Watching the Watchmen

Most companies monitor their employees in some way, but is corporate Big Brother going too far?

BY ROBERT LEMOS

CAUGHT IN THE ACT

Companies are increasingly monitoring their workers' actions as the Internet—for work and for pleasure—becomes a greater part of the job.

COMPANIES
76% monitor workers' Web connections
65% block inappropriate sites
50% store and review employees' computer files

WORKERS
61% use the Internet at work for personal reasons
92% believe company has the right to filter
12% got possible spyware sent by friend or coworker

Source: American Management Association's 2005 Electronic Monitoring & Surveillance Survey and Websense's Web@Work survey.

COMPANIES ARE INCREASINGLY LOOKING at their workers as wayward sons and daughters. Though privacy advocates have long worried about government becoming Orwell's Big Brother, it's the corporate world that is quickly adopting the technology to monitor its employees.

To be fair, although employees generate revenue, their online work habits can quickly get a company in trouble, whether through viewing offensive content, sending inappropriate e-mail, or opening unsafe content. But this issue is a slippery slope. The vast majority of employees may readily concede that companies have the right to block them from browsing unsafe or inappropriate sites, but it's unlikely that they are comfortable with the lengths to which their employers have gone.

More than three-quarters of all companies are monitoring their employees' Internet activity, and two-thirds use filtering software to block inappropriate Web sites in the same way that they block telephone calls to 900 numbers, according to a 2005 study conducted by the American Management Association. Nearly two-thirds of companies also routinely monitor employees' Web-surfing habits, and more than a third store and monitor e-mail as well as record keystrokes. This practice was brought into sharp relief after the fracas with HP, which accessed the phone records of company board members and nine reporters without authorization. (See the sidebar for more information on the dos and don'ts of using your employer's computer and Internet connection.)

The level of monitoring can be as simple as keeping track of the log files that traffic over a company's network invariably creates. Or it may involve more specialized techniques such as a keystroke logger (a small device that attaches to a keyboard and records every character typed) and data-auditing software, which manages the various media devices on a worker's PC, tracking the data that the employee attempts to copy.

The extent to which some companies monitor their workers sometimes seems driven by the latest marketing push from content-security firms—which is aimed more at curtailing threats to productivity than at security. In a recent survey, one company warned that 1 out of 50 Web sites that workers browsed was related to a search for either a new job or a new home. That data does not tell the whole story, however. Workers searching on either of those topics likely view a great number of pages, so the actual percentage of employees involved might be lower by a factor of ten or more. Moreover, it's unlikely that those types of sites lead to a disproportionate number of security threats.
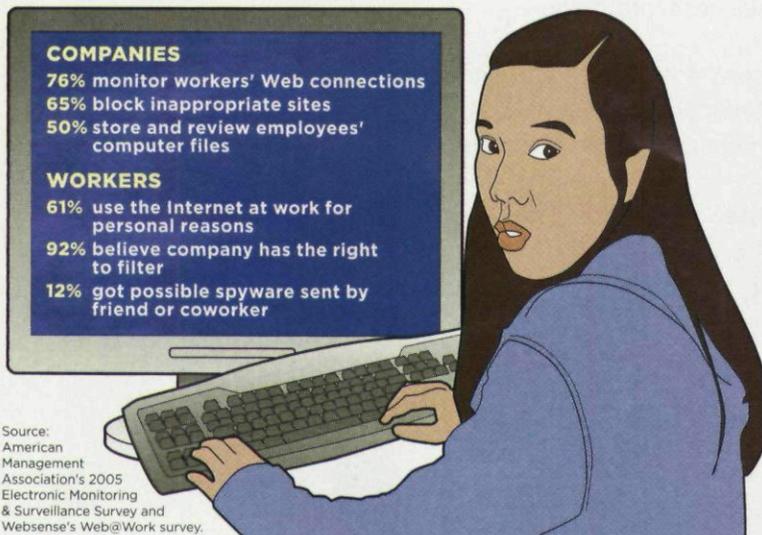
Workers have little recourse for protection against monitoring. By working for a company and agreeing to its information policies, the employee gives permission for such monitoring to take place. Moreover, U.S. courts have repeatedly upheld the right of employers to monitor their workforce.

With the division between work and home rapidly eroding, companies are increasingly vulnerable to employees' bringing viruses and Trojan horses back to the office system on a laptop or storage device. The flip side is that workers increasingly have to worry that their employers' security measures and monitoring are taking a peek into their private lives.

Robert Lemos is a freelance journalist and the editor-at-large for SecurityFocus.