CENTER FOR DEMOCRACY & TECHNOLOGY

Dear Senator:

We are writing to urge you to oppose an amendment to the Commerce, Justice and Science Appropriations Act for FY 2017 that would expand national security letter ("NSL") authority to permit the acquisition of sensitive electronic communications transactional records without prior court review.

Dubbed the "ECTR Fix" amendment, the McCain-Cornyn amendment doesn't "fix" anything. Instead, it strips the Foreign Intelligence Surveillance Court ("FISA Court") of the authority to determine whether information such as whom a person has been emailing and what websites they have been viewing should be obtained by the FBI because they are relevant to an investigation relating to terrorism or counterintelligence. It also makes permanent the controversial "lone wolf" provision of the Intelligence Reform and Prevention Act of 2004 ("IRTPA"), which has never been used since its inception over a decade ago.

"ECTR Fix" Amendment Would Be an Astounding Expansion of FBI Authority that Evades Judicial Review

The so-called "ECTR fix" would make several new categories of information available to the FBI under its NSL authority. In addition to phone records, the FBI would be able to obtain various details about your internet service: your account number, the identifier for your modem, types of service, how you pay, and when you log on or off, among other things.

Most concerning, however, is the fact that the FBI would be able to obtain "Internet Protocol . . . address or other network address" information and "communication addressing, routing, or transmission" information. This is dragnet language that essentially means that every time you interact with the internet, the record of that interaction can be obtained by the FBI. These records make up your entire digital fingerprint, and include: **your email history** (e.g., who emailed whom, and when), **your web browsing history** (e.g., what blogs you read), **logs of all your text messages, detailed location information**, and other sensitive data that paints an intimate picture of everything you do online.[1]

While the FBI has argued that this data is limited to top level domains, such as https://secure.trump2016.com or https://www.hillaryclinton.com, this limitation would still reveal very sensitive information and is not enshrined anywhere in statute. This information may show, for example, that you have made plans to visit a reproductive health clinic, that you made campaign donations to a particular candidate, or that you recently purchased a firearm or attended a gun show.

[1] Note that in spite of the fact that the amendment exempts cell tower information, location information can be derived from a wide variety of other sources including Wi-Fi addresses and other routing information.

Under the "ECTR fix," the FBI would be able to obtain all of this information – and all without judicial review.

FBI Already Has Broad Authority To Obtain Information In Intelligence Investigations

Once the FBI opens a preliminary investigation, like the one it commenced of Omar Mateen prior to the terrorist attack in Orlando, it can use virtually every lawful investigative technique available to it. It can use mail covers, undercover operations, polygraph examinations, subpoenas, and pen registers and trap and trace devices. When it has probable cause, it can also compel the disclosure of emails, text messages or other stored communications content.

The Attorney General Guidelines governing FBI investigations specifically authorize the FBI to, in a preliminary investigation, use compulsory process to compel the disclosure of transactional records under Section 215 of the Patriot Act and under 18 U.S.C. § 2703(d).[2] The standard that the FBI has to meet under Section 215 to compel the disclosure of transactional records is virtually the same as the standard it has to meet to issue a National Security Letter or NSL.[3] The FBI can use these authorities to secure the records that it seeks through the "ECTR fix"; it merely has to get a FISA court order. In fact, NSL authority was deliberately cabined to a narrow class of records precisely because it does not require review by a judge.

Congress Should Not Strip the FISA Court of Authority to Decide These Issues

Since the transactional records that would be made available to the FBI with an NSL under the McCain-Cornyn amendment are already available to the FBI when it has a Section 215 order, the effect of the amendment is clear: it strips the FISA court of the authority to decide whether the records sought are relevant to an investigation, and vests that authority solely in the FBI.

Unfortunately, lack of judicial oversight has led to the FBI's abuse of its NSL authority in the past: in a 2007 report, the Justice Department's inspector general revealed that the FBI frequently used NSL's to obtain the personal records of U.S. citizens, rather than foreigners related to terrorism or counterintelligence investigations. In addition, it often obtained vast quantities of records with a single NSL request. Without any judicial oversight, such abuse was able to continue for several years.

The "Lone Wolf" Provision is as Dangerous as it is Unnecessary

The McCain-Cornyn amendment would make permanent a controversial provision of the IRTPA that has never been used. The "lone wolf" provision gives the FBI the authority to wiretap non-U.S. citizens located in the United States even if they are not connected to any foreign nation or terrorist group. All that is required is a showing that the potential target is engaged in international terrorism or in preparation thereof—a showing typically sufficient to obtain a Title III surveillance order from a

[2] *See* Attorney General Guidelines at 31-32.

[3] For NSL's, the information sought must be "relevant to an investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709 (2012). Under Section 215, the information sought must be "relevant to an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861 (2012).

CENTER FOR DEMOCRACY & TECHNOLOGY

criminal court. Once again, this provision of the McCain-Cornyn amendment serves no other purpose but to cut out judicial review from the FBI's surveillance process.

The Amendment Would Not Have Prevented the Orlando Terrorist Attack

Nothing in the McCain-Cornyn amendment would have helped the FBI prevent the Orlando terrorist attack. This is because the FBI already has broad authority to open investigations, the scope of which it determines in its sole discretion. Once it opens an investigation, it can keep it open indefinitely, and under its own authority. In the case of Omar Mateen, the FBI opened a preliminary investigation, held the investigation open for 10 months, and closed the investigation when it determined that there was no reasonable suspicion of crime—the standard that must be met to open a full investigation.

The McCain-Cornyn amendment would roll back key procedural protections and would have done nothing to prevent the worst mass shooting in American history. We strongly urge you to vote "no."

Sincerely,

The Center for Democracy & Technology

For more information, please contact Gabe Rottman, grottman@cdt.org, or Jadzia Butler, jbutler@cdt.org.