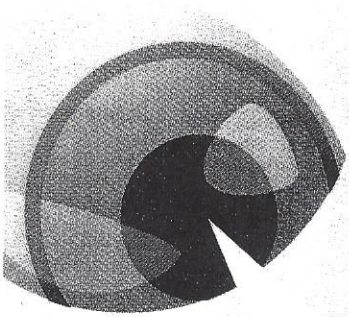
THE NATION'S NEWSPAPER
USA TODAY
NO. 1 IN THE USA

Wednesday, March 17, 2010



Cover story

Feel like someone's watching? You're right

Workers monitored both on and off job

By Laura Petrecca
USA TODAY

Almost every worker has done it: gotten in a little Facebook updating, personal e-mailing, YouTube watching and friend calling while on the clock.

Such indiscretions often went undetected by company management everywhere but the most secure and highly proprietary companies or governmental agencies. Not anymore.

Firms have become sharp-eyed, keenly eared watchdogs as they try to squeeze every penny's worth of their employees' salaries and to ensure they have the most professional and lawsuit-proof workplaces.

Managers use technological advances to capture workers' computer keystrokes, monitor the websites they frequent, even track their whereabouts through GPS-enabled cellphones. Some companies have gone as far as using webcams and minuscule video cameras to secretly record employees' movements.

"There are two trends driving the increase in monitoring," says Lewis Maltby, author of the workplace rights book *Can They Do That?* "One is financial pressure. Everyone is trying to get leaner and meaner, and monitoring is one way to do it. The other reason is that it's easier than ever. It used to be difficult and expensive to monitor employees, and now, it's easy and cheap."

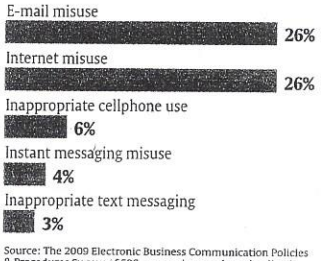
Employers no longer have to hire a pricey private investigator to install a complicated video system or computer-use tracking devices. Now, they can easily buy machine-monitoring software and tiny worker-tracking cameras at a local

Please see COVER STORY next page ▸

By Sam Ward, USA TODAY

On the firing line

Has your organization ever fired an employee for any of the following reasons?



Source: The 2009 Electronic Business Communication Policies & Procedures Survey of 586 companies, conducted online in April and May. Margin of error: ±4 percentage points.

By Karl Gelles, USA TODAY

Cover story

Employees find that it can pay to be paranoid

Continued from 1B

electronics store or through Internet retailers.

Monitoring has expanded beyond expected, highly regulated industries such as pharmaceuticals and financial services. Employees at radio stations, ad agencies, media outlets, sports leagues, even thinly staffed mom-and-pop workplaces are tracked.

Smarsh, one of many firms that offers technology to monitor, archive and search employee communications on e-mail, IM, Twitter and text-messaging, services about 10,000 U.S. workplaces.

"Employees should assume that they are going to be watched," says CEO Stephen Marsh.

Keeping an eye out

Two-thirds of employers monitor workers' Internet use, according to an American Management Association/ePolicy Institute survey from 2007, the latest data available from those groups. Nearly half of employers said they track content, keystrokes and time spent at the keyboard.

They're seeking increased productivity but also are watching workers to make sure they're not spilling trade secrets, sending boss-slamming e-mails to bloggers who cover their particular industry, sexually harassing co-workers or posting discriminatory remarks on personal blogs.

Such monitoring has increasingly become part of the public debate in recent months because of several publicized events:

▶ Next month, the U.S. Supreme Court will hear oral arguments in a case examining the allowable scope of monitoring workers' use of a company-provided pager.

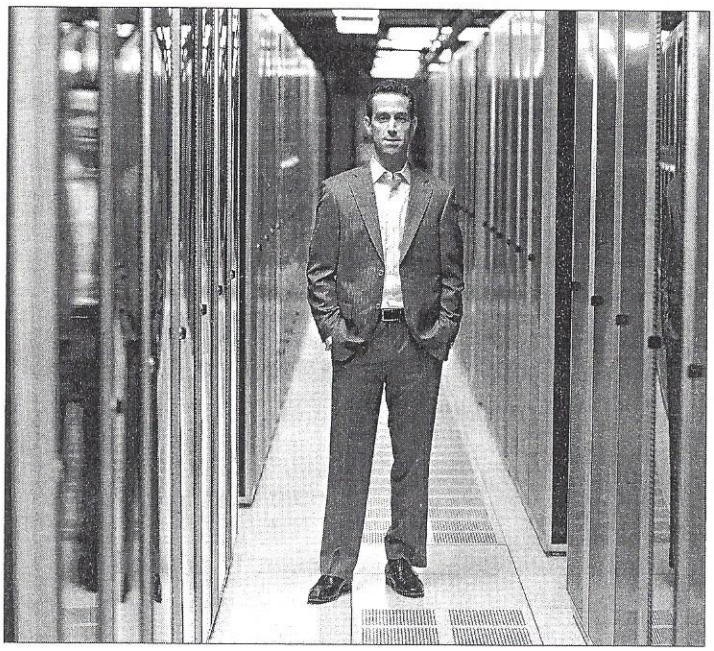
Ontario, Calif., police officer Jeff Quon sent personal, and sometimes sexually explicit, text messages to his wife and a co-worker using an employer-provided pager. His office had a written company policy stating it retained the right to monitor work activities such as e-mail and Internet use but didn't specify text messages. Quon says his rights were violated because the department had an informal practice of not reviewing messages when the employee paid for overage charges, which he had done.

Among the issues the Supreme Court will examine: "Does the employee have an expectation of privacy when using an employer-issued handheld device to transmit personal messages? … And whether his wife, who was not an employee, had a privacy expectation," says Wendy Lane, an attorney at Rutter Hobbs & Davidoff.

The decision in this case could be a "game changer" if Quon prevails, says Nancy Flynn, founder of training and consulting firm ePolicy Institute. "This could have implications for all (employer-supplied) electronic devices."

▶ The National Transportation Safety Board last month suggested using the "black box" cockpit recorders to routinely monitor pilots' conversations to make sure they are focused on work. The NTSB says this type of monitoring is a safety "essential" to make sure pilots are focused on flying — but pilots' unions say the practice would be intrusive.

▶ Japanese cellphone maker KDDI this month announced the creation of motion-sensing technology that can monitor even the smallest movements by employees, such as walking, climbing stairs and cleaning, according to a BBC report. If strapped to a cleaning worker's waist, a device with this technology can track actions such as scrubbing, sweeping and emptying garbage cans — and report the results back to managers.



No privacy online: "Employees should assume that they are going to be watched," says Stephen Marsh, the CEO of Smarsh, which sells technology used to monitor employees' online activities.

Employers use myriad ways to monitor employees

Physically going undercover

Some top managers are known for surreptitiously strolling into their company's retail stores to see how the front lines are doing. CBS turned this practice into a reality show, last month launching *Undercover Boss*.

"I typically try to find things that are positive," says 7-Eleven CEO Joe DePinto, who was recently featured on the show. "But I will always see things that can be improved."

DePinto adds that managers can sometimes get more candid feedback when they go undercover: When employees know they're talking to the CEO, they often "tell you what you want to hear rather than what is really happening."

Scrutinizing social-media use

"With social media, (employers) can monitor the actual posts and (view) what the pages and accounts look like, and take snapshots," says Stephen Marsh, CEO of Smarsh, a firm that offers monitoring technology. "If you don't like that someone is going to follow someone on Twitter, you can block that action."

Last year, 2% of employers said they terminated workers for content posted on personal social-networking sites such as Facebook and MySpace; 1% lost their jobs due to videos posted on sites such as YouTube.

Monitoring e-mail and IMs

A quarter of companies said they fired employees for e-mail policy violations in 2009, up from 14% in 2001, according to an American Management Association/ePolicy Institute poll. And 4% of companies said they've had IM-related terminations — double the 2% in 2006.

Tapping office phones

Employers can listen in on business calls and personal voice mail messages, says author Lewis Maltby. But they can't eavesdrop on personal calls while they're taking place, since that would violate federal wiretapping laws.

Watching personal Web postings

"So many people have been fired for the content that they posted on their personal blogs, that there's a term for that — it's dooced," says Nancy Flynn, founder of training and consulting firm ePolicy Institute. (That term came about after the founder of the *Dooce.com* blog was fired from her software job because of her blogging.)

"People put anything that pops in their head on their personal websites and social-networking sites, thinking their boss will never read it, but that's not true," says Maltby.

Employer advantage

In most cases, the employer has the upper hand.

"Federal law gives employers the legal right to monitor all computer activity," says Flynn. "The computer system is the property of the employer, and the employee has absolutely no reasonable expectations of privacy when using that system."

That means employers can track which websites workers visit, the instant messages they send to co-workers, even e-mails sent through personal accounts — such as Gmail — while employees are logged onto the company network or using company-owned equipment such as a laptop.

"A classic mistake is thinking that changing to your personal account buys you any privacy," says Maltby. "If you send an e-mail out, it goes through your company server. If they're monitoring e-mail, the personal e-mail gets monitored just like business e-mail." Often, employers have good reason to snoop. According to a 2009 AMA/ePolicy survey:

▶ 14% of employees admit to e-mailing confidential or proprietary information about a firm, its people, products and services to outside parties.

▶ 14% admit to sending third parties potentially embarrassing and confidential company e-mail that is intended strictly for internal readers.

▶ 89% of users admit to using the office system to send jokes, gossip, rumors or disparaging remarks to outsiders.

▶ 9% have used company e-mail to transmit sexual, romantic or pornographic text or images.

On the employer side, 1-in-10 say they've gone to court to fight lawsuits that were specifically triggered by employee e-mail. In addition, 2% of employers were ordered by courts or regulators to produce employee instant messages (IMs). That's twice the amount reported in 2006.

Seen as intrusive

Maltby's book and a new report from the law firm Jackson Lewis list multiple examples of employees getting fired for something as innocuous sounding as social-media use. But once employees step into dangerous areas such as publicly criticizing their company, they are vulnerable to employee discipline.

Bosses can penalize employees for what they deem as "inappropriate" posts, videos and pictures on social-networking sites, even if a worker uses those sites during non-working hours.

Management at independent brokerage and investment banking firm J.P. Turner not only tracks e-mail, it also follows up on the personal Twitter and Facebook use of the approximately 100 employees at their Atlanta headquarters and the company's registered representatives at more than 180 U.S. offices.

J.P. Turner doesn't allow "unapproved, professional use of social-networking sites," and searches for company mentions on those sites — such as an employee listing the firm name on his or her personal Facebook biography. If a posting associated with the company doesn't reflect good judgment on behalf of the user, the firm notifies that worker's supervisor and asks to have the post removed, says Compliance Officer Michael Isaac.

Even as they make some seemingly harmless — and some not-so-harmless — infractions, employees are usually horrified when they realize they are being watched.

"Frankly, employees tend to resent monitoring," says Flynn.

And they are often surprised and embarrassed at the ramifications.

In 2001, Heather Armstrong launched the blog *Dooce.com* to write about topics such as pop culture and music. She also wrote about her co-workers at a small software company.

"I really, really thought that my employer was not ever going to find it," she says. But a fellow employee tipped off the company vice presidents, and Armstrong was fired.

"They just said it was unacceptable that I had done this," she says.

All of her belongings were boxed up, and she was escorted to her car. "I was humiliated," she says. "It was a dumb move on my part."

Her advice for would-be bloggers: Get company permission. "No matter who you don't want to read it — they'll find it," she says.

They have their reasons

Many staffers don't realize that their employers have legal and ethical reasons behind their snooping. Workplaces with monitoring policies often don't let employees know they are trying to prevent serious issues such as sexual harassment cases.

"You can't expect an untrained workforce to be compliant," says Flynn. "If employers would just take the time to do some training and explain, 'Here's why we're doing the monitoring. We're not electronic voyeurs, we're not trying to dig into your personal life, that's not our concern,' then the whole monitoring scenario would go over much more successfully with employees."

Yet, even if a company is seemingly open about its monitoring, there is reason for workers to be concerned about what communications they receive from management.

A court precedent says that employees have no rights to privacy in e-mail, even if a company promises not to track it, Maltby says. Also, workers should never assume that if they don't get any memos on monitoring, that it isn't happening. "Just because your boss doesn't tell you he's monitoring, that doesn't mean it's not happening," he says.

Maltby and other workplace experts suggest a healthy dose of paranoia — as well as the purchase of a personal cellphone and computer that are never used for work-related tasks — as the only safe way around the watchful boss.

"It's technically possible to monitor just about anything," says Marsh. And for those who really want to be safe, he suggests leaving the work building, going around the corner and "talking to someone face to face."