FBI Should Not Be Able to Use NSLs to Demand Electronic Communications Transactional Records (ECTRs)

The FBI has renewed a push for Congress to authorize a significant expansion in the FBI's surveillance powers that would enable the FBI to demand highly sensitive electronic communications transactional records (ECTRs) using administrative subpoenas called national security letters (NSLs). What follows is an explanation of what ECTRs are and what personal information they can reveal, as well as an overview of NSLs.

What Electronic Communications Transactional Records (ECTRs - pronounced *eck-ters*) are: ECTRs are metadata that are created when individuals engage in any kind of activity online. That metadata includes information like Internet users' account numbers, login history, session times and durations, the types of services and subscriptions they use, web browsing history, IP address or other network address information, and communication addressing, routing, or transmission information.

ECTRs can reveal extremely sensitive information about a person in enough detail that law enforcement could create profiles of Americans' habits and preferences. ECTRs can expose personal information like individuals' medical and mental health concerns, political leanings and religious beliefs, reading interests, hobbies, and much more. Specifically, ECTRs can reveal information about average American Internet users like:

- Identity and location;
- 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 such as Spotify, Netflix, and newspaper subscriptions.
- A person's browsing history, including the specific pages they visit, and the name of the web host (ex. what articles someone reads on Politico or NY Times websites, what medical conditions they research on WebMD, which items they shop for on Amazon.com, what films or TV shows they view on Netflix), or what e-books they borrow from the library;
- What time and how long a person spends on particular websites, like online dating websites, or on websites providing religious counseling, medical advice, or substance abuse support;
- The size of a web page, which can indicate whether it contains videos or photos;
- The links a person clicks in order to be redirected to other web pages; and
- Information concerning the sender and recipient(s) of e-mails; time of email; subject line (DOJ currently considers this "content" but there is no such limitation in statute leaving it open to interpretation, so that policy is subject to change); size of email; and possibly the presence, size, and type of attachments.

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

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.

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