

Cornyn ECTR Amendment Would Expand Surveillance, Reduce Oversight, and Threaten Privacy

New America's Open Technology Institute strongly opposes any proposal to expand National Security Letter authorities to include the issuance of demands for electronic communications transactional records (ECTRs), such as Senator Cornyn's proposed amendment to the Email Privacy Act and the Commerce, Justice, and Science Appropriations bill. Any such proposal would significantly threaten privacy by expanding FBI surveillance of Americans' communications, allowing them to access and use that 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. Cornyn's amendment would also substantially weaken oversight of the FBI's access and use of ECTRs since FBI agents issue NSLs independently, without any judicial oversight, despite a troubling history of abuse.

ECTRs listed in the 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 or what they watch on Netflix);
 - 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;
 - The network an Internet user is connecting from (ex. home, work, public, or at a business)
- **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.

Allowing the FBI to Obtain ECTRs via National Security Letters (NSLs) Would Threaten Privacy, Undermine Essential Judicial Oversight, and Open the Door to Abuse:

- **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.
- **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.
- **FBI has historically abused NSL authorities:** A 2007 Inspector General audit concluded that the FBI [abused NSLs](#) more than almost any other surveillance authority, including using NSLs for [bulk collection](#), which is why the [USA FREEDOM Act](#) explicitly prohibits this going forward - though some large-scale collection is still possible. 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.
- **Over ten thousand NSLs are issued every year covering tens of thousands of accounts:** While the USA FREEDOM Act reforms should ensure that NSLs can no longer be used to engage in bulk collection to the scale Inspectors General found in the past, they can still be used to collect information on large numbers of people. For example, a single NSL could cover all of the toll billing records of New America, a think tank with over 150 employees and fellows who are in communication with countless others. 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 ECPA 2703(d) orders and Patriot Act Section 215 Orders. The FBI's complaint is not that it cannot access the information that it needs - because it can - it is that in order to obtain ECTRs, it must be overseen and approved by a judge. Given the history of NSL abuses and the highly sensitive nature of ECTRs, removing judicial oversight is a recipe for disaster.