BRENNAN CENTER FOR JUSTICE

August 2017

Reforming Section 702: We Can Protect Americans' Privacy *and* Protect Against Foreign Threats

The Top Line

Section 702 of FISA was enacted in 2008 to give the government more powerful tools to use against foreign threats. The law allows the government to collect the communications of foreign targets without obtaining a warrant, even when the communications pass through or are stored inside the United States. Intelligence officials report that it's been a critical tool to monitor suspected foreign terrorists, discover their networks, and disrupt their plots.

But Section 702 has also had some unintended consequences and uses, which have become much more apparent since it was last reauthorized in 2012. Because some of the statutory language is ambiguous or simply overbroad, surveillance under Section 702 unnecessarily pulls in a massive amount of *Americans*' communications. The protections for this "incidentally" collected data have far too many loopholes. As a result, the government is using Section 702 to read Americans' e-mails and listen to their phone calls without a warrant – something Congress never intended. Moreover, the loose definitions in the statute are threatening the global competitiveness of the U.S. tech industry.

Fortunately, there are surgical solutions that will leave intact the core of Section 702 – the ability to conduct surveillance of foreign threats without obtaining a warrant – while better protecting the rights of Americans and the economic interests of our country.

Problems and Solutions

Problem: The law's overbroad language sweeps in too many innocent citizens. Although the statute's goal was to facilitate surveillance of suspected foreign terrorists and other legitimate foreign targets, it was written broadly enough to permit surveillance of *any* foreigner overseas. The only limit is that the government's purpose must be to collect "foreign intelligence information." But that term is defined so broadly, it could include conversations about current events.

This creates two problems. First, Section 702 allows the government to collect *all* of the targets' communications – including those with Americans. Some collection of innocent Americans' communications is unavoidable, even when targeting suspected terrorists. But if the government can target ordinary people in other countries, it will inevitably sweep in vast amounts of innocent conversations between law-abiding Americans and their friends, relatives, and associates overseas.

Second, the government's ability to target even completely innocent foreigners overseas is creating enormous (and unnecessary) problems for the U.S. tech sector. European courts are striking down data sharing agreements between U.S. and EU companies because there are so few limitations on the NSA's ability to acquire the data. Major U.S. tech companies are pressing for sensible reforms to Section 702 that will allow them to remain competitive in the global marketplace.

Solution: Congress should require the government to have a reasonable belief that targets of surveillance are foreign powers or agents of foreign powers, or that they pose a threat to the nation's security or have information about such a threat. Intelligence officials' public descriptions of Section 702 "success stories" all involved targets who would easily meet these criteria, so this change will not diminish the law's effectiveness.

Problem: Agency rules allow the government to examine Americans' communications without a warrant. Congress expressly prohibited "reverse targeting" – i.e., using Section 702 collection to get at Americans' communications. That's because the Constitution requires the government to get a warrant when an American is the target. To initiate collection under Section 702, the government must certify to the FISA Court that it has no interest in getting information on any particular, known Americans.

And yet, the moment the communications land in agencies' databases, internal agency rules allow them to sift through the data, searching for phone calls and e-mails of particular, known Americans – *the very people in whom they just denied having any interest*. The FBI can even use these communications in criminal cases that have nothing to do with foreign intelligence or national security.

This is a bait and switch that violates the spirit, if not the letter, of Congress's ban on reverse targeting. It also creates a dangerous end run around the Fourth Amendment. The government should not read Americans' e-mails or listen to their phone calls without a warrant – period.

Solution: Congress should require the government to obtain a warrant before searching Section 702 data for Americans' communications. Contrary to what some opponents of reform have suggested, restrictions on searches of lawfully obtained data are commonplace – and vital to preserving Fourth Amendment freedoms in the digital age.

Problem: "About" collection sweeps in domestic conversations. For years, when collecting communications that were in transit over the Internet backbone (known as "upstream" collection), the NSA acquired not just communications *to* or *from* targets, but communications that merely *mentioned* their e-mail addresses or other information about them. Section 702 does not expressly authorize this so-called "about" collection, but the NSA claimed it was a technical necessity.

Communications that merely mention information relating to a target are much more likely to be entirely innocent and wholly domestic (i.e., American-to-American). For this reason, the FISA Court placed special restrictions on data obtained through upstream collection. When the NSA proved unable to comply with those limits, it chose to discontinue "about collection" in order to avoid a showdown with the FISA Court. But it reserved the right to restart "about" collection in the future.

Solution: Congress should codify the end of "about" collection. Intelligence officials report that "about" collection comprises a tiny fraction of upstream collection, which itself amounts to less than 10% of Section 702 surveillance. While the practice is thus a very small part of Section 702, it presents uniquely significant privacy concerns. This is a clear case of the risks outweighing the benefits.

***

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.