Senators Should Vote "NO" on McCain-Cornyn Amendment 4787 That Would Expand Surveillance, Reduce Oversight, and Threaten Privacy

Tomorrow morning, the Senate is scheduled to vote on the McCain-Cornyn amendment 4787 to the Commerce, Justice, and Science Appropriations bill. New America's Open Technology Institute strongly opposes this amendment and urges Senators to vote no on this dangerous proposal. The McCain-Cornyn Amendment would undermine the reforms to surveillance laws that we achieved just last year by significantly expanding FBI surveillance of Americans communications and Internet activities without any judicial approval or oversight. The amendment would expand the NSL statute to include electronic communications transactional records (ECTRS). This would significantly threaten privacy by enabling the FBI to access and use this revealing information to develop profiles of Americans' habits and preferences, such as those concerning individuals' medical and mental health concerns, political leanings and religious beliefs, reading interests, hobbies, and much more.

ECTRs as Defined in the McCain-Cornyn Amendment Reveal Personal Information Like:

- *Account number*
- *Login history:* Reveals when and from where an Internet user signed into an online account.
- *Types of service (and means of payment):* This could reveal:
  - An Internet user's credit card and bank account information;
  - The types of services a person uses, such as social media accounts like on Facebook or online dating websites; email service providers, including those that provide added privacy and security features like end-to-end encryption; and entertainment and news services like Spotify, Netflix, and newspaper subscriptions.
- *IP Address or other network address, including temporarily assigned addresses:* This could reveal:
  - Location information that can be traced back to an IP address, revealing where the Internet user is geographically, and information concerning all IP addresses on a network, subject to the requirements of the USA FREEDOM Act.
  - An Internet user's identity when combined with other easily accessible information, and occasionally on their own.
- *Communication addressing, routing, or transmission information, including network address translation information:* This could reveal:
  - An Internet user's browsing history, including the specific pages they visit, and the name of the web host (ex. what articles someone reads on the Politico or New York Times websites, what medical conditions they research on WebMD, which items they shop for on Amazon.com
    - DOJ's current position is that it can only access top-level domain names from a person's browsing history. For example, this would include revealing information like that someone visited http://alcoholicsanonymous.com, but not that they visited a subpage on "if AA is right for me". Top-level domain names can be easily associated with religious institutions, medical providers, political organizations, hobbies, news sites, or other interests. Thus, DOJ's self-imposed restriction would leave Americans little privacy protection from the abuse or misuse of the NSL authority. What's more, DOJ's policy could change and enable the FBI to access subpages as well as top-level domains. There is nothing in the statute or in the proposed amendment that would prevent such an overreach.
  - The size of a web page, which can indicate whether it contains videos or photos;
  - The link an Internet user clicks in order to be redirected to another web page;
  - E-mail metadata: sender; receiver(s); time of email; subject line (DOJ currently considers this content but the amendment includes no limitation); size of e-mail; possibly the presence, size and type of attachments;
  - Location information concerning the recipient of a communication;

For more information, please contact Robyn Greene, Policy Counsel at New America's Open Technology Institute, at greene@opentechinstitute.org.

- The network an Internet user is connecting from (ex. home, work, public, or at a business, as well as the location of that network)
- *Session times and durations:* This could reveal information like what time and how long an Internet user spends on an online dating website, or on a website providing medical advice or substance abuse support.

What National Security Letters (NSLs) are: NSLs are administrative subpoenas that can be issued by FBI agents in field offices, without any oversight or approval by courts. Currently, if the FBI issues an NSL under Title 18, it can only demand information concerning the name, address, length of service, and local and long distance toll billing records of a person or entity.

FBI Has a Long History of Abusing NSL Authorities: Inspectors General have found that NSL authorities have been abused more than almost any other surveillance authority available to the FBI - including using NSLs for bulk collection. Additionally, in 2008, the White House Office of Legal Counsel (OLC) told the FBI that it was not authorized to demand ECTRs under NSL authorities. Since then, the FBI and DOJ have repeatedly urged Congress to expand the statute to include that authority, and Congress repeatedly considered and rejected their proposals. Despite this, NSLs recently released by Yahoo!, including one issued as recently as 2013, show that the FBI continued to improperly use NSLs to demand ECTRs.

NSLs are compulsory and are almost uniformly subject to gag orders: When a company, organization, or other person or entity receives an NSL, they are required to provide any responsive information that they have, and are subject to a gag-order that prohibits them from telling anyone - including the subject of the NSL - about its existence, unless that person is providing legal counsel concerning the NSL or is necessary to procuring information that is responsive to the demand.

The FBI Issues NSLs for Information on Tens of Thousands of Accounts Every Year: The DNI reports that in the last two years, the FBI issued 29,218 NSLs demanding information concerning 81,666 individuals or accounts, and over the last ten years, it has issued over 300,000 NSLs.

FBI Can Currently Obtain ECTRs Pursuant to Other Authorities: There are a plethora of authorities under which the FBI can get a court approval to obtain ECTRs, such as under Patriot Act Section 215. The FBI must meet the same standard to get a 215 order from a FISC judge for ECTRs that it would self-certify under the NSL statute: it must show that the information sought is relevant to a terrorism or counterintelligence investigation. The McCain-Cornyn amendment would not give FBI access to new information; the amendment would only enable FBI to avoid any meaningful oversight of the use of those authorities - oversight that is necessary to protect against a pattern of repeated abuses of NSLs.

McCain-Cornyn Amendment Would Make "Lone Wolf" Provision Permanent: The "Lone Wolf" statute is set to sunset in 2019, and in the 12 years since it was passed, the FBI has never used it; not once. Nonetheless, this amendment would make this controversial and apparently unnecessary provision permanent. The statute allows the FBI to go to the FISA Court get a warrant for electronic surveillance of non-US persons who are suspected of planning or committing an act of terrorism, instead of going to a regular Title III court for a wiretap warrant, which would impose stricter guidelines for when the warrant would issue and how it must be used.

OTI strongly opposes the McCain-Cornyn Amendment 4787 as a threat to privacy, and little more than an effort to reduce needed judicial oversight and expand dangerous surveillance authorities. We urge Senators to VOTE NO on the McCain-Cornyn Amendment 4787.

For more information, please contact Robyn Greene, Policy Counsel at New America's Open Technology Institute, at greene@opentechinstitute.org.