



Powered by 

Employers look closely at what workers do on job Advertisement

Updated 11/7/2006 10:15 PM ET

By **Stephanie Armour**, USA TODAY

Employers have long warned their workers that company e-mail, Internet use and even phone calls are subject to monitoring.

But what many employees don't realize is that spying is going high-tech. In the spirit of James Bond wizardry, companies are tracking workers' whereabouts through Global Positioning System (GPS) satellite, implanting employees with microchips with their knowledge and hiring private investigators to check up on what employees are really doing at work.

Hewlett-Packard became embroiled in a spying scandal after being accused of hiring private eyes to spy on its directors, sending computer spyware to reporters and probing private phone records to ferret out boardroom leaks.

The developments suggest that a Brave New Workplace is here. Employers in today's highly competitive and lawsuit-driven work environment are monitoring employees with unprecedented zeal.

Marc Rotenberg, executive director and president of the Electronic Privacy Information Center, a public interest research center in Washington, says many companies have legitimate and legal reasons for such monitoring, but gumshoe tactics also can erode trust as employers become suspicious of their own staff.

"It raises questions of trust, but in fairness to employers, they have an incentive to be sure employees are doing their jobs," Rotenberg says. "We're more concerned that people are entitled to some privacy. Where do you draw the line?"

While more employers may feel they have justifiable reason to pry, others believe the practice is too corrosive to the employee-employer bond. Chuck Rauenhorst, CEO of Minneapolis-based Rauenhorst Recruiting, says monitoring employees is not something that he would do.

"Colleagues who trust one another have synergy and work better as a unit," Rauenhorst says in an e-mail. "Eavesdropping, electronic or otherwise, is always going to tear that fabric of trust."

The surveillance of employees has become increasingly commonplace, research shows. Already, 76% of companies monitor employees' website connections, and 65% block access to specific sites, up from 40% in 2001. About 35% track the content, keystrokes and time spent at the keyboard, according to the 2005 study by the American Management Association and The ePolicy Institute, a Columbus, Ohio-based training and consulting firm. More than half of employers retain and review e-mail messages.

For example:

- CityWatcher.com created a media flurry this year after the Cincinnati security company implanted microchips in some of its employees. The chips were not for tracking employees but to enable them to gain access to secure rooms, according to numerous media reports.

CityWatcher did not return repeated calls seeking comment. But the headlines about microchips, which are about the size of a grain of rice and can be implanted under the skin in the arm, raised concerns that employers could force workers to get the implants. Wisconsin this year passed legislation that would ban companies from requiring workers to be implanted with such chips. Employers who violate the law face a fine of \$10,000 a day.

"It's a frightening prospect," says state Rep. Marlin Schneider, D-Wis., who sponsored the bill. "Employers would be able to monitor people wherever they go."

•Some employers require workers to use company-provided cellphones that allow whereabouts to be monitored via satellites. Xora, a Mountain View, Calif., provider of GPS-based mobile workforce management software, provides GPS technology and has sold systems to 7,000 companies representing tens of thousands of employees, mostly in construction, transportation and business services.

"Companies always want to know what's happening," says Michael Berger, manager of product marketing for Xora. "It streamlines operations."

•Some employers are scanning their employees' fingerprints or eyes to track activities or limit access to certain computers. Use of such technology is small but growing. Already, 5% of companies use fingerprint scans and 2% use facial recognition, according to the survey by the AMA and ePolicy Institute. The technology is so new that the question wasn't asked in a 2001 survey on monitoring.

At Columbus Children's Hospital in Ohio, most employees who access electronic medical data must first scan a fingerprint, a system designed to enhance security.

"From a security standpoint, it works well. You can't reproduce a fingerprint," says David Rich, medical director of clinical informatics at the hospital. "(Employees) have taken it well."

But what employees do on work equipment — even what they may do on their free time — can now cost them their jobs if their employer is watching.

Major employers such as Delta Air Lines and Google have fired employees for what they put on their own blogs. Ellen Simonetti, a Delta flight attendant, says she was fired in October 2004 after she posted pictures of herself in her uniform in suggestive poses on her blog.

"Employees should know that your employer is looking over your shoulder. If they catch you, they're canning you," says Nancy Flynn, executive director of The ePolicy Institute and author of *Blog Rules*. "You can be fired for anything, even for blogging right at home in your jammies."

Spying is necessary

Some employers say they're not damaging trust. Instead, they say, spying on employees is necessary today in large part because technology has raised the risk that workers will goof off or do something that leaves a company vulnerable to lawsuits.

Michael Prencipe wondered what his 15 employees were really doing on work time, so the partner at HR Staffing Solutions began monitoring workers' e-mail, phone calls and where they surfed on the Internet.

He was in for some surprises.

He saw employees visit pornography sites, use e-mail to troll for other jobs and even e-mail others about him, he says. So Prencipe cracked down.

He gives each employee at the staffing company an oral warning for the first inappropriate e-mail or website visit and twice has resorted to written warnings. No one has been fired.

"You're never going to stop the e-mail jokes, but sometimes you can get an eyepopper," says Prencipe, of Springfield, Va.

Employees are "usually embarrassed and humiliated," he says. "You get a downcast look and an 'I won't do it again.'"

Workplace monitoring has become so commonplace that many employees simply take it in stride. Kim Conner, 31, of Madison, Wis., works as a contractor for LiveOps, which hires independent agents to handle call-center work from their homes. LiveOps records every call its agents take.

Conner says supervisors have listened to how she handles calls and have given her pointers on how to improve.

"Sometimes you get lost in a call. A supervisor hears it and says, 'You could have done this better or differently,'" Conner says.

"It helps me with sales."

A breakdown of trust

Still, some privacy advocates and employers are leery, saying that monitoring is pitting employers against their own employees. Keith Ayers is president of Integro Leadership Institute, a leadership consulting group based in West Chester, Pa. He says employees who don't

feel trusted don't, in turn, trust their companies. Why, he asks, would employees work hard for a company that does not respect them? He says many employees may goof off online as a way to rebel.

"The very fact they're increasing effort to monitor people is an indication there's a lack of trust in the first place," Ayers says. "They're saying, 'I don't trust you. I have to keep an eye on you.' "

But concerns continue, in large part because technology provides workers with savvier ways to goof off, from shopping on eBay to running a blog. They can also use technology to steal company secrets, harass other employees or make employers vulnerable to lawsuits.

There may be legitimate reason for the concern. Sixty-five percent of men and 58% of women who use the Internet at work admit to accessing non-work-related websites when they're on the clock, according to a May 2006 survey by Harris Interactive for Websense, a provider of Web security and filtering software. Six percent of men and 5% of women said they had intentionally viewed pornography on the job.

Legally, employers are on safe ground monitoring their employees, especially if they notify workers beforehand, says Bill Nolan, an employment lawyer in Columbus, Ohio.

He also says employers face more risk today because employees can do more damage, such as spilling company secrets on a personal blog or using camera-phones to take pictures of products.

"Anything bad that employees could do before, they can do infinitely more because of technology. Sexual harassment, exposing trade secrets. So much information can move so quickly," Nolan says. "You've got to know what your employees are doing on their computer."

Gary Steele, CEO of Proofpoint, a Cupertino, Calif.-based messaging security company, says employers who use his e-mail-monitoring software have caught gaffes and shenanigans of all types — sharing confidential memos from the CEO with outsiders, revealing new product designs, using sexually harassing language and forwarding drafts of company earnings reports.

Business is doubling every year, he says.

At DeKalb Medical Center in Atlanta, e-mails are monitored in large part because of the need to protect patient confidentiality. About 3,300 employees have e-mail access. Confidential information or vulgar or abusive language can be flagged, and employees are notified.

"The hospital has a policy of full disclosure. Everything is fully monitored," says Sharon Finney, information security administrator.

"Everybody signs a document that (they understand) they're monitored. The reaction has either been positive or 'OK, fine, I understand.' "


Find this article at:

http://www.usatoday.com/money/industries/technology/2006-11-07-spy-cover-usat_x.htm

Check the box to include the list of links referenced in the article.

Related Advertising Links

What's this?

 **Hot Technology Stocks**
Fast moving technology stocks on the ground floor. Free report.
www.toptechnologystocks.com

Scottrade: \$7 Online Market Orders
\$7 stock trades. Free in-depth market research, news, quotes, charts.
www.scottrade.com

Free Terrell Owens Jersey
We'll send you an official T.O. Cowboys jersey for free! Survey req.
www.ontheweb-offer.com

Place your ad here