DAILY BEAST

NSA Chief Hedges on Future of Phone Surveillance Dragnet

Kevin Poulsen and Spencer Ackerman

March 6, 2019

Amidst huge technical problems with the latest iteration of its domestic post-9/11 activity, the NSA's director isn't committing to its renewal.

SAN FRANCISCO—The head of the National Security Agency is hedging on whether the surveillance giant will seek to retain a revamped database of Americans' phone records plagued with technical problems.

"We're in a deliberative process right now," said Gen. Paul Nakasone, speaking at the RSA security conference here Wednesday. "We will work very, very closely with the administration and the Congress."

It was Nakasone's first public comments about the phone-logs program since the New York Times reported Monday night that a senior congressional aide stated the NSA had quietly shut the program down. Nakasone merely said he was "aware" of the Timesreporting and did not confirm or deny it.

The authority underpinning the program is a 2015 law, the USA Freedom Act, passed to curb the NSA's bulk collection of Americans domestic phone data, disclosed by Edward Snowden in 2013. The USA Freedom Act is set to expire on Dec. 15, and Nakasone did not commit to seeking its renewal.

The uncertain future of the USA Freedom Act is the latest twist over a surveillance activity begun secretly and warrantlessly after 9/11. Over a variety of iterations, the NSA has harvested Americans' domestic phone data in bulk. The USA FREEDOM Act, a compromise that neither the NSA nor privacy advocates loved, shifted the burden for conducting massive analysis of phone logs, ostensibly to reveal connections between Americans and foreign terrorists. After Snowden revealed that the program was collecting millions' of Americans' call logs daily, U.S. officials were forced to concede the program had not thwarted a single terrorist attack.

But the post-2015 transformation has been plagued with problems. Last June, the NSA shocked observers by deleting its entire USA FREEDOM Act database—a database that had amassed 685 million call records in the prior two years alone. The phone companies, under the law, were now performing massive phone-data analysis on behalf of the NSA, and had been supplying the agency with data it "was not authorized to receive"—and so the agency purged three years' worth of data wholesale.

On a Lawfare podcast this weekend, an aide to Kevin McCarthy, the House GOP leader who is one of eight legislators privy to the country's top intelligence secrets, said that after the purge, the NSA stopped using the USA FREEDOM Act phone data. The aide was skeptical that the administration would seek renewal of the USA FREEDOM Act.

"That expires at the end of this year, but the administration actually hasn't been using it for the past six months because of problems with the way which that information was collected, and possibly collecting on U.S. citizens in the way that was transferred from private companies to the administration after getting FISA Court approval," said the aide, Luke Murry, in an exchange first reported by the Times.

"So if the administration does ask on that, that's inherently a very sensitive subject, and we've seen that sensitivity be true in other areas of USA Freedom Act and I think that's going to be a real challenge for Congress," Murry said. "But I'm not actually sure the administration will want to start that back up given where they've been over the past six months."

The NSA told The Daily Beast Monday night it would not respond to questions about the future of the USA FREEDOM Act.

Several observers are skeptical that the NSA has actually ended a surveillance activity that it has performed for a generation. They noted the NSA's tendency to migrate surveillance across different legal authorities as convenient. Liza Gotein of the Brennan Center at New York University Law School and Julian Sanchez of the Cato Institute said that the NSA might be able to replicate the activity under a passel of authorities, including a Reagan-era executive order known as 12333 or a weakness in the Electronic Communications Privacy Act.

Sanchez, however, noted that the rise in encrypted communications tools like Signal, which would not show up in an NSA-useful way in phone company records, might have inclined the agency to think the activity wasn't worth salvaging.

"If their argument is, 'you need the haystack' [to find terrorist connections], it's not how people really communicate any more, certainly not [anyone] with a modicum of operational security," Sanchez said.

Surveillance critics said that the fallow database indicated that legislators ought to let the USA FREEDOM Act die.

"It is increasingly clear to me that the NSA's implementation of reforms to the phone records dragnet has been fundamentally flawed," Sen. Ron Wyden (D-Ore.), a member of the Senate intelligence committee, said in a statement Tuesday. "In my view, the administration must permanently end the phone records program and Congress should refuse to reauthorize it later this year."

Nakasone also used his keynote address to take a victory lap over a supposed U.S. cyber attack that reportedly gummed up part of Russia's election interference apparatus last year, though he didn't confirm or expand on the details.

"I am very proud of the work that was done in Cyber Command and the National Security Agency," he said. "We acted with speed, agility and purpose."

The Washington Post reported that Cyber Command, the U.S. combatant command dedicated to online warfighting, staged an assault against Russia's Internet Research Agency last November that swept the troll farm off the Internet on election day, and kept it off for days afterwards. According to NBC News, the hack attack was directly authorized by President Trump.

Wearing his second hat as Cyber Command's leader, Nakasone said a full range of U.S. state and federal agencies worked together to protect the 2018 midterm election from foreign disruption or interference. The NSA, for example, shared technical indicators of foreign hacks with the FBI and DHS, who passed them on to state election officials.

But he also described Cyber Command as having a uniquely pro-active role to play in tamping down foreign aggression. "We're going to be outside of the United States states to make sure that we understand what our adversaries are doing ... and then, if necessary and authorized, we're going to act against those adversaries."

He expects more such actions to follow.

Nakasone described the U.S. as entering a new phase of continuous, low-level "persistent engagement" in cyberspace, after many years of American inaction. "I think what's changed over the past year is the idea that as a nation, we have to have a more proactive, forward-leaning approach to our nation's defense in cyberspace," he said.

And he said he expects that the tempo in the secret war in cyberspace is only going to increase.

"The best thing that we can do is continue to understand our adversaries," he said. "2020 begins now.... We anticipate it's going to be a very interesting election year."