JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

All About "About" Collection

Julian Sanchez

April 28, 2017

The National Security Agency announced Friday that it will be halting a controversial form of collection it had been conducting under Section 702 of the FISA Amendments Act—so called "about" collection. I had heard such an announcement was slated for next week, but appears to have been bumped up in response to a *New York Times* story that reported the shift in policy on Friday afternoon. So: What does this mean, and how big a deal is it?

First, what exactly is "about" collection? Normally we think of surveillance as involving the interception of communications *to* or *from* the target of surveillance: You designate a particular e-mail address, for example, as a "selector" and then "task" collection of messages to or from that address. That's roughly how things work with respect to "downstream" (formerly "PRISM") collection under §702, which is conducted with the direct assistance of U.S. communications platforms like Google (which owns Gmail) or Microsoft (which owns Hotmail). But the NSA also conducts so-called "Upstream" surveillance, vacuuming traffic directly off the Internet backbone—a somewhat messier process that among other things enables them to capture communications that are tranisiting *through* the United States, but may not be destined for an e-mail server located *in* the United States. When conducting Upstream surveillance, NSA did not restrict itself to scanning for selectors in e-mail headers—messages sent to or from one of their foreign targets—but also sucked up messages that included a selector in the body of the message. Thus, an e-mail from an American that was neither to nor from a foreign target, but only contained that person's e-mail address, might be intercepted as a result.

It's important to note that nothing in the statutory text of §702 explicitly authorizes such surveillance. Indeed, when the Supreme Court rejected a challenge to §702 in *Clapper v. Amnesty International*, the Court's opinion presumed (wrongly) that only by being in direct communication with one of the roughly 95,000 "targets" of §702 surveillance could an American's communications be intercepted under that authority. What the Court—and seemingly many members of Congress who voted for §702—failed to appreciate was that the intelligence community's definition of "target" is not so restrictive. Rather, as the legislative history of the original Foreign Intelligence Surveillance Act makes clear, our spy agencies define the "target" of surveillance as the "individual or entity *about whom* or from whom information is sought." That original FISA House Report goes on to explicitly acknowledge that: "In most cases this would be the person or entity at whom the surveillance [or other acquisition activity] is physically directed … but this is not necessarily so." As I noted back in 2012, the government had already creatively used this definition to argue that surveillance of a U.S. person's home and mobile telephones had actually been "directed at" a foreign target, Al Qaeda, rather than the person whose phones had been tapped. So the loophole that permitted "about" searches was in

principle apparent to anyone familiar with the legal meaning of "target" for intelligence purposes, but it does not appear to have been widely understood that the NSA was exploiting this to search the contents of e-mails under §702 until it was disclosed by *The New York Times* back in 2013.

This practice of scanning e-mail traffic for the purpose of "about" searches has long been one of the aspects of §702 collection most objectionable to civil libertarians, for several reasons. First, and most fundamentally, it inverts the normal order of operations for surveillance. Instead of scrutinizing the contents of the communications of a particular individual who has been designated as a target, it scrutinizes the contents of all communications, and uses the results of that automated scrutiny as the justification for collecting a particular message. In effect, a search is justified not by some antecedent grounds for suspicion, but by *the results of the search itself.*

Second, and somewhat more legalistically, "about" collection seems hard to square with the Foreign Intelligence Surveillance Court's own understanding of the purported "foreign intelligence exception" to the Fourth Amendment's warrant requirement. According to partially declassified FISC opinions, a particularized warrant based on probable cause is not needed to intercept communications—even the communications of an American citizen—sent to or from an agent of a foreign power. But, of course, even if §702 "targets" are in practice limited to foreign agents—a restriction not found in the text of the statute—there is no reason to think a message that is merely *about* a target satisfies the exception, rendering it mysterious why interception would be constitutionally permissible absent a particularized probable cause warrant.

Third, because "about" collection involves messages that are not necessarily either to or from a particular, known foreign target reasonably believed to be abroad—as targets of §702 must be—there is necessarily a greater risk that "about" collection will intercept wholly domestic messages. While NSA employs a variety of filters meant to avoid this, a substantial part of the justification for §702 was precisely that it is often difficult to be confident in realtime where the endpoints of an Internet communication are located. Thus collection of communications to which neither party is a known foreign targets inherently risks collection of messages whose sender and recipients are both located in the United States, even if measures are taken to filter out the most obviously domestic messages.

Why the recent change, then? Well, as Marcy Wheeler recently noticed, the FISC does not appear to have issued an order last year approving §702 surveillance. The statement by NSA announcing the change in policy alludes to some "inadvertent compliance incidents related to queries involving U.S. person information in 702 'upstream' internet collection," resulting in delays in the court's approval of the annual §702 certification. That suggests the FISC may have been troubled either by the sheer volume of domestic content being swept in as a result of "about" searches, or in the inability of analysts to follow rules governing how that pool of data could be accessed. Oversight bodies—and the general public—should certainly be pressing for more information about the nature of these "compliance incidents."

How significant is the shift? For all the reasons discussed above, civil libertarians should surely welcome this announcement, but a few caveats are in order. First, it is entirely possible that the change is driven in significant part by the broader post-Snowden adoption of STARTTLS encryption of communications between e-mail servers. That is, it is quite plausible that a large and growing percentage of transiting e-mail traffic is simply no longer

visible to NSA, and must be accessed "downstream" at the e-mail server itself, rendering this form of collection less worth picking fights with the FISC over. Second, to the extent the traffic remains visible to NSA, they may simply have decided that it is easier to do the same "about" scans outside the borders of the United States, beyond the purview of either FISA or the FISC.

Finally, it is worth noting that it is rather hard to square NSA's statements today with the characterization of "about" surveillance that appears to have been taken on faith by the Privacy and Civil Liberties Oversight Board in its report on §702. The PCLOB accepted "about" collection as a matter of technical necessity—something the NSA *had* to do in the course of collecting messages "to" or "from" its foreign targets. As Robert Chesney observes at Lawfare, NSA's latest statement appears to tacitly acknowledge that this is simply not so, as plenty of folks who understand how e-mail operates suspected from the outset. Rather, the release today seems to acknowledge that forsaking "about" collection may also require missing *some* messages to or from the target, it is in general perfectly possible to restrict collection to the latter category without "gutting" the program altogether. This suggests that when judges or oversight bodies are evaluating claims of "technical necessity" as justifications for some intrusive technique, they ought at the very least to run those claims by an actual technologist outside the agency making the request.

Julian Sanchez is a senior fellow at the Cato Institute and contributing editor for Reason magazine. Follow him on Twitter (@normative).