TULLY RINCKEY PLLC
YOUR LAWYERS FOR LIFE - 1888LAW4LIFE.COM

The Government Already Has the Technology to Monitor Cleared Employees

The government for years has continuously, electronically surveilled the behavior of personnel in sensitive security positions and does not need a whole new system to catch the next leaker, a former top technology executive in the intelligence community said. His comments came as debate heats up about building new technology to catch rogue federal employees."It’s not new technology -- it’s a matter of making more it more encompassing, making it more scalable, making it faster” at searching for signs of changes in behavior, said Dale Meyerrose, the first chief information officer of the intelligence community, under the Director of National Intelligence, during an interview. "A lot of it is the same infrastructure, the same sensors, the same networking technology. You just put in the software code new rules [detailing which databases to scour], new processes, new applications."On Monday, the Associated Press reported

that intelligence officials plan to use “a sweeping electronic system to continually monitor workers with secret clearances,” such as former intelligence contractor Edward Snowden, who leaked domestic surveillance secrets.Assessing psychological changes is not the goal of the tools, observers noted.Mental health records are not as easy to lasso together, for structural and legal reasons, said Nicole A. Smith, an associate at Tully Rinckey PLLC and a former national security background investigator.Some cleared personnel are required to sign a waiver releasing mental and physical medical records. But, even with a waiver, the ability to continuously, electronically scan mental health records would be limited because of the way records are organized within a doctor's office."You’re not talking about getting inside someone’s brain," Meyerrose echoed. "It's all about behavior -- from that behavior, you red flag it and say we need to watch this person a lot more closely: Are they going to this drug site because they plan on dealing illegal drugs, or are they going to this drug site so that they can learn more about drugs, so that they can deal with their teenage kid who's got a drug problem?"Meyerrose left the White House at the end of the George W. Bush administration and now serves as a lecturer at Carnegie Mellon University and a federal consultant.When you see odd Web habits, "that's where you put the red flag on it, and you look for other indicators . . . to see whether or not to be worried about that behavior," said Meyerrose, who also served as CIO of three major U.S. Air Force Commands. Officials would not use a single indicator to persecute the next potential Snowden or Navy Yard shooter Aaron Alexis, who killed a dozen people.Watching cleared workers communicate in their free time is fair game."I used to conduct that all the time during exercises," in the military, Meyerrose said. “You know -- 'Loose lips sink ships,' those kinds of opsec. That’s been a part of the government culture since 1947,” with the enactment of the National Security Act mandating a major reorganization of the U.S. foreign policy and military establishments.The AP reported that the employee-surveillance "system could also link to outside databases to flag questionable behavior," and "investigators will analyze the information along with data separately collected from social media and, when necessary, polygraph tests."Background investigators, however,

say there are challenges in confirming the identity of individuals posting messages online."To me, if you're linking into social media, my first concern would be that whatever you're pulling is actually your applicant and not someone else," Smith said. "I think you still run a risk of verifying that that is your applicant's Facebook page."