

New reports detail vast scale of NSA “mega data collection”

Thomas Gaist
17 June 2013

New reports indicate that the National Security Agency (NSA) engages in warrantless wiretapping of the audio content of telephone communications of Americans, and records and archives virtually all internet usage, everywhere.

The primary concern of the Obama administration, congressional leaders and intelligence officials is to lie and obfuscate in order to conceal the true nature and extent of the spying.

The rapid pace of new revelations has been catching leading representatives of the American state in one blatant lie after another. On almost a daily basis, new information surfaces illustrating the vast, all-pervading scale of the NSA surveillance apparatus.

Obama administration officials and congressmen have repeatedly asserted that the American government does not monitor the content of telephone and other communications without a warrant. During a House Judiciary hearing on Thursday, however, Representative Jerrold Nadler cited a secret briefing with US intelligence officials exposing these assertions as lies.

When FBI Director Robert Mueller claimed that the NSA required “a special, particularized order from the FISA court direct at that particular phone of that particular individual” in order to monitor communication content, Nadler responded, “We heard precisely the opposite at the briefing the other day. We heard precisely that you could get the specific information from that telephone simply based on an analyst deciding that...In other words, what you just said is incorrect. So there's a conflict.”

Nadler's comments corroborate Snowden's assertion that, working as a low-level analyst in Hawaii, he was able to “wiretap anyone from you or your accountant to a federal judge to even the president.”

Tim Clemente, a former FBI counterterrorism agent, told CNN last month that the FBI has the capacity to access the content of previously made telephone calls when they are considered relevant to national security. “All of that stuff is being captured as we speak whether we know it or like it or not,” said Clemente.

The *Washington Post* reported Saturday that an NSA program dubbed NUCLEON “intercepts telephone calls and routes the spoken words” into permanent storage, and that the Obama administration has “resolutely refused to offer an estimate of the number of Americans whose calls or emails have thus made their way into content databases such as NUCLEON.”

William Binney, a former NSA technical director heavily involved in setting up the agency's eavesdropping system, told the *Daily Caller* that at least 500,000 to 1 million people have been placed on a “target list” and have all their phone calls recorded. “They look through these phone numbers and they target those, and that's what they record,” Binney said.

In its article, the *Post* wrote that despite legal language specifying that STELLARWIND and its successor programs, including one called RAGTIME, should target foreigners, “the programs are structured broadly enough that they touch nearly every American household in some way.”

While the NSA is technically forbidden by law from monitoring Internet communications within the US, President George W Bush first authorized the agency to tap into the Internet's backbone of fiber optic cables in the wake of 9/11. The PRISM program, first revealed on June 6 in the *Guardian* and the *Washington Post*, has systematized and perfected these efforts, sucking up staggering quantities of data from numerous companies including Yahoo, Microsoft and Google.

The NSA has been tapping into the “backbone” of the

Internet since then, as part of a practice of “mega data collection.” According to a report in the Associated Press, by plugging into these “backbone” cables, the NSA collects staggering volumes of email, financial, internet, and other types of data.

According to the AP, “[I]nterviews with more than a dozen current and former government and technology officials and outside experts show that, while Prism has attracted the recent attention, the program actually is a relatively small part of a much more expansive and intrusive eavesdropping effort.” The NSA effort, the AP reported, “snatches data as it passes through the fiber optic cables that make up the Internet's backbone” and “copies Internet traffic as it enters and leaves the United States, then routes it to the NSA for analysis.”

The NSA retains all data gathered, including from Americans, in case it becomes relevant to a “national security investigation” at some point in the future. The agency is currently developing a new center in Utah for storing the gargantuan quantities of data accumulated through this method.

Wolf Ruzicka, CEO of EastBanc Technologies, said of the spying capacity detailed in the AP report: “I’m much more frightened and concerned about real-time monitoring on the Internet backbone. I cannot think of anything, outside of a face-to-face conversation, that they could not have access to.”

“You have to assume everything is being collected,” said Bruce Schneier, an expert on computer security and cryptography.

Commenting on the flurry of denials and evasions issuing from top officials in response to the revelations of surveillance, Schneier said, “Everyone is playing word games. No one is telling the truth.”

According to the AP, “With PRISM, the government gets a user’s entire email inbox. Every email, including contacts with American citizens, becomes government property. Once the NSA has an inbox, it can search its huge archives for information about everyone with whom the target communicated. All those people can be investigated, too.”

The AP wrote: “The US someday will have a new enemy. Two decades from now, the government could have a trove of American emails and phone records it can tap to investigate whatever Congress declares a threat to national security.”



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact