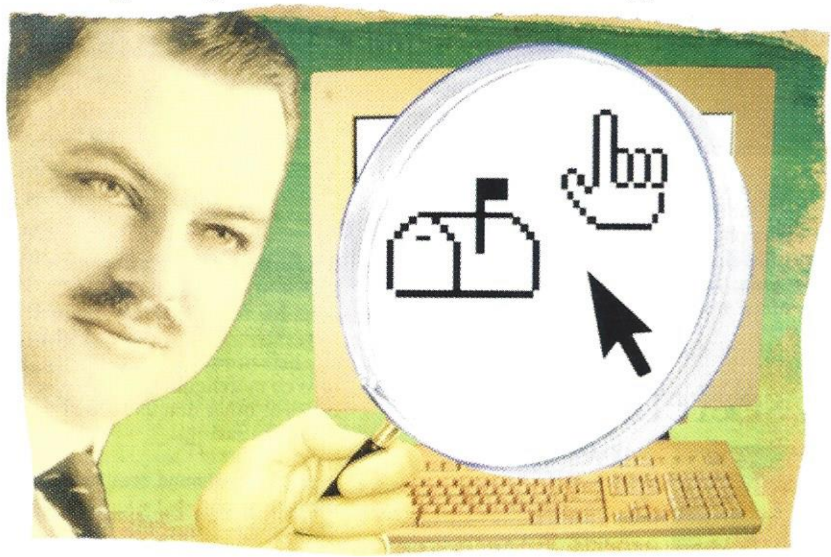
U.S.News & WORLD REPORT
AUGUST 13, 2001
www.usnews.com

Lawsuits spur rise in employee monitoring



BY DANA HAWKINS

In case you haven't heard, your company is probably peeking at your E-mail, computer files, and Internet surfing log. But why? Are employers concerned about productivity, worried about workers spilling company secrets, or are they just plain nosy? The answer may be all of the above. But the No. 1 reason for monitoring these days is to avoid the hot lights and high costs of courtroom drama. Companies say they need protection against lawsuits, and surveillance software and other tools that allow them to snoop are becoming less expensive and easier to use.

At the same time, some legal experts are taking a contrarian view. They don't believe that companies are always entitled to rummage through workers' E-mails and files for information, which can be used to fire employees at will.

A survey of 435 major U.S. firms, to be released this week by the American Management Association, in collaboration with the ePolicy Institute and *U.S.News & World Report,* examines why these companies are monitoring workers. Of the firms surveyed, almost 10 percent report having received a subpoena for employee E-mail. Nearly one third of the largest companies say they've been subpoenaed, and also report firing employees for sending sexually suggestive or otherwise inappropriate E-mails. One quarter of the firms surveyed say they perform key word or phrase searches, usually looking for sexual or scatological language.

The motivation is clear: "Almost every workplace lawsuit today, especially a sexual harassment case, has an E-mail component," says Nancy Flynn, executive director of the ePolicy Institute, which develops E-mail and Internet policies for employers. The survey also found that barely half of firms require staff to acknowledge, in writing, that they understand the company's computer-use policy, which is often vague and buried in an employee handbook.

The rise in monitoring and the resultant firings have paralleled the increased reliance on technology in the workplace over recent years. The new Electronic Policies and Practices Survey is a follow-up to the AMA's annual look at employee surveillance, released last spring. That report had found that more than 75 percent of major U.S. firms record and review their workers' communications—double the 1997 figure. Last June, at least 20 state employees in South Dakota were fired or disciplined for allegedly burning job time surfing sports, shopping, and porn sites. An investigation of the 100 workers who visited the most Web sites during a three-week period revealed thousands of inappropriate hits, says a spokesman for the governor's office.

E-mail as evidence. Employees are asking why they are so often kept in the dark about when and how their computers are searched. Some workers fired from the *New York Times*'s business office and more recently at Computer Associates International say that although they received offensive E-mail, they did not send it. Both companies dispute the claims. Some employees also say they weren't shown the evidence against them. "We didn't want to bring pornography into the employee meetings, because it's not appropriate," says Deborah Coughlin, a spokesperson for CAI. Giving workers a chance to respond to such accusations can make a big difference. Officials in South Dakota say when they discussed the reports with workers, one was cleared because he successfully argued that he wasn't even in the office when his computer recorded a substantial number of visits to questionable Web sites.

James M. Rosenbaum, chief judge of the U.S. District Court in Minneapolis, is challenging the conventional wisdom that businesses own not only the computers that employees use but also the personal messages, unfinished drafts, and other thoughts that they casually type into them. In a recent essay published in the *Green Bag*, a law review, Judge Rosenbaum proposes that investigations of workers' computers be handled like other legal searches. Companies should have probable cause, searches must be limited in scope, and employees need to be given prior notice and allowed to be present during the search, he argues. "I'll bet you all the money in the world I can go into your computer and find a basis to fire you," says Rosenbaum. "Computers never forget, which would be terrific if humans were perfect, but they aren't." ●

WHERE TO LEARN MORE

- **Survey results.** For the full report, go to the American Management Association's site at *www.amanet.org/research.*
- **The ePolicy Handbook.** Available at *www.epolicyinstitute.com,* it contains sample E-mail, Internet, and computer-use policies for companies.
- **Job loss monitor.** The Privacy Foundation's Workplace Surveillance Project, *www.privacyfoundation.org,* keeps tabs on firms that have fired or disciplined employees based on computer use.

ILLUSTRATION BY ELLEN WEINSTEIN FOR *USN&WR*