

U.S. House of Representatives
Permanent Select Committee on Intelligence

November 30, 2017

Re: Oppose the FISA Amendments Reauthorization Act of 2017

Dear Representative,

The undersigned 36 groups write to express their strong opposition to the “FISA Amendments Reauthorization Act of 2017,” which is scheduled to be marked up in the House Permanent Select Committee on Intelligence on December 1, 2017.

The proposed bill is *not* a reform measure. It does not make “key changes to Section 702 and other intelligence authorities to protect Americans’ privacy rights,” as bill sponsors have suggested.¹ On the contrary, it would expand surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA), grant the government more authority under other provisions of FISA, and could be read to codify current unlawful surveillance practices.

Indeed, the bill is measurably worse than a short-term straight reauthorization of Section 702 with a sunset. Given this— and the enormous privacy interests at stake— it is astounding that the bill is being rushed through committee and was released less than 48 hours before the scheduled markup. Among other things, we expect that the government will argue that the bill:

Expands existing surveillance authorities under FISA, which permit targeting of Americans and foreigners, both domestically and internationally. The bill expands the definition of “foreign power” and “agent of a foreign power” to include individuals or entities engaging in an array of cyber related activities. This could be used by the government to justify surveillance of Americans and foreigners for foreign intelligence purposes, even in cases where they are not acting on behalf of a foreign power, are not a member of a terrorist organization, and are not a member of a foreign political organization. Indeed, the broad language of the bill could be interpreted by the government to sweep in individuals only tangentially related to malicious cyber activities.²

Expands surveillance under Section 702 by including language suggesting that the government can target “a facility, place, premises, or property” for surveillance, which is far broader than current practice. The government may argue this gives it the right to spy on entire facilities containing millions of users, even if the vast majority of those users were U.S. persons that the government is prohibited from targeting under Section 702.

¹ Intel Committee Introduces Section 702 Reauthorization Bill (November 29, 2017), available at <https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=826>

² For example, the bill permits surveillance of someone who knowingly aids or abets malicious computer intrusions; courts have interpreted analogous language in other contexts to include individuals who may have consciously taken an act, such as deliberately sharing or selling information about a software vulnerability, without knowledge of how it would be used.

Codifies the government’s practice of warrantlessly searching Americans’ communications, which is illegal. The government routinely conducts warrantless searches of Section 702 databases looking for information about Americans, a practice referred to as “backdoor searches.” The House has voted on two occasions to reform this practice by requiring the government to obtain a warrant before conducting searches using U.S. person identifiers (with narrow exceptions).³ The FISA Amendments Reauthorization Act of 2017 would not require the government to obtain a probable cause warrant where it conducts U.S. person searches or seeks to access responsive content, even when related to a criminal case. Instead, it gives the government the *option* to apply for a court order, which the court must issue if it finds probable cause to believe the communications will provide evidence of either criminal activity, contraband or similar items, or property to be used in committing a crime. If the government does not obtain this order, however, it is still free to access any communications content, rendering the provision meaningless as a limit on warrantless searches or access. Additionally, the bill imposes no restrictions on access to non-content information, which could include metadata, URLs, search queries, location information, and a host of other sensitive information.

Permits Section 702 information to be queried, accessed and used in criminal cases without the probable cause warrant generally used in criminal cases. For example, the government could use the bill to access Americans’ information without a court order in criminal prosecutions involving specified domestic crimes and in cases where the Attorney General makes an unreviewable determination that a criminal proceeding is merely “related to” national security, a category so broad it could be interpreted to encompass a wide array of domestic crimes. Furthermore, it could be used to permit use of Section 702 information in all other criminal cases, provided the government obtains a court order finding probable cause to believe the communications will provide evidence of either criminal activity, contraband or similar items, or property designed to be used in committing a crime. Moreover, the bill contains no restrictions on using Americans’ information outside a criminal courtroom—raising concerns that information collected could be used in civil rights cases, immigration proceedings or to pressure people to become informants.

Codifies “about” collection rather than halting the practice. The government has wrongly interpreted Section 702 to allow it to collect information that is not to, or from, a target, but merely “about” such a target, including wholly domestic communications. In April of this year, the NSA halted “about collection” at the insistence of the FISA Court following numerous instances in which the agency failed to comply with court-imposed privacy protections. Instead of prohibiting this collection, the bill could be used by the government to restart it with the approval of the FISA court, an authority the government already claims. Once intentional “about” collection is re-approved by the Court, the bill would impose a one-month time period in which Congress could pass a law preventing it from re-starting—a time period so short that it would virtually ensure Congress’ approval through inaction.

³ Massie-Lofgren Amendment, H.Amdt.935, 113th Cong. (amending H.R.4870, Jun. 16, 2014), <https://www.congress.gov/amendment/113th-congress/house-amendment/935/text?q=%7B%22search%22%3A%5B%22hr+4870%22%5D%7D>, and Massie-Lofgren Amendment, H.Amdt.503, 114th Cong. (amending H.R.2685, Jun. 11, 2015), <https://www.congress.gov/amendment/114th-congress/house-amendment/503/text?q=%7B%22search%22%3A%5B%22hr+2685%22%5D%7D>.

We urge you to oppose the “FISA Amendments Reauthorization Act of 2017” and instead take up a bill to meaningfully reform our broad surveillance authorities. If you have questions, please contact Neema Singh Guliani, Legislative Counsel of the ACLU at 202-675-2322 or nguliani@aclu.org, Robyn Greene Policy Counsel and Government Affairs of New America's Open Technology Institute at 240-476-2172 or greeneg@opentechinstitute.org, or Elizabeth Goitein, Co- Director, Liberty & National Security Program, Brennan Center for Justice at 202-249-7192 or elizabeth.goitein@nyu.edu.

Sincerely,

Access Now

Advocacy for Principled Action in Government

American Civil Liberties Union

American Library Association

Arab American Institute

Brennan Center for Justice

Center for Democracy & Technology

Center for Media Justice

Color Of Change

The Constitution Project

Constitutional Alliance

Defending Rights & Dissent

Demand Progress Action

Electronic Frontier Foundation

Engine

First Amendment Coalition

Free Press Action Fund

Freedom of the Press Foundation

FreedomWorks

Friends Committee on National Legislation

Government Accountability Project

Government Information Watch

Human Rights Watch

Indivisible

NAACP

National Association of Criminal Defense Lawyers

National Council of Churches

National Immigration Project of the NLG

New America's Open Technology Institute

OpenTheGovernment

PEN America

Project On Government Oversight

Restore The Fourth

Sunlight Foundation

TechFreedom

Yemen Peace Project