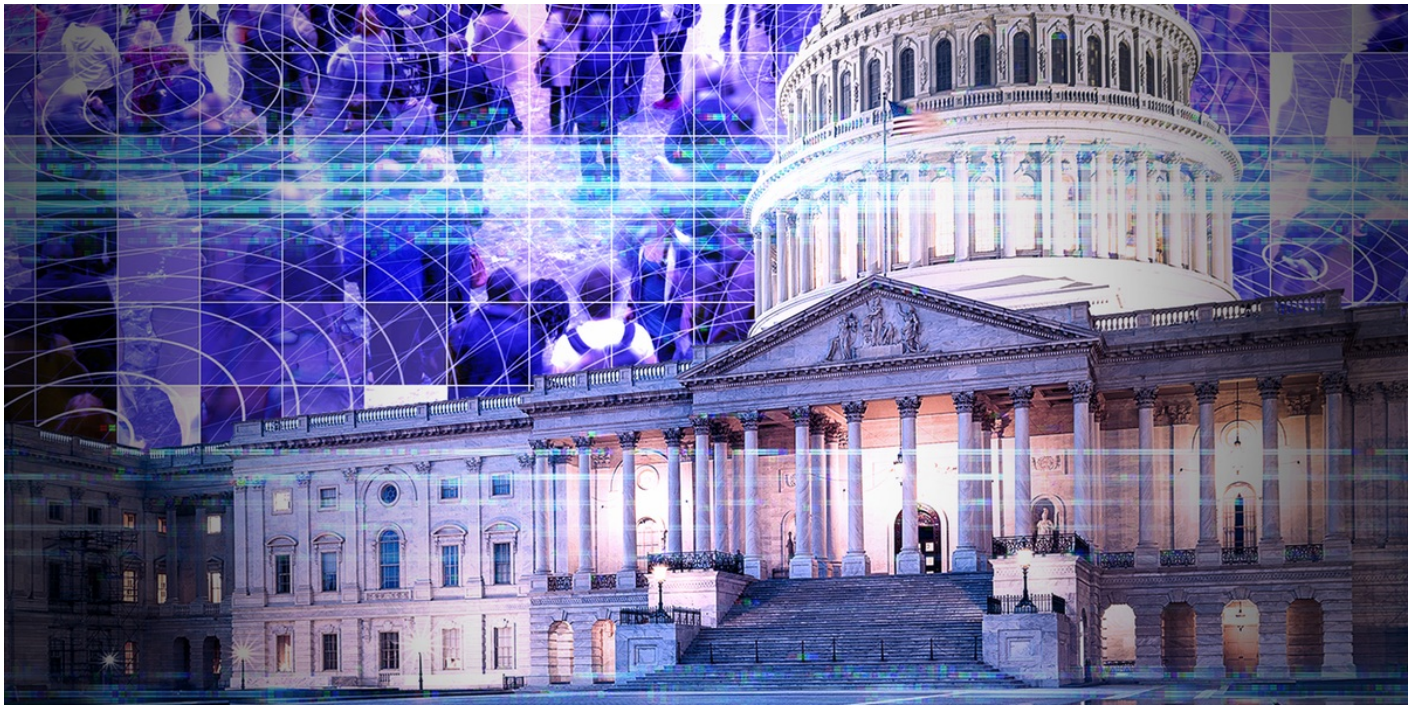
THE CENTURY FOUNDATION | 1919 2019



REPORT SURVEILLANCE & PRIVACY

Will Congress Vote to End Warrantless Surveillance of Millions of Americans?

JANUARY 10, 2018 — BARTON GELLMAN AND LAURA K. DONOHUE

In 2008, Congress amended the Foreign Intelligence Surveillance Act (FISA) to grant expansive new powers to the NSA and FBI. One of the amendments, known as Section 702, was so controversial that Congress added a "sunset clause," meaning the law was supposed to expire at the end of 2017 unless Congress renewed it. At the end of December, Congress kicked the can into the new year by passing a short-term extension. With a government shutdown looming, lawmakers have until January 19 to decide FISA 702's fate. I invited a leading player in the behind-the-scenes debate to talk with me about what's at stake in this decision.

Congress is split at least three ways, with unusual coalitions that cross party lines. The choices are to renew the law exactly as is, let it die, or amend it to address what privacy advocates, myself included, regard as significant flaws.

Laura K. Donohue, who is a professor of law at Georgetown and runs the Center on National Security and the Law, joins me in the conversation transcribed below. In the nearly forty-year history of the Foreign Intelligence Surveillance Court, which meets in secret to oversee these surveillance programs, it was only in 2015 that Congress amended the law to require the court to appoint five amici to provide a counterpoise to the executive branch when novel questions of constitutional law arise. Donohue is one of them. She is also a leading advocate for reform of Section 702. (Here's an influential argument she published with the Council on Foreign Relations.)

Before we jump into the conversation, some quick context:

Section 702 is important because it allows intelligence agencies to intercept electronic communications on U.S. territory for foreign intelligence purposes without prior approval of a court—a practice that had been outlawed for decades. Under that legal authority, the NSA scoops up international communications as they pass through large internet switches in the United States, and the FBI, on NSA's behalf, collects email, chats, photos, documents, and other electronic data stored by U.S. companies such as Google, Yahoo, and Microsoft.

The "targets" of this kind of surveillance have to be foreign nationals. Even so, a lot of Americans—the NSA says it can't count how many—are also swept in. One important point to understand, as you read on, is that Section 702 allows intelligence agencies to choose their targets without disclosing or defending them in court. The FISC approves a set of rules and procedures once a year and the government promises to follow them. But the government does not have to tell a judge who it is spying on or why.

My 2014 reporting for the *Washington Post*, based on files provided to me by Edward Snowden, showed that Section 702 has allowed the U.S. government to collect electronic information on a far larger scale that it had before and that a significant portion of it included U.S. citizens or permanent residents. After the Snowden disclosures, the lion's share of attention in Congress and in public debate went to another program—the collection of U.S. call records, which reveal

who talks to whom and when. The law we discuss today lets the NSA collect the *contents* of emails, personal photographs, spreadsheets, business documents, and video streams without a particularized warrant from a judge. The words, voices, and images may belong to Americans. Those are collected "incidentally," a term of art that means they were not deliberately targeted. What happens to them afterward is a major point of debate.

Despite President Trump's short-lived anxiety about domestic "wiretapps," and numerous charges as to the unconstitutionality of the executive branch's current actions, the White House has endorsed the intelligence community's request for a clean renewal of the expiring law, without any privacy-enhancing reforms.

This transcript has been edited for length and clarity.

Barton Gellman: So here's the background. In 1978 and for forty years afterward, U.S. intelligence agencies had strict limits on their power to eavesdrop on Americans or on foreigners in America to collect foreign intelligence. The law, which was passed in response to the domestic surveillance scandals of the Johnson and Nixon years, was called the Foreign Intelligence Surveillance Act (FISA). Congress amended it in 2008 and added new powers; those amendments were reauthorized in 2012.

One part of the 2008 amendment, called Section 702, is what Congress is debating now. So Laura, what is Section 702 and why does it matter?

Laura Donohue: Section 702 was introduced as part of the 2008 FISA Amendments Act after revelations about President Bush's "Terrorist Surveillance Program." In the wake of 9/11, the government had been warrantlessly wiretapping internet and telephone communications inside the United States, as well as between the United States and abroad, entirely outside FISA.

Gellman: And without telling almost anyone in Congress or in the judiciary about it.

Donohue: Yes. Bush had clearly violated the statute. It was a constitutional moment: Congress and the Executive share foreign affairs power. When the president acts against the direction of Congress—which had explicitly stated in 1978 that FISA was to be the *sole* means via which the Executive could conduct domestic electronic surveillance—then he is at his "lowest ebb" of power. And the courts were on the legislature's side. In 1972, in a case called *U.S. v. U.S. District Court*, the Supreme Court required that the executive branch obtain some sort of warrant for surveillance in cases of domestic security, in order to satisfy the Fourth Amendment. The 1978 law made good on that demand. But the president just ignored it.

In the fallout that came after that, the intelligence community made an argument—a good one—that when you have, say, two foreign terrorists communicating overseas, but they're communicating through the United States—that is, using a U.S. internet service provider—it is troublesome that we would require the government to go to the Foreign Intelligence Surveillance Court (FISC) to monitor them. Traditionally, if two non-U.S. citizens based overseas were communicating over foreign telephone wires, you wouldn't expect the CIA or the NSA to have to get a court order to listen to them. But with the internet, that changes.

Gellman: Right. This a new problem because the internet doesn't respect geography.

Donohue: Or international borders.

Gellman: You could call France from Germany, and your call may pass through switches in the United States.

Donohue: Exactly. So the 2008 FISA Amendment Acts tried to address this by saying, we can collect communications inside the United States of non-U.S. persons reasonably believed to be outside the United States, for up to one year. The attorney general and the director of national intelligence name the target, and then that target can be put under surveillance. The FISC approves a set of general rules—targeting and "minimization" procedures meant to reduce the acquisition of U.S. persons' data and mask their identities—but the government doesn't have to go to the FISC for an individualized court order.

Section 702 could be used for two kinds of collection. They're called "upstream" and "downstream." Upstream is when they collect inside the United States, as the communications traffic crosses a particular point on the internet backbone. There are approximately 106,000 targets under Section 702. Until April of this year, the NSA collected communications not just to or from those targets but also *about* the targets. And then there's downstream, which is when the intelligence community sends a target to an internet service provider (ISP) and obtains communications to or from the target that way.

Gellman: So to clarify, "upstream" means you are intercepting traffic on the move, across internet switches. And "downstream" means you're intercepting communications when they're sitting in storage at Google or Yahoo.

Donohue: Yes, with a slight tweak: downstream means that you obtain the communications from the ISP directly. Now, the legislation forbade the intentional targeting of anyone known to be located in the United States. So it was supposed to be outward-facing. It also outlawed what's called "reverse targeting." Say you wanted to intercept the communications of someone on U.S. territory. That's not allowed. But suppose the target's grandmother was overseas. You didn't actually suspect the grandmother of anything, but you suspected the target. You couldn't target the grandmother just to get the

communications of her grandson. That's not allowed under 702.

Gellman: Right. But here's where the problem comes in. Under the old system, for every target, every time NSA wanted to intercept communications from any individual, it had to go to the Foreign Intelligence Surveillance Court, in a classified proceeding, and say, "Here's our probable cause to believe that this target is a foreign power or an agent of a foreign power. Please look at our evidence and decide whether we meet your standard." That was then. What they have now is, the judge doesn't actually even know the identities of the targets. And the judge doesn't know the specific grounds for putting surveillance on that target. What the judge does is approve a set of rules and a set of promises from the U.S. government that it's going to comply with those rules. And after that, the government chooses the targets, engages in the surveillance, and does all that on its own.

Donohue: That is one of the key differences. The other element of FISA, traditionally, was that you also had to have probable cause that the individual to be targeted was going to use a particular "facility."

Gellman: Explain that for our readers. What's a "facility?"

Donohue: Previously a facility was an actual telephone number. The government had to specify one phone as its target. But after 9/11, they secretly changed the definition of facility to mean even a cable head or a gateway.

Gellman: Which means instead of intercepting communications to or from one telephone number, you're intercepting from a piece of infrastructure that could be used by thousands or tens of thousands of telephone numbers.

Donohue: That's exactly right. Not only that, but now the targets may be defined broadly. So it doesn't have to be a particular person. It could be a group or an organization. Say the European Union is a target: if the other end is domestic, then your conversation with anybody in that entity, group, organization, or whatever, can also be swept up. Under what's called "about" collection, they could intercept the communications of anybody talking *about* the European Union targets—or selectors [such as an email address] associated with the targets—as well.

When the communications of Americans are picked up under that very broad definition, this is what the intelligence community calls "incidental collection." That means traffic that is swept up in the process of surveilling a legitimate target—traffic that flows over the target facility or that is to, from, or about the target, and so on. The government uses this term, "incidental," to suggest that it only happens a couple of times. But, in reality, it's not a small number. It's a significant amount of communications that can be scanned, duplicated, retained, and then analyzed to look for potential evidence of criminal activity.

Gellman: I've read some very interesting "myths and facts" press releases published by the House Intelligence Committee. The chairman is very much for retention of this law. The example he gives to explain why an American might sometimes be caught up in this sort of surveillance is that a terrorist overseas is talking to an American in the United States about his plans. You really want to know what that conversation is about, and it sounds quite reasonable to target the terrorist even if an American is in the conversation. Is that what incidental collection is?

Donohue: In part, yes. But that's not everything. For example, there are these things called multi-communication transactions, or MCTs. Say you have a collectable communication between an overseas terrorist and somebody in the United States, and your target was the individual overseas. Well, the way the internet works is that other communications can become *bundled with that communication*. So your email about a PTA meeting might also travel with the terrorist's email, and that also can be collected "incidentally." Similarly, if you're scanning "to, from, or about" traffic, then you're likely to pick up a range of communications that are not at all to or from the target but happen to mention the target or selectors associated with the target. And that too is considered incidental collection.

The example that the intelligence committees have given is right in the pocket of what the legislation was designed to do. But as a de facto matter, the way it actually operates, it can be impossible to distinguish between relevant and irrelevant —target and non-target—data.

Gellman: Let's give a sense of scale. It's actually impossible to know because of classification rules, but I've seen plausible estimates suggesting that tens of millions of American citizens and green card holders are being swept up in surveillance that is supposed to be aimed at foreigners.

Donohue: The government has not provided any numbers on this. Senator [Ron] Wyden [Democrat, Oregon] and others have pressed repeatedly for numbers, to find out exactly how many Americans had their communications swept up in this program. The government has refused. The *Washington Post*, in 2014, did a report on this after analyzing a large sample of intercepted communications. They found that the NSA was collecting more information on ordinary internet users than on legally targeted foreigners.

Gellman: Yes. You probably know I wrote that story. It was based on a sample of a couple of hundred thousand communications. For various technical reasons, we couldn't precisely count how many Americans were caught up in that pile. But what we could say was that more than nine out of ten of the intercepted communications involved people who were not the targets. And that there were a very large number of communicants in there who were identified in brackets as "minimized," that is to say, "masked" U.S. persons. And by the way, the masking wasn't very good because we were able to identify quite a large number of Americans whose identities were not masked at all.

Donohue: The reason this matters, why it's such an issue, really goes back to Fourth Amendment rights and your right not to have the government interfere in your personal or private life without a warrant. Under traditional criminal law, you cannot use a warrant to go on a fishing expedition to try to find evidence of illegality. But that's exactly how Section 702 is being used. It's basically providing a general warrant to collect all of these communications, and then, at the back end, the FBI is querying these databases to look for evidence of illegal activity that has no relationship whatsoever to foreign intelligence.

This, as a constitutional matter, is deeply concerning.

Gellman: Let's spell that out here—what some have called the "back-door surveillance loophole." The NSA collects a very large number of communications. They're targeting foreign intelligence targets who are believed to be overseas. But they're also sweeping in a lot of other people including some very large number, surely in the millions, who are Americans. That all gets poured into a big bucket. Including Americans who were not targeted, who were not purposely intercepted. That is not intentional as the law describes it, but it is certainly foreseeable. The NSA knew that it would intercept lots of American communications, because that's just inherent in the technology and in the operational application of that technology. So they have this big bucket. And now, without getting a warrant, the FBI feels free, because the law is silent on this, to search for Americans in that pile?

Donohue: Yes. And not only to search for Americans: to search *using U.S. persons' information* and to search for information about U.S. persons showing potential evidence of criminal activity.

Gellman: You've used the term "general warrant," so I want to remind our readers that general warrants were one of the principal grievances of the American Revolution and a big reason for the rebellion against British rule. The Fourth Amendment was written into the Constitution very specifically to say, "We're not having those. We're going to have only very particularized warrants, based upon probable cause and a particular enumeration of the places to be searched."

Donohue: Right. That's the Fourth Amendment. Under ordinary criminal law, what it means is the government may not enter your home without having probable cause that a crime has been, is being, or is about to be committed. And to do that, they have to go to a judge, they have to present specific evidence, they have to make an oath, and that evidence has to demonstrate probable cause that there's criminal activity. What Section 702 does is it provides an end run around that. It basically allows the government to collect communications in large volumes—including incidentally collected American communications—and then search through them to look for potential evidence of criminal activity. That is a violation of the Fourth Amendment.

Gellman: As you know, one of the arguments that your adversaries will make is that the courts have already ruled on this

and said the Fourth Amendment is not implicated. I want to make a comment myself here. They are citing a case in theNinth Circuit Court of Appeals, *United States v. Mohamud*. This is one of those moments in which I think the government's statement is so grossly misleading that it comes close to an outright lie. Because the court in *Mohamud* very specifically said it was not ruling on the constitutional issues: it was ruling on the narrow facts of one case, not on constitutional grounds. And it was specifically not ruling on what you're describing now, the retention and querying of incidentally collected communications. How do they get away with saying a thing like that? How do they get away with citing *Mohamud* as support for their position that there's no Fourth Amendment issue there?

Donohue: I think it's deeply disturbing. *Mohamud*, the Ninth Circuit case, was about PRISM—that is, the [downstream] collection of stored communications from an internet provider that we talked about earlier [the surveillance practice's former name]. The judges in *Mohamud* explicitly say that they're not dealing with "to, from, or about" collection, *and* that they're not dealing with upstream collection. Same thing in *U.S. v. Hasbajrami*, which was in the Eastern District of New York, decided in March 2016. That case was also PRISM collection. In fact, the court actually says the "constitutionality of upstream collection is not at issue here." That's a quote.

So these cases explicitly do *not* stand for the proposition that 702 has been upheld as constitutional by the courts.

Gellman: Let me just mention a personal concern I have here. Which is on behalf of journalists and authors who write about the government. If you look through the NSA's repositories, there's a decent chance that I have been subject to incidental collection. I happen to have been caught up in this net. And by looking through my communications, the people who I talk to and what we talk about, it would be possible to investigate who my confidential sources are. And to give government power, without a warrant, to track down confidential sources of a reporter, when it could not have legally targeted either the reporter or the sources, is deeply disturbing. It is deeply hostile to any kind of independent investigation of government behavior.

Donohue: That's an important point. There are very serious constitutional questions about 702 that extend beyond the Fourth Amendment, including, for instance, First Amendment issues and the freedom of the press, which have not been tested by a court.

Gellman: How often are the agencies doing these backdoor searches?

Donohue: Well, the NSA and the CIA are releasing numbers about their queries of un-minimized data [in which U.S. identities have not been masked]. And they've said that in 2016, for instance, they used more than 5,000 different *search terms* that they knew were linked to Americans to troll through the cache of data collected under 702. Using those search terms, they have made 30,000 queries concerning a known U.S. person. That's an enormous number. Meanwhile,

the FBI doesn't even record the number of times it queries this database, much less the search terms. They don't even track it. And they routinely use it to see if they happen to have any communications information on Americans—without ever obtaining a warrant to get the information in the first place.

Gellman: Right. I remember when the president's Privacy and Civil Liberties Oversight Board did a report [in 2014] on Section 702. The report said the FBI searched for Americans in these data repositories so often that it did not keep count.

Donohue: Which is just a remarkable statement.

Gellman: I know from reading your work that you're certainly not going to deny that the surveillance using this authority under Section 702 is quite valuable, from a national security point of view. It's important. You don't want to end it all together.

Donohue: I consider it essential. I remember when Senator Feinstein was outraged that Angela Merkel was being placed under surveillance. And my response is, well, isn't that exactly who we want to have under surveillance? *Shouldn't* we we be listening to foreign leaders? I think when our negotiators from the State Department go in, they should know what's happening in a country and understand the landscape. Or when the Department of Defense needs to make a decision, they need to have critical information. That is what foreign intelligence is for. So I'm absolutely not opposed to it. In fact, I think for a broad range of issues, we should not just wiretap certain individuals on Mondays, but Tuesday through Sunday as well.

Gellman: I should mention something else, and I'm sure you've addressed this somewhere. This program is not just used to gather intelligence on terrorism. In fact, based on the several hundred thousand communications that I was able to review, it's not even used primarily for terrorism. There's a whole range of foreign intelligence purposes served by Section 702. And so the government's constant invocation of terrorism as the emotional core of a public debating position isn't really quite honest either.

Donohue: Yes, and there have been criticisms of the program based on the breadth of foreign intelligence as a concept [i.e., "foreign intelligence" is a capacious category which can result in the surveillance of aid workers, bureaucrats, scientists, etc.]. I'm less worried about that. I actually think if the primary purpose of the collection is foreign intelligence, then that is what such a program is for. I worry that we've lost that as the primary purpose. Particularly when the Foreign Intelligence Surveillance Court of Review ruled that the *primary* purpose of a Section 702 query could be criminal in nature, that raised very serious constitutional questions for me.

I do think this program can be fixed. And I think it can be fixed by ending "about" collection; by ending the querying of the database for criminal purposes; and by requiring that the primary purpose of collection or query be for foreign intelligence. And I think it can be fixed by requiring the government to go to a court if it wants to keep any U.S. person-related information that is incidentally collected. That would bring it into line with the rest of FISA. It should be required to get an individualized surveillance order against that U.S. person, and the surveillance should have to be for foreign intelligence purposes.

If the point of Section 702 is to improve foreign intelligence collection, and that's what allows the rules to be different than the rules for ordinary criminal search warrants, then foreign intelligence should be what the program is used for. As soon as we move into surveillance in the ordinary criminal realm, it's problematic. To the extent that criminal activity relates to the foreign intelligence purpose—so, say it was for terrorism, and there was a criminal prosecution that could follow based on the attempted murder of individuals—then certainly that should be allowed. But for unrelated criminal activity, the way they are using Section 702 is deeply problematic as a constitutional matter.

Gellman: Thank you very much for joining us.

Barton Gellman, Senior Fellow

Barton Gellman is a critically honored author, journalist, and blogger. His professional distinctions include two Pulitzer Prizes (individual and team), the George Polk Award, and Harvard's Goldsmith Prize for investigative reporting.

Laura K. Donohue, Contributor

Laura K. Donohue is a Professor of Law at Georgetown Law, Director of Georgetown's Center on National Security and the Law, and Director of the Center on Privacy and Technology. Her most recent book, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (Oxford University Press, 2016), was awarded the 2016 IIT Chicago-Kent College of Law/Roy C. Palmer Civil Liberties Prize. In November 2015, the U.S. Foreign Intelligence Surveillance Court appointed her as one of five amici curiae under the 2015 USA FREEDOM Act.
