Got a Security Clearance? Now the Feds Want to Spy on You, Too

By Aliya SternsteinNational Security Agency leaker Edward Snowden had skeletons in his closet that employee records systems apparently did not share with the NSA, raising the issue of whether cleared personnel should be under continual surveillance. Today, once an employee obtains a security clearance, agencies can perform follow-up investigations every five years or when derogatory information is discovered.The New York Times

last week reported that NSA missed complaints from Snowden's former supervisor at the CIA about Snowden's troubling work habits (the supervisor suspected the technician was inappropriately attempting to access classified files) likely because the systems managing employee clearances only documented major rule violations, not suspicions about personal behavior.In September, former Defense Department Deputy Secretary John Hamre argued in the Washington Post

that someone in Snowden's position should be subjected to continuous, perhaps automated surveillance. Such ongoing scrutiny should apply to anyone with high-level clearances, including Hamre himself, he said.Electronic surveillance of cleared workers is technically possible, according to computer engineers. Federal managers, for instance, could read alerts from spyware installed on an employee's personal cellphone. But spying on the entire cleared workforce would be illegal -- unless new federal rules are issued.Today, the Fourth Amendment, Privacy Act and other civil liberties laws and regulations forbid tracking government employees outside the workplace.Short of asking employees with high level clearances to waive their privacy rights, “the government simply may not conduct surveillance by wiretapping” or remotely activating the “microphone of personal cell phones or computers," said Greg Rinckey, an attorney who specializes in military law and represents national security clearance applicants.Snowden reportedly relied on an encrypted email service, called Lavabit, to hide his activities. The ex-NSA contractor now is wanted by the federal government for disclosing domestic surveillance secrets to the press. According to a Monday Washington Post

story, Snowden leaked to the newspaper documents showing that NSA culls contacts from personal webmail and instant messaging accounts at a rate of more than 250 million lists a year, including many Americans’ address books.Any future, authorized e-surveillance of cleared personnel would have to be performed with tremendous care, privacy advocates warn. Otherwise, the process could smear innocent employees or tip off the bad guys.Most of the existing mechanisms for detecting potential insider threats are plagued by false positives and risk wrongful character assassination and other mistaken inferences, said Peter G. Neumann, a computer scientist for SRI International, a nonprofit research institute. He was sharing personal views, not those of his employer or any government agency he has advised."If someone is browsing on a subject that raises an automatic alert, that person might be trying to solve a crossword puzzle,” Neumann said. “If I get a wrong number on my cell phone or a fraudulent scam call, I am falsely linked with the caller, irrevocably.”Computer formulas probably are not smart enough to sense that researching club drugs online out of

concern for a child's health is different from researching club drugs to find the best high. "Context is everything, and it is often ignored," Neumann said.He added that any digital surveillance should be conducted "very carefully, with serious oversight and open admission of what [employers] are doing."Openly admitting to employee surveillance, however, could introduce other security weaknesses. "What about the argument that if the government reveals what it is doing, people might be able to work around it?" Neumann questioned. If I am using cryptography because of corporate secrecy, does that mean I am hiding something? No, my employer might be insisting that I use encrypted e-mail.And computerized surveillance alone probably wouldn't stop the next Snowden. He was a system administrator whose job reportedly required accessing and moving sensitive documents. To combat such an inherent insider threat, the government could grant ultimate "superuser" access privileges to the director of national intelligence or other top brass.But that move carries risks too."This is a huge slippery slope if the computer systems are already inadequately trustworthy," Neumann said. And who is to say that higher-level authorities are fault-proof? He pointed to Robert Hanssen, a former FBI agent who sold U.S. secrets to Moscow. "Hanssen had been given the task of finding the mole inside the FBI -- which was Hanssen himself," Neumann said.Even cybersecurity experts note that machines would have struggled to detect philosophical issues that might motivate the likes of Snowden to expose classified information. Snowden has said he grew disillusioned with the U.S. government while working inside intelligence agencies.Agencies must use “fine-grained access controls," including a new two-person rule prohibiting system administrators from accessing key information without another authorized individual present, "as well as role-based monitoring to detect what your administrators are doing versus what they should be doing," said Eric Chiu, president of HyTrust, a firm that helps organizations protect data flows over the Internet. "This is the only way to prevent major breaches and data center disasters in an electronic and connected world."