

Will The GOP Remake Surveillance Laws After Trump Leaks?

Eric Lieberman

March 27, 2017

Some Republican congressmen appear to be questioning the validity of a surveillance law that permits the government to surveil people's online communications, after a number of leaks from the Trump administration.

The Foreign Intelligence Surveillance Act (FISA), specifically Section 702 of the bill, allows federal intelligence agencies to collect data on foreigners. But due to the broad powers enumerated in the law and the inherent makeup of surveillance, the electronic communications of law abiding Americans are often picked up as well. The section is set to expire at the end of the year.

Republicans may not want to reauthorize the statute as some worry that such a loose interpretation, or a careless implementation, of the law could be a major contributing factor to the publicization of sensitive information pertaining to President Donald Trump and Russian officials.

Trump himself has levied numerous accusations against intelligence agencies, including the FBI and the CIA, for essentially trying to sabotage his presidency through leaks of classified information.

“The FBI is totally unable to stop the national security ‘leakers’ that have permeated our government for a long time. They can’t even.....find the leakers within the FBI itself. Classified information is being given to the media that could have a devastating effect on U.S. FIND NOW,” Trump wrote in multiple tweets. The social media posts follow reports from CNN that the FBI rejected a request from the White House to take down stories about exchanges between Trump's associates and Russia during the 2016 presidential campaign.

Republican Rep. Tom Rooney of Florida pressed FBI Director James Comey and National Security Agency (NSA) Director Mike Rogers on this issue during the U.S. House Permanent Select Committee on Intelligence (HPSCI) hearing earlier in March.

“But it’s really gonna hurt the people on this committee and you all on the intelligence community [IC], when we try to retain this tool [surveillance programs permitted through Sec. 702] this year and try to convince some of our colleagues that this is really important for national security, when somebody in the intelligence community says, ‘You know what, the hell with it, I’m going to release this person’s name because I’m going to get something out of it. We’re all

going to be hurt by that,” Rooney said to Rogers, who chairs the NSA and cybersecurity subcommittee.

Rooney was alluding to the “masking” aspect of intelligence agencies’ protocol, in which a U.S. person’s identity is supposed to be concealed, but sometimes ultimately gets out.

While Rogers agrees that an American outed after subsequent surveillance would be bad for national security, he stressed the fact that undue surveillance of Americans does not occur (or at least is not supposed to occur).

“I just wanna remind everyone and in general — FISA collection on targets in the United States has nothing to do with 702. I just wanna make sure we’re not confusing the two things, here, 702 is collection overseas against non-U.S. persons,” Rogers said.

Stewart Baker, the first assistant secretary for policy at the U.S. Department of Homeland Security under President George W. Bush, told The Daily Caller News Foundation that it’s hard to authorize section 702 without authorizing the collection of communications from Americans. He provides a telling example of a hypothetical email address like “Mahmoud@gmail.com” in which it doesn’t explicitly show if Mahmoud, who may be conversing with nefarious Yemeni nationals, is an American or not.

Baker asserts that if the NSA knew that Mahmoud was an American, it would “usually ‘mask’” his email address with some label like “USPerson No. 1 email address.”

“Section 702 is an effective program that can’t really work if we try to exclude American’s communications,” Baker continued, adding that the “‘unmasking’ provisions could be tightened up” and “they were effectively loosened as part of the sharing imperative arising from 9/11.”

Baker said America and its intelligence agencies “could do a better job of restricting the authority to unmask in contexts where abuse is a particular concern (e.g., where there’s a nexus to partisan political activity).”

Rogers said earlier in March that 20 people at the NSA, along with a few officials at the FBI, the CIA and the U.S. Department of Justice, have the ability to “unmask” Americans whose communications are entangled with the communications of a foreigner.

“Hypothetically, if the NSA obtained the communication of General [Mike] Flynn while he was communicating with the surveillance target legally, would you please explain how General Flynn’s identity could be unmasked?” Rooney asked Rogers, who subsequently refused to discuss “hypotheticals about individuals.”

But have Republicans, in general, always cared about the potential overreach of Section 720?

Patrick Eddington, a policy analyst in homeland security and civil liberties for the Cato Institute, told TheDCNF that “lots of Republicans and Democrats have been trying to rein in Sec. 702 for years,” citing the vote that occurred last year following U.S. citizen Omar Mateen’s murder of 49 people at an Orlando nightclub.

Republican Rep. Thomas Massie of Kentucky and Democrat Rep. Zoe Lofgren of California co-sponsored a two-page amendment that would have prohibited funds in the annual defense spending bill from being used to collect internet records under Section 702.

The amendment ultimately failed to pass, with 72 “ayes” and 168 “noes” from Republicans, totalling a final result of 198-222.

Ryan Hagemann, director of technology policy at the think tank the Niskanen Center, said Republicans clamoring over Section 702 is “politics, pure and simple.”

“The suggestion that former national security adviser Michael Flynn’s ties with Russian proxies may have been discovered using 702 surveillance mechanisms, and then released by a leaker within the IC, is primarily what is driving Republicans to suggest the program might not be reauthorized,” Hagemann told TheDCNF. “My guess is that certain members of HPSCI are holding the program’s upcoming reauthorization ‘hostage’ as a means of ferreting out details on the ongoing investigation into members of the Administration.”

Baker said Republicans think the Obama administration used national security investigative authority to cause harm to its political opponents in the Trump administration, “both by launching a national security investigation that was bound to focus on the Trump campaign and then by unmasking and leaking details from some of the surveillance that came from that investigation.”

He said while the concerns (whether truly new or not) may be political, there is some merit to the Republicans’ worries.

“While I support the launching of an investigation into Russian efforts to influence the election, and I can’t be sure the leak was from an Obama political appointee, I understand the GOP concern,” Baker told TheDCNF. “To my mind, that does suggest that we look for ways to deal with the risk of partisan misuse or misperception in the context of certain investigations — most notably the expected foreign efforts to influence the 2020 election.”

Despite some protest from Republicans and some loud complaints from Trump, the current administration is signaling that it does not want to reform FISA over privacy concerns.

“We support the clean reauthorization and the administration believes it’s necessary to protect the security of the nation,” an unknown White House official told Reuters in early March.

But perhaps the Trump administration’s tone will change after House Intelligence Committee Chairman Devin Nunes said Wednesday that Trump’s personal communications may have been incidentally captured as part of a surveillance sweep conducted by the Obama administration.

Nunes also said “that additional names of Trump transition team members were unmasked” but that “none of this surveillance was related to Russia or any investigation of Russian activities or of the Trump team.”