

Smallbiz.nypl.org

NYC Small Business
Resource Center

Starting a small business? Start here.

Events

Videos

Forum

FAQ

Services Directory

Business Manual



TIME

FROM THE MAGAZINE

Sunday, Sep. 3, 2006

Snooping Bosses

Think your employer is checking your e-mail, Web searches and voice mail? You're probably right

By KRISTINA DELL, LISA TAKEUCHI CULLEN

When one of his employees phoned in sick last year, Scott McDonald, CEO of Monument Security in Sacramento, Calif., decided to investigate. He had already informed his staff of 400 security guards and patrol drivers that he was installing Xora, a software program that tracks workers' whereabouts through GPS technology on their company cell phones. A Web-based "geo-fence" around work territories would alert the boss if workers strayed or even drove too fast. It also enabled him to route workers more efficiently. So when McDonald logged on, the program told him exactly where his worker was--and it wasn't in bed with the sniffles. "How come you're eastbound on 80 heading to Reno right now if you're sick?" asked the boss. There was a long silence--the sound of a job ending--followed by, "You got me."

For every employer who lets his staff know they're on watch, there are plenty who snoop on the sly. A general manager at a computer outfit in the Northeast wondered about a worker's drop-off in productivity. Using software called SurfControl, the manager saw the man was spending an inordinate amount of time at an innocently named website. It turned out to feature hard-core porn. The worker was conducting market research for his escort service, a venture for which he soon had plenty of time after he got canned. "I don't give a rat's rear what they do at home," says the manager, who wishes to keep his and his company's name private. "But what they do at work is all my business."

Learn that truth, and learn it well: what you do at work is the boss's business. Xora and SurfControl are just some of the new technologies from a host of companies that have sprung up in the past two years peddling products and services--software, GPS, video and phone surveillance, even investigators--that let managers get to know you really well. The worst mole sits right on your desk. Your computer can be rigged to lock down work files, restrict Web searches and flag e-mailed jokes about the CEO's wife.

"Virtually nothing you do at work on a computer can't be monitored," says Jeremy Gruber, legal director of the National Workrights Institute, which advocates workplace privacy. Nine out of 10 employers observe your electronic behavior, according to the Center for Business Ethics at Bentley College. A study by the American Management Association and the ePolicy Institute found 76% of employers watch you surf the Web and 36% track content, keystrokes and time spent at the

keyboard. If that isn't creepy enough, 38% hire staff to sift through your e-mail. And they act on that knowledge. A June survey by Forrester Research and Proofpoint found that 32% of employers fired workers over the previous 12 months for violating e-mail policies by sending content that posed legal, financial, regulatory or p.r. risks.

You might think the sheer volume of e-mail would mean you could get away with a crack about the boss's Viagra use. But sophisticated software helps employers, including Merrill Lynch and Boeing, nab folks who traffic in trade secrets or sexist jokes. One called Palisade can recognize data in varying forms, like the content of NFL playbooks, and block them from your Out box. SurfControl, MessageGate and Workshare check work files and e-mail against a list of keywords, such as the CEO's name, a company's products or four-letter words. Wall Street and law firms sometimes block access at work to personal accounts like Google's Gmail.

You can't really blame companies for watching our Web habits, since 45% of us admit that surfing is our favorite time waster, according to a joint survey by [Salary.com](#) and AOL. A Northeast technology company found that several employees who frequently complained of overwork spent all day on [MySpace.com](#) Information-technology departments routinely receive automatic Web reports on what sites employees visit; they tend to review them only if there's a red flag.

Computers aren't the only office snitches. Slightly more than half of employers surveyed monitor how much time their employees spend on the phone, and even track calls--up from 9% in 2001. Companies are required to inform every nonemployee that they're listening in, which is why you hear, "This call is being monitored for quality assurance." But there's no such protection for staff members. Bosses monitor calls with programs like Nice Systems', which sends an alert if your voice reaches a certain decibel level or you blurt out profane language or a competitor's name.

You might want to stay on your best behavior even off the clock. Programs like Verified Person keep tabs on employees outside the office with ongoing background checks. Got busted for DUI last week? The boss will find out. And what you do on the Internet at home is no secret either. After Penelope Trunk won an award for writing about sex online, her blushing employer asked her to start using a pseudonym. At the travel sector of one corporation, a manager's spouse was surfing the Net and found a photo album with the company's name on a picture-sharing site. The photos documented a training session, after which co-workers progressed to inebriated nakedness. Because a worker posted the pictures without consent, he was fired. "If you'd be embarrassed that your mom saw it, don't post it," advises Kevin Kraham, a law partner at Ford & Harrison.

Bloggers, be careful. Workers at Google, Delta Airlines and Microsoft have claimed their blogs got them fired. But with more than 50 million blogs out there, employers like Microsoft train new hires on blog etiquette. Curt Hopkins of Ashland, Ore., says a public radio station cut short a job interview after the boss read his blog; he was later hired by the Oregon Shakespeare Festival to "build buzz online." Trunk, who now blogs about workplace issues on [Brazen Careerist](#), says telling young workers not to blog is like telling a baby boomer not to use the phone. "When major corporations try too hard to block the electronic community," she says, "Generation Y just leaves."

The Facebook set may not like it, but courts are mostly giving the O.K. to corporate

spying. "I haven't seen one case where an employee has won on a right-of-privacy claim," says Anthony Oncidi, head of the labor and employment department at law firm Proskauer Rose. Companies can ward off privacy claims if they have informed staff members they're being monitored, even if only in a single sentence in a rarely read handbook. Even when there is no advance notice, workplace-privacy claims have proved hard to win. Only two states (Connecticut and Delaware) require bosses to tell workers they're being monitored, but even in those places, there aren't restrictions on spying.

Businesses argue that their snooping is justified. Not only are they trying to guard trade secrets and intellectual property, but they also must ensure that workers comply with government regulations, such as keeping medical records and credit-card numbers private. And companies are liable for allowing a hostile work environment--say, one filled with porn-filled computer screens--that may lead to lawsuits. "People write very loosely with their e-mails, but they can unintentionally reach thousands, like posters throughout a work site," says Charles Spearman of diversity-management consultants Tucker Spearman & Associates. "In an investigation, that e-mail can be one of the most persuasive pieces of evidence." In fact, a ruling in New Jersey last year found an employer had a duty to investigate an employee's viewing of child pornography and report it to the police.

The monitoring trend could get even more Orwellian. In *Thompson v. Johnson County Community College* in Oklahoma, the court held that employees had no expectation of privacy in a locker room because the room had pipes that required occasional maintenance. (The need to service the pipes was enough for the court to let the employer use video surveillance.) The wave of the future seems to be radio-frequency identification, a transmitter smaller than a dime that can be embedded in anything from ID cards to key fobs to hospital bracelets (to safeguard newborns, for instance). Now consider Compliance Control's HyGenius system, which detects restaurant employees' handwashing and soap usage with wireless communication from clothing tags. Skip the soap, and you are in hot water.

Think that's invasive? At Citywatcher, a Cincinnati, Ohio, company that provides video surveillance to police, some workers volunteered to have ID chips embedded in their forearms last June. No more worries about lost or stolen ID cards, the employer claimed. Sure. No more privacy either.

Copyright © 2006 Time Inc. All rights reserved.
Reproduction in whole or in part without permission is prohibited.

[Privacy Policy](#)

rate spying. "I haven't seen one case where an employee has won on a right-of-privacy claim," says Anthony Oncidi, head of the labor and employment department at law firm Proskauer Rose. Companies can ward off privacy claims if they have informed staff members they're being monitored, even if only in a single sentence in a rarely read handbook. Even when there is no advance notice, workplace-privacy claims have proved hard to win. Only two states (Connecticut and Delaware) require bosses to tell workers they're being monitored, but even in those places, there aren't restrictions on spying.

Businesses argue that their snooping is justified. Not only are they trying to guard trade secrets and intellectual property, but they also must ensure that workers comply with government regulations, such as keeping medical records and credit-card numbers private. And companies are liable for allowing a hostile work environment—say, one filled with porn-filled computer screens—that may lead to lawsuits. "People write very loosely with their e-mails, but they can unintentionally reach thousands, like posters throughout a work site," says Charles Spearman of diversity-management consultants Tucker Spearman & Associates. "In an investigation, that e-mail can be one of the most persuasive pieces of evidence." In fact, a ruling in New Jersey last year found an employer had a duty to investigate an employee's viewing of child pornography and report it to the police.

The monitoring trend could get even more Orwellian. In *Thompson v. Johnson County Community College* in Oklahoma, the court held that employees had no expectation of privacy in a locker room because the room had pipes that required occasional maintenance. (The need to service the pipes was enough for the court to let the employer use video surveillance.) The wave of the future seems to be radio-frequency identification, a transmitter smaller than a dime that can be embedded in anything from ID cards to key fobs to hospital bracelets (to safeguard newborns, for instance). Now consider Compliance Control's HyGenius system, which detects restaurant employees' hand-washing and soap usage with wireless communication from clothing tags. Skip the soap, and you are in hot water.

Think that's invasive? At Citywatcher, a Cincinnati, Ohio, company that provides video surveillance to police, some workers volunteered to have ID chips embedded in their forearms last June. No more worries about lost or stolen ID cards, the employer claimed. Sure. No more privacy either. ■

How You Can Stay out of Trouble

Everything that happens at work can be your boss's business. Keep that in mind the next time you're tempted to vent via e-mail or forward an off-color joke. Innocent words today could make good legal evidence tomorrow. Here are some precautions to take against snooping supervisors.



1. KNOW YOUR COMPANY'S POLICIES

It sounds obvious, but few people bother to read through their employee handbook, where the fine print is located. Note how long your job saves business records. "Before using a new technology, think about whether [usage or content] could violate a work policy," says Nancy Flynn, executive director of ePolicy Institute. Companies are starting to put restrictions on text messaging, camera phones and software downloads.

2. SURF THE WEB SPARINGLY

Web surfing equals time wasting to most companies, so keep those ESPN.com hits to a minimum. Don't leave your Hotmail window open for hours, even if it's idle. Anyone monitoring your Web activity may think you spent all day e-mailing your friends and relatives. Delete your Web history from the preferences page, and never update your MySpace page at work—because work is the boss's space.

3. THINK TWICE BEFORE YOU HIT "SEND"

E-mails get forwarded, they can lack subtlety, and they're a written record. Be careful! Limit personal use of your

work account, and erase all personal mail at the end of each day. While it's likely to be archived, your employer would have to work harder to retrieve it. Avoid using your boss's name or other terms snooping software might be searching for.

4. PROOFREAD PROFILES

Treat blogs and online profiles (even e-mails) as you would a résumé: check for spelling and grammar mistakes. "Be careful any time you leave a written record," says Flynn. "Once it's in writing, you're not getting it back, since posts are forwarded and linked to all over the Web." Never use your company's name or logo without permission. Blog postings should avoid hot-button topics like politics and religion. And skip items that could leave a bad impression, like your college beer-pong championship.

5. SNAIL-MAIL YOUR RESUME

Be careful e-mailing your résumé as a Word document, since programs like Workshare let employers view earlier edits made to electronic drafts that could show mistakes or inflated language. If you must e-mail, disable the "track changes" feature in Word

and cut and paste it into a new document, or use Workshare yourself to wipe away older versions.

6. HOLD YOUR TONGUE

Don't leave voice mails you wouldn't want your boss to hear. Some companies archive voice messages, often turning them into data files. Voice mail is particularly revealing at a trial because the jury can hear, for instance, if you laughed after insulting a co-worker. "It's a smoking gun," says Flynn.

7. FORWARD WITH CARE

Delete raunchy jokes. Once you forward them, you put yourself in the mix, and some companies have treated those employees more harshly than the ones who simply opened them.

8. USE PASSWORDS

They help ensure that no one can hijack your computer to do Internet searches or send e-mail attributed to you. Do the same for pictures you send and receive at work. Passwords don't mean a higher expectation of privacy; they just make posts more secure.

9. NO PORN AT WORK

Enough said. Yes, we know: you go to Playboy.com for the articles. —K.D.