Privacy advocates worry about monitoring of government workers

By Lisa Rein, Washington Post

When the Food and Drug Administration started spying on a group of agency scientists, it installed monitoring software on their laptop computers to capture their communications.

The software, sold by SpectorSoft of Vero Beach, Fla., could do more than vacuum up the scientists' e-mails as they complained to lawmakers and others about medical devices they thought were dangerous. It could be programmed to intercept a tweet or Facebook post. It could snap screen shots of their computers. It could even track an employee's keystrokes, retrieve files from hard drives or search for keywords.

"Every activity, in complete detail," SpectorSoft's Web site says about its best-selling product, Spector 360, which the company says it has sold to dozens of federal agencies.

Government workers have long known their bosses can look over their shoulder to monitor their computer activity. But now, prompted by the WikiLeaks scandal and concerns over unauthorized disclosures, the government is secretly capturing a far richer, more granular picture of their communications, in real time.

Federal workers' personal computers are also increasingly seen as fair game, experts said.

Nonintelligence agencies spent $5.6 billion in fiscal 2011 to safeguard their classified information with hardware, software, personnel and other methods, up from $4.7 billion in fiscal 2010, according to the Information Security Oversight

Office. Although only a portion of the money — the amount is not specified — was spent on monitoring for insider threats, industry experts say virtually every arm of the government conducts some form of sophisticated electronic monitoring.

“It used to be, to get all of an agency’s records out you needed a truck,” said Jason Radgowsky, director of information security and privacy for District-based Tantus Technologies, which evaluates monitoring systems for the Federal Aviation Administration, the Export-Import Bank and the National Institutes of Health. “Now you can put everything on a little USB thumb drive.”

The stepped-up monitoring is raising red flags for privacy advocates, who have cited the potential for abuse. Among other concerns, they say they are alarmed that the government has monitored federal workers — including the FDA scientists, starting in 2010 — when they use Gmail, Yahoo or other personal email accounts on government computers.

Although the FDA has said it acted out of concern that the scientists were improperly sharing trade secrets, the scientists have argued in a lawsuit that they were targeted because they were blowing the whistle on what they thought had been an unethical review process.

Read the whole story