BRENNAN CENTER FOR JUSTICE

October 2017

Reducing "Incidental" Collection Under FISA Section 702: A Critical Protection for Americans

The Top Line

Under current law, the National Security Agency (NSA) could be collecting millions of innocent Americans' communications each year without a warrant. That's largely because Section 702 allows the NSA to target ordinary people in other countries—not just government officials or suspected terrorists—and collect all of their communications with Americans. Limiting the permissible pool of foreign targets to people who reasonably might have information about threats to our security would help ensure that large numbers of law-abiding Americans don't get caught in the net.

The Problem

Section 702 allows the NSA to target foreigners overseas and collect their calls and e-mails—including those with Americans—without obtaining a warrant. Because the target is the foreigner, Americans' communications are obtained only "incidentally."

The wider the pool of permissible foreign targets, however, the greater the volume of "incidental" collection. And when targets can be ordinary people who are not suspected of any wrongdoing, the resulting surveillance could potentially sweep in millions of wholly innocent conversations between Americans and their friends, relatives, and business associates overseas.

Under current law, the NSA may target anyone reasonably believed to be a foreigner overseas. A significant purpose of collection must be the acquisition of "foreign intelligence information." But that term is defined so broadly, it could permit surveillance of conversations about current events. A conversation between friends about the merits of the North American Free Trade Agreement, for instance, would qualify as "foreign intelligence information" because it is information that "relates to . . . the conduct of the foreign affairs of the United States." **In other words, the pool of permissible foreign targets is almost unlimited—opening the floodgates to mass "incidental" collection of law-abiding Americans' communications.**

This problem can't be cured by strengthening "minimization" procedures—the official agency rules that provide some limits on the retention, sharing, and use of communications after collection. Even with the strongest privacy protections in place, massive amounts of innocent Americans' communications would still be sitting in the databases of intelligence and law enforcement agencies, where they are vulnerable to hacking or data theft, inadvertent mishandling (a problem that has plagued Section 702 since its inception), and potential abuse.

Minimization procedures also won't remove the looming threat to the U.S. technology sector. In 2015, the European Court of Justice struck down an agreement governing data transfers between U.S. and EU companies, largely because Section 702 gave the NSA broad access to Europeans' data held by U.S. companies. Although the EU recently approved a new agreement, experts agree that European courts are likely to strike it down again if Section 702 isn't amended to be more narrowly tailored to actual threats. That would strike a devastating blow to the U.S. tech industry's competitiveness in the world market.

The Solution

The only way to reduce unnecessary "incidental" collection and the dangers its poses to Americans' privacy is to narrow the pool of permissible targets to those who might reasonably have useful information.

The government should continue to be able to target any foreigner overseas when seeking to protect against the specific threats to national security identified in 50 U.S.C. § 1801(e)(1). But if it seeks to obtain information that merely "relates to" national security or foreign affairs generally (as permitted under 50 U.S.C. § 1801(e)(2)), it should have a reasonable belief that its targets are "foreign powers" or "agents of foreign powers"—terms broadly defined in FISA to include not only foreign governments and government-controlled entities, but political factions and terrorist groups.

This change would be easy to implement. It could simply be incorporated into the government's existing targeting procedures, since the "reasonable belief" determination would be an internal one—the government would not have to seek FISA Court approval.

There is no reason to think that this important reform would inhibit the collection of needed threat information. The government has made public several Section 702 success stories; ***the change proposed here would not have limited the surveillance in any of those cases.*** In the often-cited case of Najibullah Zazi, for instance, the target of Section 702 surveillance was a known Al Qaeda courier in Pakistan. And although many other success stories remain classified, we know from intelligence officials' general description of them that the government typically started with a reasonable belief that the target had terrorist ties.

Narrowing the scope of collection in this sensible way would be a critical protection for the millions of Americans who have no connections to terrorists or foreign powers, but who regularly communicate with ordinary people in other countries. It would also help insulate the new U.S.-EU data-sharing agreement from legal attack, preserving and protecting U.S. technology companies' ability to do business overseas.

***

If you have questions about this document or other aspects of Section 702, please contact Elizabeth Goitein at 202-249-7192 or elizabeth.goitein@nyu.edu.