WIRED

A Big Change in NSA Spying Marks a Win for American Privacy

Andy Greenberg

April 28, 2017

The charter of the National Security Agency limits its powerful surveillance to the rest of the world, not US citizens. But one controversial carve-out in NSA rules has for years allowed it to vacuum up communications that aren't "to" or "from" a foreign target, but merely "about" one—no matter who sends or receives it. Now the NSA says it will end that practice. And in doing so, it concedes a significant win to the privacy advocates who have fought it for years.

The loophole the NSA is closing, as first reported by the New York Times, falls under the 702 provision of the Foreign Intelligence Surveillance Act. The NSA's interpretation of FISA allowed it to search the vast firehose of internet data that passed through its wiretaps of fiberoptic cables for certain "selectors," or search terms, and collect that data if any part of the communication passed outside the US—even if one or both people communicating were in fact Americans.

"NSA will no longer collect certain internet communications that merely mention a foreign intelligence target," reads a statement from the agency. "Instead, NSA will limit such collection to internet communications that are sent directly to or from a foreign target."

About Time

Exactly why the NSA decided to end those "about" searches still isn't entirely clear. But privacy advocates are cautiously declaring a victory.

"The problem of this kind of 'about' searching is that it meant actually scanning the contents of every email to see if the messages contain the target selector," says Robyn Greene, policy counsel at the Open Technology Institute. "That implicates foreign affairs, human rights activism abroad, international businesspeople, lawyers who work internationally and researchers…Stopping 'about' collection is a huge boon to privacy for both Americans and individuals abroad."

For at least a decade, the NSA has interpreted FISA to allow it to collect so-called "upstream" data based on search terms that go beyond merely who send or received it. It also takes into account strings of information that might be included in the communications, like an email address, phone number, IP address, or the "signature" that identifies a certain piece of malware.

In 2008, the Foreign Intelligence Surveillance Court, which serves as the judicial watchdog for the NSA's potential privacy violations, approved that legal interpretation in a classified ruling.

The practice has remained contentious. Privacy advocates argue that it's unconstitutionally indiscriminate, violating Fourth Amendment protections from warrantless searches of US citizens. Any American communicating about a certain selector could have their communications caught in the NSA's dragnet if their communications simply pass through a foreign server, something they have little or no control over. "This could just be two people talking something, or a reporter writing a certain email address. It really broadens the aperture for the collection of communications without a warrant," says Andrew Crocker, an attorney with digital rights group EFF. "In our view, it's been unconstitutional all along."

It also happens frequently. In 2011, for instance, the FISC revealed an estimate that about .2 percent were between Americans, amounting to tens of thousands of individual communications. The same year, it blocked the NSA from doing any upstream data collection for close to six months, though it never revealed why. In 2014, a report by the White House's Privacy and Civil Liberties Oversight Board raised the issue of the broad, indiscriminate targeting of "about" searches once again.

That board also pointed to the problem exacerbated by so-called Multi-Communication Transactions: Due to the complexities of how data is packaged and moves around the internet, the NSA's filter pulled in entire bundles of digital communications despite many of the messages containing nothing to do with the target selector. "You would have one message that met the conditions to trigger collection, and then whoops, they got everything else in the same package including totally domestic emails," says Julian Sanchez, a privacy-focused research fellow with the Cato Institute.

Legal Remedy

To deal with those inherent problems, the NSA at some point agreed to store the domestic communications it collected with special protections, and only grant access to analysts under certain, secret conditions. In its public statement, though, the NSA conceded to "inadvertent compliance lapses," indicating that those special procedures failed. After reporting the violations to Congress and the FISC, the NSA decided to cease its "about" collection altogether, and even to delete older data collected under the practice.

"Even though the Agency was legally allowed to retain such 'about' information previously collected under Section 702, the NSA will delete the vast majority of its upstream internet data to further protect the privacy of US person communications," the NSA statement reads.

But while privacy advocates applaud that move, they also argue it's not enough. Instead of leaving the decision to the NSA's discretion or secret court rulings, Congress should encode the rollback in law when it renews the Foreign Intelligence Surveillance Act later this year, says OTI's Robyn Greene. "We need to codify an end to 'about' collection in the law," says Green, "This decision doesn't reduce that need for legislative reform, it highlights the need." In response to the NSA's statement, Senate Intelligence Committee member Ron Wyden said he intended to introduce that very legislation.

Privacy advocates now hope that the NSA's decision to stop the "about" searches might reduce