

RESOURCES

## CAREERS

 SITE INDEX 
**FREE Technical Papers** View our expanded library!  
 

# Big Brother at Work

**New surveillance tools and a lack of regulation give employers the upper hand**

By David Kushner

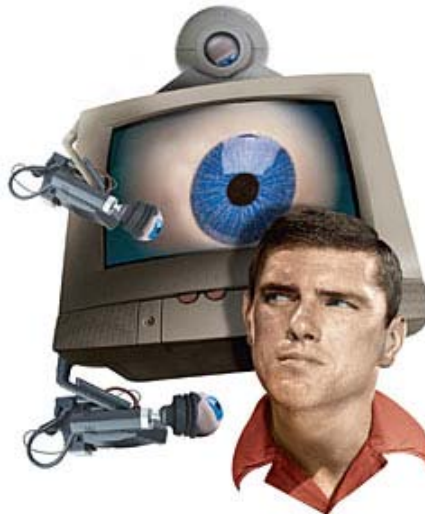
It can happen innocently enough. You open your e-mail. There's a message from a co-worker down the hall. You double-click to find an off-color joke, along with a randy JPEG.

These days, employees who swap racy e-mails might get something worse than bad jokes; they could get the boot. At several companies, including the New York Times Co., Xerox, and Dow Chemical, workers have been fired for allegedly sending or storing pornographic images on office networks. And while employers have been eavesdropping on their workers' phone calls for some time now, newer technologies are allowing employers to keep tabs on workers as never before.

These tactics range from radio frequency identification (RFID) tags to Global Positioning System (GPS) chips embedded in cellphones and company cars. Even video surveillance is being reborn, with searchable digital systems that can run over a network. According to the American Management Association in New York City, nearly 80 percent of U.S. companies now engage in some form of workplace monitoring, up from 15 percent of companies in 1997.

To be sure, employers have their reasons for watching. After all, a disgruntled employee can make off with many megabytes' worth of company secrets on a thumb-size drive. Managers may worry that productivity could slip if workers spend too much time surfing eBay. But employers can go too far, says Frederick S. Lane, author of *The Naked Employee: How Technology Is Compromising Workplace Privacy*. "The problem is that this technology gives employers access to so much information that they really get to call all the shots."

**ONE BIG REASON** employers are snooping more is that they can: there are few laws protecting privacy at work, particularly in the United States. While there are certain standards



for privacy in one's own home, those rights generally don't extend to the workplace. Some countries, such as Germany and Australia, are beginning to address workplace snooping, but in the United States "these laws are still in the Dark Ages," says Lewis Maltby, president of the National Workrights Institute, an organization based in Princeton, N.J.

As a result, workers are left to fend for themselves. The question is whether there's anything they can do. Employers clearly have the upper hand in terms of snooping technology. Office computers tend to be connected to networks, rather than stand-alone machines, which makes it easier to filter e-mail for pornographic language or to monitor activity on employee computers.

One software package, from TrueActive Software Inc., Kennewick, Wash., automatically logs all the activity on a PC—recording keystrokes, Web site visits, and even what text has been cut and pasted. Another company, Stellar Internet Monitoring LLC, Naples, Fla., sells software that tracks Web usage in real time. A monitoring program, installed on one computer of a network, filters and encrypts Internet traffic information on the fly.

Such innovation is not necessarily a bad thing, says Maltby. "As the technology becomes more sophisticated, it enables employers to do what they need to do without invading people's privacy," he says. "Instead of opening every e-mail that uses a suspect word, technology today can look for other words before deciding whether it should be opened."

Location-tracking tools let employers know where their workers are at any time of the workday. Earlier this year, the Orlando, Fla., police department conducted a pilot program that used GPS devices in patrol cars to track its officers. Though such technology could be used to, say, locate an injured cop, the officers balked at the invasiveness, and the program was dropped.

RFID tags are another way to track the movements of workers and goods. Access Inc., a security technology firm in Carrollton, Texas, sells an RFID system designed to prevent the theft of valuables. RFID readers placed throughout the workplace can detect an Access tag affixed to an object or embedded in an employee badge from up to 20 meters indoors.

With such a system, employers can be assured that laptops aren't walking out the door without authorization. They'll also know, with great precision, who's talking to whom and how long each worker spends at the water cooler.

**SO WHAT'S A CONCERNED** employee to do? For one thing, be careful. Privacy experts suggest not sending personal e-mail from work. To make it harder to track your Web surfing, Stealth Ideas Inc., in Sherman Oaks, Calif., sells the StealthSurfer, a US \$99 USB thumb drive, whose self-contained browser caches the files and cookies you accrue while surfing.

Aside from such countermeasures, experts encourage employees to find out whether and how their companies monitor the workplace. "If you're not sure if your company conducts monitoring," Maltby says, "just ask."

## TO PROBE FURTHER

For a short review of privacy laws, see "Workplace Privacy Laws—Or the Lack Thereof" on the Web at <http://www.spectrum.ieee.org/careers/>.

ILLUSTRATION: VIKTOR KOEN

## >> IEEE Spectrum Advertiser Marketplace

The following is commercial information. Click [here](#) for details.

### [Complete HDL Design Entry & Verification Solution](#)

Active-HDL 6.3 supports mixed VHDL, Verilog, C/C++, SystemC and EDIF simulation f...

### [PCBpro-Easiest Site to Quote/Order Circuit Boards](#)

Free quotes for circuit boards in seconds with no sign up required. Easy order p...

### [Prototype Circuit Boards from PCBexpress](#)

Leading Internet supplier of prototype circuit boards. Successfully selling pcbs...

### [New Acqiris Software for Multichannel DAQ Systems](#)

Acqiris launches a stand-alone Multichannel Acquisition Software package that si...

[Buy a Link Now!](#)