



JULY 22, 2003

SPECIAL REPORT: SAFEGUARDING PRIVACY

Ever-Sharper Eyes Watch You Work

Corporate monitoring of employees' e-mail, Web surfing, or behavior in general is getting more sophisticated -- and widespread

On July 10, Jeanne Phillips, who writes the syndicated newspaper column Dear Abby, printed a letter from a staffer in an unnamed corporate technology department who, while monitoring his company's systems, has seen the savings-account balances of fellow employees, tracked their bids on auction site eBay, and noted which Web sites they frequent. He has also read their e-mail, which ranged from mundane to entertaining to graphic, complete with descriptions of the sender's personal dimensions. "I will never look at certain employees the same way again," he wrote.

Most corporations have recorded their employees' phone calls and e-mail, and videotaped their movements for years. A recent survey by the American Management Assn. (AMA) found that 52% of 1,100 respondents believed their employers monitor e-mail, up from 47% in 2001. The actual number could be higher, since 13% of the people surveyed didn't know whether they were being watched or not.

Most likely, they are: Companies today are gathering more and more data on their internal processes and the people who manage them -- thanks, in part, to new government regulations such as the Sarbanes-Oxley Act. That law, which will take effect next summer, will require publicly traded companies to keep track of which employees have looked at sensitive documents, for example -- all in the name of helping ensure the accuracy of financial reporting.

NOT "OUT HUNTING"? In addition, Corporate America is becoming increasingly aware of the huge threat wayward employees represent. About 70% of attacks on corporate computer systems come from the inside, according to e-Security, a Vienna (Va.) supplier of corporate security systems. This can be something as simple as a disgruntled travel-agency employee canceling dozens of client tickets or an alienated marketing manager erasing valuable customer data. The costs of such mischief, while often unreported, tend to exceed losses from external attacks -- which ran to \$202 million at 500 companies surveyed this spring by the FBI and the Computer Security Institute in Southampton, Pa., an association of technology professionals.

The good news for employees is that as the amount of information collected snowballs to unmanageable levels, many corporations are starting to look for alternative methods of surveillance. After the layoffs of the past two years, most info-tech departments are spread too thin as it is. Plus, most companies "don't feel that [snooping] is warranted," says Robert Richardson, editorial director at the Computer Security Institute. "Most places don't go out hunting."

Instead, many companies are turning to more effective -- and less obtrusive -- ways of uncovering internal threats: statistical analysis, employee surveys, and software that guards sensitive documents and systems. Privately held Boston startup Verdasy's has developed software that guards closely held information, such as customer data. The product, which is due to start beta-testing in August, keeps a journal of people who look at a file.

SCREEN-SAVER DEFENSE. It also reports if a person prints out the information or burns it onto a CD. "Our customers want to move on to security activities that have more of a direct impact on their business" than sifting through all workers' correspondence, says Verdasy's CEO Seth Birnbaum. "I see customers becoming more practical."

Another approach is to control access to an organization's information systems. e-Security sells software that makes sure all corporate computers have a password-protected screen saver enabled. The screen saver turns on whenever the PC stays idle for 20 minutes, and that helps protect the system from unauthorized access during lunch hours and on weekends. "Most

organizations care about their assets and aren't looking to track their employees' behavior," says Joseph Payne, president and CEO of e-Security.

In fact, employee behavior can be now tracked with statistical-analysis software without invading privacy unnecessarily. Privately held startup Stone Analytics in San Diego uses such analysis to detect unusual patterns in data collected from e-mail systems and Web logs, among other applications. Such patterns could raise a red flag -- leading to further investigation -- if, say an employee were to blast 10,000 e-mail messages from a company account or try to log into the system with the wrong password 100 times in one day, explains CEO Christy Joiner-Congleton.

SEE AND TELL. The product, which is already used by the government and by private clients, helps identify problems before they occur, says Paul Proctor, vice-president for security and risk strategies for IT consultancy Meta Group. "We view this as the next evolution of monitoring," he adds.

Some of the methods being used even rely on employees to divulge what they see around them. Every week, privately held eePulse in Ann Arbor, Mich., sends out two to three questions, plus space for comments, to 30,000 to 40,000 employees at clients such as General Motors ([GM](#)). It then aggregates the anonymous answers for its clients' middle managers to peruse.

Employees complain of everything from dirty bathrooms to a co-worker who brings a gun to work. Then their managers, who receive the results of these anonymous surveys, have to provide upper-level execs and the employees with a list of actions that rectify the problem, explains eePulse CEO Theresa Welbourne, a human resources professor who bases the surveys on 17 years of her own research.

PREVENTIVE MEDICINE. The results speak for themselves: GM, which has used eePulse for two years in its Parma (Ohio) metal-fabrication plant, has found that employees have begun feeling better about their jobs, says Jay Wilber, executive director of Quality Network at GM. More important, they "are coming up with ideas to improve the business," he says. "You'll get enough good ideas to offset the cost" -- ranging from \$24 to \$120 per employee per year, depending on company size.

And when it comes to uncovering problems, "eePulse would be much more effective than an invasive tactic," Wilber says. He adds that GM doesn't use video cameras to monitor its employees.

Finally, many companies opt for blocking unwanted behavior instead of monitoring it, says Andrew Meyer, vice-president for marketing at Websense ([WBSN](#)), a San Diego company that sells software used for managing employees' Internet usage. Its software stops workers from going to so-called spyware sites, which gather user information without a visitor's knowledge and can scan hard drives. The software also blocks employees from downloading hacking tools onto the company network.

"CULTURE OF TRUST." This kind of protection will gradually become more widely used, believes Dan Geer, chief technology officer at security consultancy @Stake in Boston. Today, most companies protect their systems from incoming threats -- but don't prevent viruses from leaving their systems and infecting those of partners and customers. Such negligence could damage relationships, and Geer expects corporations to address this problem soon. The solutions can be as easy as screening outbound messages for viruses.

The goal at many companies is to avoid making employees feel like inmates. "There's a culture of trust and respect for individuals in our organization," says Michelle Gaines, IT manager for the Port of Portland, which maintains a number of marine terminals, airports, and business parks in Oregon. And she wants to keep things that way. So the port doesn't monitor the contents of its employees' e-mail, and if it ever did, it probably would be only to block incoming spam, she says.

What's more, most companies don't mind limited personal use of the Web. Half of Websense's clients set up the software to allow 30 minutes a day for employees' personal business, such as opening e-mail, checking stock quotes, or shopping. The rest of the time, these sites are blocked. Following recent layoffs, workers now end up bringing work home -- and it's only fair to allow them to bring some personal business to work, says Lewis Maltby, president of the National Workrights Institute in Princeton, N.J. About 90% of the AMA survey respondents report that they receive or send personal e-mail at work.

SPARING THE INNOCENT. Of course, many companies in highly regulated industries such as health care and the financial sector will continue to become more vigilant. Also, companies will keep zooming in on employees suspected of committing fraud. So, workers would be kidding themselves if they expect to ever have more on-the-job privacy than they do now. "I don't think [companies] are monitoring without using the information," observes Matthew Finkin, labor law professor at the University of Illinois.

Still, corporations can pinpoint the bad guys without making staffers feel like felons, in part by better educating employees on corporate rules. Today, a surprisingly small 71% of companies have written policies concerning e-mail, for example -- down from 81% in 2001, according to the AMA.

In her reply to her Dear Abby reader, Phillips expressed hope that employees will become more aware of -- and more leery of -- workplace monitoring. That's bound to happen given the extent to which companies are watching every step workers take.

By [Olga Kharif](#) in Portland, Ore.

[Advertising](#) | [Special Sections](#) |
[MarketPlace](#) | [Knowledge Centers](#)

Xerox Color. It makes business sense.

[Terms of Use](#) | [Privacy Notice](#) | [Ethics Code](#) | [Contact Us](#)

The McGraw-Hill Companies

Copyright 2000- 2008 by The McGraw-Hill Companies Inc.
All rights reserved.