



## HR Must Know When Employee Surveillance Crosses the Line

*The debate over Internet monitoring at work rages on, and HR not only must know the issues, but should be part of the decisions on whether (and how) to monitor.*

**By Eilene Zimmerman**

---

John Fox is a senior technical analyst at Sapphire Technologies, an IT placement firm in Woburn, Massachusetts. He's the man to call when the server is down, the network fails, or the system crashes. He's also the guy to call if someone at the company is sending harassing e-mails or viewing porn sites.

Fox is Sapphire's tech-enabled Big Brother. A year and a half ago, the company installed both e-mail and Internet monitoring systems from Elron Software in Burlington, Massachusetts. The e-mail product, Message Inspector, is set up using triggers -- certain words, video files, or attachments -- that, when detected, forward the message immediately to Fox for review. The Web component of the monitoring system automatically blocks graphically explicit sites, and if an employee tries to go to a blocked site, Fox is notified. Using parameters given to him by human resources, essentially to block hardcore porn and violence sites, Fox can veto the block, which sometimes occurs automatically because a certain word, say "naked," appears on a Web page too many times.

---

**"If you find that someone who never works after 6 p.m. is suddenly showing up at the office in the middle of the night and going online, that should raise eyebrows."**

---

The majority -- 57 percent -- of U.S. companies now monitor their employees' e-mail and Internet use, according to IDC, a technology research and analysis firm in Framingham, Massachusetts. And the number is expected to rise substantially in the next couple of years. Large companies are more likely to monitor their employees than small ones: at the end of 2001, 70 percent of firms with 1,000 or more employees had implemented electronic monitoring systems. For companies of any size, the decision on whether or not to read an employee's e-mail and monitor his or her Internet activity is highly emotional and intensely controversial.

Employers say they monitor to increase productivity and to protect themselves from potentially disastrous computer viruses, harassment lawsuits, and leaks of confidential information to competitors.

An IDC survey conducted in the fall of 2001 reports that 48 percent of the employers who monitor employees say that their intention is to protect against viruses and the loss of information; 21 percent as a way to limit legal liability.

Many employees, privacy rights experts, and workers' rights advocates, however, are angered and offended by the monitoring trend. They argue that privacy is a guaranteed human right -- at home and at work. They say workplace monitoring is an unnecessary infringement on that right. A recent Privacy Foundation study found that 14 million U.S. workers are already subject to continuous monitoring while online. The nonprofit Denver-based organization studies communications, technologies, and services that may pose a threat to privacy.

Lewis Maltby, president of The National Workrights Institute Inc., in Princeton, New Jersey, says the most frequent complaint his organization hears from workers is that employers don't distinguish between personal and workplace communications. "They look at everything," he says.

George Baroudi is vigorously opposed to the use of electronic monitoring. He is chief technology officer and an Internet security expert at iLabyrinth, a company that develops network security systems headquartered in Hockessin, Delaware. "The Internet is a tool for learning, not a way to invade privacy," he says. "Just as the United States Postal Service is permitted to deliver your mail but not open it, e-mail is the property of the recipient, not the message carrier."

Proponents of monitoring challenge that point of view, and insist that they are only looking at e-mails that signal a problem -- such as sexual harassment or a predilection for child porn, and are not endorsing personal snoop squads.

For many corporate decision-makers, a potential violation of privacy rights and the possibility of stunting creativity are minor concerns compared to the advantages of monitoring. That's why the market for monitoring and filtering software is growing by about 36 percent a year, and revenue in the industry is expected to triple in the next three years, according to IDC.

Although companies have different reasons for monitoring, Fox says Sapphire began the practice as a way of preventing potential legal problems. If one employee makes allegations about another employee's behavior, for example, checking e-mail correspondences can substantiate the charge.

Fox notes that, despite company warnings, three people at Sapphire have been fired for spending time surfing adult-oriented Web sites. The company reminds its 350 employees that they are being monitored each time they log on to the network. Fox says that no one

has quit because of the monitoring, and that he has heard only a few complaints from employees about violations of privacy rights. "Generally, people know that if they aren't doing anything wrong, they have nothing to worry about."

Bart Lazar, a partner in the high-tech group at the Seyfarth Shaw law firm in Chicago, says smart employers do monitor e-mail and Internet use in "some way, shape, or form." Lazar was lead counsel for GeoCities in 1998 in the country's first Internet privacy suit. The Federal Trade Commission sued GeoCities, arguing that the company took consumer information collected on its Web site and disclosed that information to a direct mail marketing company. (GeoCities eventually settled with the FTC.)

Lazar advises his clients -- which include Fortune 1000 companies in the financial services, high- and low-tech manufacturing, media and education industries -- to use filtering or monitoring systems. Many do, largely to protect computer systems from viruses and junk e-mails, some of which could be offensive to certain employees, prompting hostile-work-environment lawsuits.

Employers also use monitoring to protect trade secrets and prevent other proprietary information from getting out. "Suppose you're a loyal employee in a chat room on the Internet and you see someone bashing the company's profits," Lazar notes. "The employee sends a message saying, 'No, you're wrong. In fact, we're about to announce our best quarter ever.' Well-intentioned sure, but what they did is illegal."

Nancy Flynn, founder of the ePolicy Institute in Columbus, Ohio, and author of [\*The ePolicy Handbook\*](#) (AMACOM, 2001), says a company can also set up its monitoring system to alert management to suspicious behavior. "If you find that someone who never works after 6 p.m. is suddenly showing up at the office in the middle of the night and going online, that should raise eyebrows. Why is this employee online? Is she downloading proprietary information?"

Even if employees aren't conversing in chat rooms, leaking trade secrets, or furtively looking at porn, they may be active recreational surfers, day traders, or radio listeners who are wasting a lot of company time and bandwidth.

Judi Epstein, product manager for iPrism, an Internet monitoring and blocking system from St. Bernard Software in San Diego, says her clients typically find that an employee goes online for business purposes and then gets unintentionally sidetracked, sometimes for a few hours. "At other times it is intentional," Epstein says. "At my last job, I worked with a woman who ran a side business on eBay Inc. while at the office -- eight hours a day."

For all of the pros and cons, knowing what electronic monitoring systems cost and how much money they save is an obvious concern. But is it possible to figure out the ROI of monitoring software?

---

**"All sorts of problems arise if you do monitor. Workplace studies on productivity show a detrimental effect on employee morale and an increase in employee stress"**

---

Vendors such as iPrism say yes. Companies use gains in productivity to calculate the ROI, Epstein says. iPrism's software, for example, costs about \$20 per employee per year, or about a nickel a day. Websense, a provider of Internet blocking and monitoring software located in San Diego, cites the same cost for its product. Vice president of marketing Andrew Meyer says the firm's research shows that the average employee spends about three hours a week on personal surfing. If monitoring helps cut that wasted time down to one hour, and the average employee earns about \$20 per hour, the investment in Websense is paid back in a week.

Epstein is, of course, an advocate of monitoring. Still, she says the majority of workers who use the Internet are not overtly malicious. Most of iPrism's clients still allow their employees a lot of latitude in using the Internet, she says.

Even the most vociferous proponents of corporate snooping agree that the rules and morality now governing electronic monitoring are far from clear. Bruce Kasanoff, a former partner at marketing consultancy Peppers and Rogers Group and author of *[Making It Personal](#)* (Perseus, 2001), finds electronic monitoring frightening. His book discusses how technology enables companies to play Big Brother.

He is concerned not only about what companies are doing today, but also about what they will be able to do in the very near future. In the next year or two, states will begin implementing a system called e911, which will require cell phones to send the location of a call to their phone-service carrier. Pinpointing the location of a cell phone user in the event of an emergency could save lives, but the technology could be used for more ominous purposes.

"Today companies read what you write in e-mails, where you go on the Web," Kasanoff says. "Two years from now they will be able to track, for example, where their salespeople go and what they do. Where will it end?"

Many of these same concerns are receiving a great deal of attention in board-rooms and courtrooms. In May, Federal Appeals Court Judge Alex Kozinski and other judges ordered the shutdown of software that tracked the online activities of all employees in the Ninth Circuit Court of Appeals. In an open letter to federal judges published in the *Wall Street Journal* on September 4th, Kozinski likened the monitoring of judiciary employees to the treatment that prison inmates receive. "The proposed policy tells our 30,000 dedicated employees that we trust them so little we must monitor all their communications...How did we get to the point of even considering such a draconian policy?"

In September, the Judicial Conference of the United States, which sets policy for the courts, approved a revised version of the monitoring program, allowing only limited tracking of Web surfing and no e-mail monitoring.

Chris Hoofnagle, legislative counsel for the Electronic Privacy Information Center in Washington D.C., hopes that because the judges themselves want privacy, they will be more apt to uphold privacy rights

in worker-versus-employer cases coming before the courts. Regardless of a company's position on monitoring, he says, it's still imperative that all businesses have a written Internet-use and e-mail policy and that they notify employees regularly if monitoring occurs.

"Right now the law heavily favors employers' right to monitor," he says. "But all sorts of problems arise if you do monitor. Workplace studies on productivity show a detrimental effect on employee morale and an increase in employee stress."

A Websense random survey of U.S. companies conducted last fall found that one third of those surveyed had fired an employee for Internet misuse; and over 60 percent had disciplined an employee.

Andrew Schulman, chief researcher with the Privacy Foundation, says employers falsely defend the use of electronic monitoring by saying it protects the company against lawsuits. But in all the hostile-work-environment cases he has seen, none began with an offensive e-mail. Instead, they started as sexual-discrimination cases in which female employees were not promoted but male employees were. "And as one piece of evidence used to show gender bias, the women's lawyer says, 'Look, this guy thinks it's funny to trade e-mails with his buddy about why beer is better than women.' But the lawsuit wasn't triggered by the e-mail," he relates.

Attorney Ann Kiernan is a solo practitioner in New Brunswick, New Jersey, who specializes in preventive law for employers and is also one of the principals in Fair Measures Corporation, a group of attorneys who train executives and managers on how to prevent employee lawsuits. She says that monitoring may actually *increase* a company's potential liability. Right now, the law states that employers aren't liable for harassment unless they are made aware that harassment is occurring. Once the company becomes aware of the problem, it must take prompt corrective action. But if a company monitors employees, Kiernan says that business assumes responsibility for everything it sees and everything it monitors on the Internet, whether an employee brings it to the company's attention or not. "You suddenly have a duty to investigate everything," she says.

Schulman and other privacy-rights advocates say electronic monitoring may be warranted in specific cases if there is suspected wrongdoing, but that monitoring should always be used as narrowly as possible to prevent abuse and misuse.

A reoccurring problem is that companies often make a snap decision about how they are going to use monitoring software. One story circulated by analysts and researchers tells of a CEO who read a Sunday newspaper article linking lost productivity at work to too much Internet use. Convinced that it was a problem at his own company, the CEO took the article to work on Monday and went straight to IT -- rather than HR -- and ordered the department to immediately install an electronic-monitoring system.

The story also is a reminder of why HR -- and not IT -- should be responsible for creating a monitoring policy and carrying it out. "When you have the IT department saying to the CEO, 'Everyone is doing all this browsing on CNN and we have to put a stop to this,' you have the cops making the laws, and that's not good," says Bill Gassman, research director for Gartner, a business consulting firm specializing in IT infrastructure operations.

It's also problematic to ask employees to give informed consent to a policy of surveillance when they aren't able to view the data collected about them. Schulman says if they can't see the data, they can't verify that the information is accurate.

One service -- FastTracker -- puts out reports that resemble a telephone bill and allow employees to see their own usage. FastTracker, a product of Fatline Corporation in Boulder, Colorado, analyzes its clients' Internet traffic and sends reports back to the company for examination by both management and employees.

When employees have access to their own Web usage statistics -- where they've been and how long they were there -- they become responsible for managing their own time, says Bob Silk, FastTracker's vice president of sales. "When you block sites, you treat employees like children. You don't give them any responsibility. Our product makes each employee responsible for his or her actions."

Ultimately, an employee who wants to break the rules will break the rules, those close to the issue say. Sexual harassment was occurring long before the Internet existed, and confidential information can just as easily leave a company in a face-to-face conversation as it can in an e-mail.

Attorney Ann Kiernan says she thinks employers who e-monitor should ask themselves why they don't also monitor phone calls, mail, and faxes.

"How much time do you, as an employer, want to spend policing your employees?" she asks. "From a practical point of view, isn't it better to have someone who is skilled in information technology or human resources doing something productive, rather than playing nanny?"

*Workforce*, February 2002, pp. 38-45