. The employer hired a private investigator to tail her. When she was allegedly caught cutting lawns during her FMLA leave, she was fired. Despite the employee's privacy objections, the Seventh Circuit Court of Appeals found there was nothing illegal with this type of monitoring and upheld the termination.

This type of surveillance, however, still may be dangerous for employers. Over-zealous investigators might get employers in a lot of trouble. So, it is very important for employers to have the right checks and balances in place if they are going to conduct this type of monitoring.

Work Performance

Employers have also effectively used surveillance to monitor—and hopefully improve—the performance of employees who work in the office or telecommute. It's now easier than ever to employ different technologies to conduct this kind of surveillance, with current software allowing employers to view workers computer screens in "real-time," and, for example, see if employees are working enough while they are at home.

However, employers should carefully engage in this monitoring, providing a legitimate business reason for surveillance, especially for employees who telecommute. For example, for certain types of job, it is reasonable to use this type of monitoring to make sure that employees are entering data correctly or are otherwise performing their certain tasks the right way. And, it is vital that employees receive notice—preferably in several different forms—that the company may engage in this type of monitoring.

Data Security

Most IT people will tell you that the greatest threat to their data lies within—from their own employees. Not surprisingly, many companies monitor e-mail and Internet use to prevent the introduction of computer viruses to their systems—costing organizations millions each year. This is a basic type of monitoring that all companies should employ to substantially decrease this threat.

Trade Secrets and Confidential/Proprietary Information

Almost anyone can buy a multi-gigabyte flash drive literally storing millions of pages of information. This poses a great threat to the sanctity of an employer's trade secret and confidential/proprietary information. To protect this information, many employers monitor an employee's e-mail and Internet usage, while some also examine that individual's access to certain highly confidential and sensitive information on a server. In fact, alerts can be set up to notify companies when certain documents/servers are accessed.

It is also possible to monitor an employee's VPN or Citrix access during non-working hours. If a worker is suddenly obtaining highly sensitive information from home, especially at odd hours, the employer should look into it.

The same is true for e-mail monitoring. Employers can look at e-mail to ensure that employees are not sending highly sensitive and confidential material—like client lists—to their homes.

Again, this could be a sign that the employee is getting ready to depart with the information for a competitor.

What's more, employers can watch an employee's physical access to the worksite through key card or smart cards access systems. This type of surveillance can be helpful to ensure that workers are not engaging in late night office visits to hide their preparations to leave, or to steal trade secrets and confidential information.

Again, with this type of monitoring, it is vital that the company notifies all employees that they are subject to this type of surveillance.

Legal Liability

Companies also monitor to decrease their legal liability. Over the past several years, numerous harassment suits have been filed based on the improper use of the Internet and lewd e-mails. Proactive employers now monitor to ensure that their workers are not misusing the employer's Internet or e-mail systems.

Despite the notoriety of these suits, employees still abuse the Internet for prurient purposes. More than one-fourth of the employers in the AMA survey have fired employees for e-mail misuse, including violation of any company policy (64%); inappropriate or offensive language (62%); excessive personal use (26%); breach of confidentiality rules (22%); and other miscellaneous issues (12%).

And, 30% of these employers fired workers for Internet misuse, including viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); and other miscellaneous issues (9%).

You would think that all employees would understand that they cannot get away with this type of misconduct. However, the AMA survey suggests otherwise. Thus, employers should also monitor their employees' access to Web sites. Employees should not be permitted to use employer equipment to surf sites that are sexually explicit, violent, or otherwise objectionable.

Employees should also be prohibited from transmitting material that is hateful, hostile, abusive or is racially, sexually, religiously, or otherwise biased against certain individuals. This type of conduct must be eliminated from the workplace entirely, including the employer's technology. Monitoring is one way to make sure this happens.

In addition, with e-mail becoming the focal point of jury trials as the most common type of exhibit, surveillance is vital. Proactive employers understand this point, and perhaps have learned this lesson the hard way. No one enjoys being burned by their own e-mail at trial. So, many companies now monitor e-mail usage to verify employees are representing the company's interests in a professional and accurate manner. Workers should be trained not to use any language that is offensive or could imperil the company's image. Before writing any e-mail, employees should assume that it will be read by 20 outsiders. All e-mail must be drafted with this in mind.

The Unpredictability of Blogs and Social Networking

Despite the growth of blogs and social network sites, most employers do not monitor these sites or activity. In fact, only 12% of the employers from the AMA survey monitor blogs to review what is being said about the company, and only 10% look at social networking sites.

But, blogs and social networking sites present challenges for employers. Employees can release damaging information about the company, or divulge highly sensitive and confidential information to the entire Internet. Even in defending their company, workers can inadvertently reveal information about the company's finances, triggering insider trading liability issues.

While employees in the private sector have little protection for blogging and related activities, employers cannot discriminate against them for blog use. In other words, employers must fire all similarly situated employees the same way—i.e., you shouldn't fire a worker who is over 40 years old for blogging, when younger employees who engage in similar conduct are not terminated.

Similarly, any punishment for blogging must not violate the anti-retaliation protections of state and federal law. Before imposing discipline for blogging, employers must ensure that the conduct at issue is not protected under a state or federal statute. Examples of federal statutes with anti-retaliation protection include: Title VII, Sarbanes-Oxley, OSHA and numerous environmental statutes. There are also issues under the NLRA for protected concerted activity.

Companies must also be careful when disciplining employees who

blog on their own time and own computers. Some states, including California, New York, Colorado and North Dakota, have posted laws protecting employees' conduct outside the workplace. While many of the statutes are not specifically designed to cover blogging, they can be used to protect workers who engage in blogging from being terminated for that conduct, so long as they do it on their own time.

LEGAL GROUNDS

Is all this monitoring legal? The short answer is yes—if done the right way.

Currently, the law heavily favors an employer's right to conduct workplace monitoring. There is no specific constitutional right to privacy in private employment. The Electronic Communications Privacy Act (ECPA) is the closest federal law that relates to employee monitoring, prohibiting the interception of certain communications, including electronic communications. ECPA focuses on contemporaneous interception of communications, and therefore does not apply to stored e-mail communications because they are not sent and intercepted at the same time.

The ECPA also has an exception for interception that occurs in the "ordinary course of business," making it easier for employers to conduct employee monitoring that would otherwise violate the Act. Many states have adopted versions of the ECPA, with similar interpretations.

Most of the lawsuits regarding employee privacy are governed by the common law right to privacy. These torts are premised on the employee's reasonable expectation of privacy. According to most courts, employee monitoring is perfectly legal, so long as the employee does not have a reasonable expectation of privacy. There are several questions companies need to ask to determine this, including:

- Is conduct taking place in public or at the employer's premises?
- Is the employee using company-owned equipment?
- Did the employer give notice to employees that their activities would be monitored?

Once these are answered, how can an employer make sure that an employee does not have a reasonable expectation of privacy? Most importantly, the company should alert employees that they could be monitored in specific activities. Only two states, Delaware and Connecticut, require employers to give employees notice regarding their monitoring activity. However, according to the AMA study, most employers give this notice even though it's not specifically required. Over 80% of employers inform workers that the company is monitoring content, keystrokes, and time spent at the keyboard and let employees know the company reviews computer activity. More than 70% of the same employers alert employees regarding e-mail monitoring.

Even if not legally required, companies should be open about their monitoring activities. Workers who file lawsuits for invasion of privacy will have a tough time arguing that their privacy was compromised when they had fair notice, for example, that their employer may monitor all of their e-mail communications.

Notice must—at minimum—be in writing. Employers should establish clearly written policies regarding Internet use at work, and the use of company provided e-mail and company-owned computer equipment, including cell phones, PDAs, Blackberries, and, of course, laptop computers.

The policy should include a warning addressing the potential discipline for violations of the policy, in addition to clearly outlining that the employer has the right to monitor an employee's e-mail and Internet computer usage. If a company plans to conduct keystroke tracking, workers should be given notice of this as well.

If an employer gives proper notice to employees, can it still get in trouble? Yes, by violating company policies and establishing a practice that leads employees to believe that their personal use of an employer's equipment will not monitored. For example, in *Quon v. Arch Wireless Operating Co.*,[2] the employer gave cell phones to employees to use. In this case, the employer did not have an official policy for text messaging. It allegedly told the employee that he could use his pager devices for personal use if he paid overage charges. The Ninth Circuit found that this created an expectation of privacy for employees who used the pagers to send personal text messages.

To avoid a situation like the employer in *Quon,* the key is to ensure that it's clear to all workers that personal use of the employer-owned equipment, like cell phones, PDAs and laptops, is forbidden or that any such use is

subject to monitoring. Otherwise, employees may have their privacy protected.

SENDING THE RIGHT MESSAGE

When deciding whether or not to conduct certain surveillance, it is important to be aware of what a potential jury would think. Although most cases never go that far, it's critical for employers to begin with the end in mind. This helps ensure that employers do not find themselves in a tough situation where they have to pay an unreasonable settlement to avoid a jury.

Thus, companies should think how they would try to justify their surveillance to twelve average people off the street. Make sure there is a cogent business interest for the surveillance. Most jurors are not employers, but employees who want to make sure that "Big Brother" does not rule the workplace. They will sit in the jury box initially favoring the employee.

So, send the right message about monitoring practices. Always be upfront about your policies and do not monitor for the sake of monitoring. Make sure your company has the checks and balances to control against excessive employer use of monitoring technology. And, when deciding whether to engage in monitoring that is aggressive, always make sure you ask yourself: "What would a jury think?"

■

NOTES

1. Vail v. Raybestos Products Co., 533 F.3d 904, 184 L.R.R.M. (BNA) 2718, 13 Wage & Hour Cas. 2d (BNA) 1537, 156 Lab. Cas. (CCH) P 11060, 156 Lab. Cas. (CCH) P 35457 (7th Cir. 2008)
2. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 27 I.E.R. Cas. (BNA) 1377, 91 Empl. Prac. Dec. (CCH) P 43233, 155 Lab. Cas. (CCH) P 60628 (9th Cir. 2008).