Senators Should Reject the Deeply Flawed Intelligence Authorization Act of 2017

The annual Intelligence Authorization Act should be a non-controversial bill that provides the Intelligence Community with the authorizations to do its work at specified funding levels. However, this year, the Senate Intelligence Committee is using the authorization process as a vehicle for debating controversial policy proposals in secret and attempting to turn them into law. The Intelligence Authorization Act for Fiscal Year 2017 (S. 3017) would grant the FBI a significant expansion of its surveillance authority under a National Security Letters statute. It would also limit the Privacy and Civil Liberties Oversight Board's (PCLOB) jurisdiction in a way that could prove harmful not only to individual privacy, but also to our economy.

National Security Letter (NSL) Expansion - Electronic Communications Transactional Records (ECTRs): The Intelligence Authorization Act includes a provision that would expand the National Security Letter (NSL) statute under title 18 to allow the FBI to obtain electronic communications transactional records (ECTRs). Right now, the FBI is supposed to obtain these highly sensitive records only pursuant to a court order, based on a showing of specific and articulable facts that the records sought are relevant to an investigation. NSLs, on the other hand, are subject to no judicial oversight. FBI field agents are able to issue NSLs on their own accord, and they routinely come with gag orders of questionable constitutionality. The expansion to the NSL statute included in the authorization bill would thus do-away with the requirement for judicial approval - a necessary protection given the highly revealing nature of ECTRs.

What ECTRs Are: ECTRs are metadata about Internet users' online communications. They can expose extremely sensitive information about a person in enough detail that law enforcement could create profiles of Americans' habits and preferences. ECTRs can divulge 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 shops for on Amazon.com or what films or TV shows they view on Netflix);
- What time and how long a person spends on particular websites, like online dating websites, or on a website 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, 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.

FBI Track Record with NSLs Shows Repeated Abuses: 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. This history of abuse makes clear that maintaining judicial oversight of these authorities is essential to protecting Americans' privacy and civil liberties.

Limitation on PCLOB Jurisdiction Poses a Threat to Privacy and the Economy: The authorization bill would also limit the PCLOB's jurisdiction by removing its authority to consider the privacy impact that NSA surveillance has on non-US persons. This would be in direct contravention of the White House's priorities when it authorized PPD-28, which established limitations on the Intelligence Community and privacy protections concerning surveillance of non-US persons. Additionally, this provision may throw the new Privacy Shield into jeopardy.

When the European Union Court of Justice struck down the Safe Harbor agreement because of concerns over NSA surveillance, US and EU officials scrambled to draft a new agreement - the Privacy Shield - that would address the Court's concerns and enable US tech companies to transfer customer data internationally. The US tech industry could lose billions of dollars if the Privacy Shield is struck down - a real possibility given that its sufficiency is already being litigated, and in June, and the German Data Privacy Authority fined three American companies for transferring data from Europe to the US in violation of privacy laws. The limitation on the PCLOB's jurisdiction that has been included in the Intelligence Authorization Act will put the Privacy Shield on even shakier ground. This provision would undermine the assertions that US negotiators made to the Europeans that the PLCOB, in its oversight function, could serve as a check against the abuse of European citizens' privacy.

Intelligence Authorization Act Is Not a "Must-Pass" Bill: The Intelligence Authorization Act is not a "must-pass" bill. In fact, during the entirety of President Bush's second term in office, no intelligence authorization bill became law. Yet, intelligence agencies were able to continue their operations uninterrupted because they are permitted to use funds Congress provides in its appropriations bills in the absence of an authorization bill.

While in recent years Congress has passed an annual authorization bill, the language of these bills was mostly non-controversial, and none of the bills that were signed into law included significant domestic surveillance provisions. This year, behind closed doors, the Senate Intelligence Committee debated and approved a deeply controversial bill that includes provisions that expand surveillance authorities and undermine oversight. The ECTR expansion, in particular, has been opposed by privacy and civil liberties organizations, and technology companies, and has been considered and rejected several times by Congress. Given the serious defects in this year's Intelligence Authorization Act, the Senate Intelligence Committee should either go back to the drawing board and draft a clean authorization bill, or Senators should oppose it.

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