INTERNATIONAL BUSINESS TIMES

NSA FISA Controversy: What Illegal Activity Is Hidden In The Secret FISA Court Opinion?

By: Pema Levy – July 3, 2013

In response to leaked documents detailing the expansive surveillance activities of the National Security Agency, the Obama administration and top intelligence officials have tried to reassure Americans that the NSA's activities are legal and respect their privacy. But a secret court opinion from 2011 proves that, even under the lenient supervision of the Foreign Intelligence Surveillance Court, this has not always been the case.

In 2011, the FISC, which issues secret opinions and orders overseeing the NSA's eavesdropping activities, ruled that some of the government's surveillance activity violated the Fourth Amendment. But because the opinion is classified, only vague details about what the illegal conduct could be are known to the public. To get the full story, the Electronic Frontier Foundation, a digital rights group, is suing the Department of Justice for the release of the opinion. (The International Business Times reported on the details of the case last week.)

If the EFF is successful, Americans will find out more details about how the NSA crossed the line in the course of its enormous data collection efforts. But without the opinion, deducing what's in it is a guessing game based on a few known facts.

What is known is that the unconstitutional activity involved the collection of data under Section 702 of the 2008 FISA Amendments Act, the provision under which the NSA collects the online communications of foreign persons outside the United States or communications between one person in the U.S. and another non-citizen outside the country. (The NSA is not supposed to snoop if both parties to a message are citizens.) Section 702, for example, provides the authority for the bulk data collection conducted under PRISM, one of the programs revealed by confessed leaker Edward Snowden. The second known fact about the case is that it had to do with so-called "minimization procedures," the guidelines for how the NSA handles the domestic communications it inadvertently sweeps up while snooping on a foreign target.

We know these two things -- and the very existence of the opinion -- because of Sen. Ron Wyden, D-Ore., who in 2012 got the Office of the Director of National Intelligence to allow him to publish two statements vaguely referring to the FISC decision.

- [O]n at least one occasion, the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment.
- I believe that the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion the FISA court has reached the same conclusion.

Though no one knows anything for sure, privacy experts think it's likely that the NSA was involved in a broad data collection effort that didn't sufficiently filter out Americans' communications while going after a foreign target.

One theory is that the minimization procedures themselves led to unconstitutional collection. Much of what we know about the NSA's minimization procedures come from 2009 documents leaked by Snowden. It's not publicly known whether those documents have been updated, or whether they led to the unconstitutional activity in the 2011 opinion. But the 2009 procedures raised eyebrows among privacy advocates for the loopholes that allowed them to collect, examine and retain Americans' communications under the FAA.

"The system as a whole seems set up to guarantee that a large number of those communications will be pulled in and the government can go through them, it can keep them, it can turn them over to other law enforcement authorities for criminal prosecution purposes," Patrick Toomey, a fellow at the American Civil Liberties Union's National Security Project, said in reference to the 2009 procedures. The secret opinion could concern "a lot of similar kind of techniques or procedures that are built into the law that pull in U.S. communications even while allowing the government to deny, as we've heard them do repeatedly, that they're targeting U.S. persons."

Given the red flags privacy advocates see in the NSA procedures that have been made public, as well as past violations that are now known, surveillance expert Julian Sanchez of the libertarian Cato Institute says there are a number of possible scenarios that could have led to over-collection. Here are some of those possible scenarios.

First, the NSA has argued that instead of being limited to collecting communications between someone in the U.S. and the foreign target, agency analysts can collect communications about the target but not to or from the target -- as long as at least one of the parties is a foreigner outside the country. For instance, the target might be Osama bin Laden, but the NSA decides to go after people who are talking about bin Laden. According to Sanchez, this kind of scenario can lead to snooping on an email address or phone line "in some unreasonably broad way" that would turn up an unacceptable number of totally domestic communications.

Similarly, in trying to pick up emails about a target, the NSA could have been using overly broad search criteria for what emails it collects, such as signifiers in the content of the emails or ranges of IP addresses, that brought in too many domestic communications. "If you're off by a number" when searching a range of IP addresses, "it might mean you get 10,000 people's emails that are beyond the scope of your authority," Sanchez said.

A second scenario could involve targeting a foreign corporation that has, for example, a website server based in the U.S. Targeting that domestic server on the pretense that it belongs to the foreign target could result in a large number of domestic emails, or even emails that are one-end foreign but are still beyond the scope of the NSA's authority.

This kind of problem was hinted at by a senior intelligence official speaking to The New York Times in 2009. "Say you get an order to monitor a block of 1,000 e-mail addresses

at a big corporation, and instead of just monitoring those, the NSA also monitors another block of 1,000 e-mail addresses at that corporation," the official said. "That is the kind of problem they had." Though the 2009 problem was reportedly resolved, Sanchez said this could be "a distinct incident but not necessarily a distinct issue."

A third option is overly broad targeting of a foreign power or the communications registered to a foreign company, says Sanchez, activity that has been flagged as problematic in the past. For example, perhaps the NSA went beyond its Section 702 authority by targeting all emails coming in and out of a certain country. Or, they could have decided to pick up all emails addresses of a foreign company -- say, all the addresses registered to a foreign version of Hotmail -- on the pretense that the people using the service were probably foreign and outside the U.S.

Whatever it turns out to be, some privacy advocates are optimistic that at least a portion of the secret ruling will eventually come out and at least some of the illegal activity will become known. "We think that the government is over-collecting in very dramatic ways," Toomey said.