The American Conservative

The New FISA Reform Still Doesn't Protect Your Privacy

Patrick G. Eddington

May 2, 2017

During the first 100 days of the Trump administration, the nearly 40-year old Foreign Intelligence Surveillance Act (FISA) saw its profile raised to a level not seen since Edward Snowden's explosive revelations almost four years ago. Late on April 28—in typical Washington "bury the bad news on Friday afternoon" fashion—FISA made still more surveillance-related headlines that directly affect every American.

The National Security Agency's (NSA) announcement regarding changes to intelligence collection under the nearly decade-old FISA Amendments Act was as succinct as it was misleading:

NSA will no longer collect certain internet communications that merely mention a foreign intelligence target. This information is referred to in the Intelligence Community as "about" communications in Section 702 "upstream" internet surveillance. Instead, NSA will limit such collection to internet communications that are sent directly to or from a foreign target.

You're probably asking, "What exactly is the FISA Amendments Act, specifically Section 702, and why should I care about any of this?"

The FISA Amendments Act was passed in 2008 after a more than two-year effort to make the Bush administration's previously illegal STELLAR WIND warrantless mass-surveillance program legal. Section 702 of the legislation allows the government to target the communications of foreign individuals and entities if a "significant purpose" (not more precisely defined) is the acquisition of "foreign intelligence."

As Stanford University's Jennifer Granick has noted, "Section 702 proponents emphasize the FISA statute's requirement that surveillance under the 702 provision only target non-US persons located abroad. They then push the seductive (but false) implication that this requirement means section 702 does not materially affect Americans."

In fact, a partially declassified FISA Court (FISC) opinion from November 2015 explicitly acknowledges that "there are substantial quantities of information concerning United States persons within the Section 702 data subject to querying by the FBI." And you don't have to be a

criminal to have your communications sucked up into NSA's Section 702 dragnet; all you have to do is call, text, fax, or email somebody overseas, or vice versa.

If you've communicated with anybody overseas, the odds are very high that your data has been collected under Section 702 (or possibly other surveillance programs carried out pursuant to the nearly 40-year old Executive Order 12333), and as the Michael Flynn episode has demonstrated, your identity—and the identity of those you were talking to overseas—could be publicly revealed.

How would your family and friends react if a news story broke that NSA collected your communications with overseas parties? Would your friends start to wonder if you were a terrorism suspect? How would it affect your job status?

Exactly how many Americans have had their communications swept up through Section 702 collection remains secret, despite repeated efforts by Senate Intelligence Committee member Ron Wyden (D-Ore.) over the last six years to get specific numbers from the Office of the Director of National Intelligence.

As the Privacy and Civil Liberties Oversight Board noted in its report on the Section 702 program, "Although U.S. persons and other persons in the United States may not be targeted under Section 702, operation of the program nevertheless results in the government acquiring some telephone and Internet communications involving U.S. persons, potentially in large numbers."

The only reason NSA has made this highly publicized recent change is that it got caught violating past FISC rulings holding that warrantlessly searching the captured communications of Americans that simply mentioned a foreign target was unconstitutional.

And if Edward Snowden's revelations of U.S. government mass surveillance have prompted you to start using encrypted message apps like Signal or WhatsApp, that 2015 FISC opinion I cited earlier also allows the government to keep and try to break your encrypted messages.

So even if you have broken no law, the secret court that oversees America's secret laws thinks it's just fine for NSA and FBI to collect and try to break into your conversations with your family, friends, co-workers, etc.

There's nothing remotely American about this, as *The Atlantic* reminded us recently in an article detailing the Founders' use of encrypted messages, both while in government and as private citizens.

And as Jennifer Granick notes in her excellent new book *American Spies*, executive-branch claims that Section 702 has been vital to preventing terrorist attacks on America are just as specious as previous such claims about the warrantless telephone metadata program that Snowden exposed in 2013.

Of the four Section 702 "success stories" touted by Intelligence Community officials, one involved the transfer of money to the Somali Salafist terrorist organization Al-Shabab for a plot that was not directed at America. Regarding the other three examples, Granick notes that "the terrorist either was or should have been under surveillance per narrower and more targeted surveillance that impacts fewer people."

In other words, the available public record shows that Section 702 collection has not made us safer while collecting huge quantities of sensitive information on potentially millions of innocent Americans—data that is sitting on government computer servers, just waiting to be hacked by foreign powers or hacker collectives.

Unfortunately, many privacy and civil-liberties advocates hailed NSA's court-ordered change as a victory, with Senator Wyden telling the *New York Times* that "This change ends a practice that allowed Americans' communications to be collected without a warrant merely for mentioning a foreign target. For years, I've repeatedly raised concerns that this amounted to an end run around the Fourth Amendment. This transparency should be commended." Accepting a change to a surveillance power that should never have existed is a win for NSA, not the Bill of Rights.

FISA has also figured prominently in the "Russiagate" episode, from the furor over the highly improper antics of House Permanent Select Committee on Intelligence (HPSCI) Chairman Devin Nunes (R-Calif.) to the *Washington Post*'s revelations that former Trump campaign aide Carter Page has been the target of a counterintelligence investigation since last summer. In early March 2017, Nunes stated that the "Russiagate" scandal made a renewal of Section 702 (set to expire on December 31) "problematic"—but we now know it was not that scandal, but NSA's own misconduct in illegally searching Americans' communications, that prompted this latest change.

We also now know that when Nunes and his House Intelligence Committee colleagues learned of these NSA violations of previous FISA court orders, they did nothing to punish NSA for those violations and failed to pass legislation to prevent it from ever happening again.

Congress passed the FISA Amendments Act without mandating that the intercepted communications of innocent Americans be destroyed immediately upon discovery or requiring annual evaluations of the effectiveness of the law. Instead, it's allowed federal intelligence and law-enforcement agencies to collect, store, and search your "incidentally" collected phone calls, emails, and text messages without a criminal predicate and a probable cause-based warrant as the Constitution's Fourth Amendment requires. And as Granick's research shows, the very collection the FISA Amendment Act authorizes hasn't made us safer. Those facts should be front and center when Congress debates reauthorization of this law later this year.

Patrick G. Eddington is a policy analyst in homeland security and civil liberties at the Cato Institute.