

Civil liberties advocates call for more oversight of NSA surveillance

By: Grant Gross- June 21, 2013

Congress should press for privacy protections and more information about surveillance programs at the National Security Agency, some technology and civil liberties activists said Friday.

After recent news leaks about two broad surveillance programs at the NSA, it's clear that congressional and court oversight of the agency is lacking, representatives of the American Civil Liberties Union and the Cato Institute, a libertarian think tank, told congressional staffers during a briefing on the NSA programs.

Oversight of the surveillance programs by the Senate and House of Representatives intelligence committees has been "pretty feeble," Julian Sanchez, a research fellow at the Cato Institute, said at a surveillance forum hosted by the Congressional Internet Caucus Advisory Committee.

The limited number of lawmakers and the judges that are supposed to check the NSA programs appear to have fallen victim to a form of a governmental phenomenon called "regulatory capture," when a body that is supposed to regulate an industry begins to "serve its interests," Sanchez said.

Lawmakers outside the intelligence committees need to provide oversight of the programs, added Michelle Richardson, the ACLU's legislative counsel.

"So far, Congress has allowed the intelligence committees to do secret oversight of secret programs allowed under secret court orders, and it has led to the collection of every American's phone calls," she said. "This cannot continue. The secret oversight is not working."

Representatives of both intelligence committees didn't immediately respond to requests for comment on the criticism from Sanchez and Richardson.

When the Federal Bureau of Investigation asks the Foreign Intelligence Surveillance Court for a broad swath of U.S. telephone records, there's no opposing attorney, Richardson said.

"No one is representing the interests of the people whose records are collected," Richardson added. "It is just the government before a secret court, and no one is representing the other side."

Richardson and other speakers at the event called on Congress to add transparency to the surveillance court process.

The mass collection of data on U.S. phone calls and Internet communications under the two programs represents a “dangerous shift” in the way the government views the Fourth Amendment to the Constitution protecting U.S. residents from unreasonable searches and seizures, Sanchez said. There appear to be fewer prohibitions on the government collecting data and more mass collection, with some restrictions on how intelligence agencies can access the data they have collected, he said.

“Analysts themselves have the discretion to select which things are going to be queried for search,” he added. “Back-end restrictions on what you do [with the collected data] last only until you decide to change them, and the record so far suggests we won’t necessarily know if they decide to change them.”

While four of the five speakers at the event said they were troubled by the surveillance programs, lawyer Michael Vatis, a former official at the FBI and the U.S. Department of Justice, said he wasn’t overly concerned about reports of the NSA collecting Internet communications from nine Web service providers.

The Prism collection program, as described, appears to give the NSA little new surveillance power than it has always had, said Vatis, now a partner in the Steptoe & Johnson law firm. The NSA’s longtime mission is to provide surveillance on overseas communications, and the Prism program appears to be an extension of that, he said. The NSA is targeting U.S. Web companies because much of the Internet’s traffic routes through the U.S., he said.

Vatis said he had some concerns about the NSA’s bulk collection of U.S. phone records, but he takes some comfort that the agency is collecting phone numbers and not the content of phone calls.

If the NSA and DOJ have strong procedures in place to protect privacy, as they say, then the data collection can help protect U.S. residents, Vatis added. “In the worst-case scenario, when an individual brings a suitcase nuke onto Wall Street and detonates it, the questions are going to be, ‘The government had this technical capability to keep track of people, but didn’t use it,’” he said. “That will be the scandal.”

Critics of the data collection were surprised about the “breadth of the order” allowing the NSA to collect all Verizon phone traffic, countered Alan Davidson, a visiting scholar in the Technology and Policy Program at the Massachusetts Institute of Technology and a former public policy director at Google.

The data collection raises not only civil liberties and privacy concerns but also business concerns, Davidson added. “If people don’t trust these services, they’re not going to use them,” he said.

Vatis discounted the business concern. “Have many people stopped using Gmail or Yahoo?” he said.