CENTER FOR DEMOCRACY & TECHNOLOGY

February 2024

Requiring a Warrant for U.S. Person Queries is Critical for FISA 702 Legislation

This week the House will vote on legislation to reauthorize Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"), largely modeled off of a bill developed by the House Intelligence Committee. FISA 702 is controversial because it is a warrantless surveillance authority, and even though targets must be non-U.S. persons abroad, a huge number of Americans' communications are swept up. The FBI, CIA, and NSA then conduct U.S. person queries to deliberately pull up and read through Americans' private messages, all without a warrant. This process has been subject to systemic and ongoing abuse, and according to a recent poll over 75 percent of Americans want this loophole closed.

Members should vote for a planned amendment to require a warrant for U.S. person queries, and oppose the bill if it fails to include this critical measure.

Key Fact #1: U.S. Person Queries Are Abused on a Mass Scale and in a Manner Antithetical to Democratic Society

- Warrantless U.S. person queries occur on a mass scale. In 2022 (year of most recently published date), *the FBI conducted over 200,000 U.S. person queries, including an estimated 4,000 queries in violation of their own rules.*
- Improper queries in recent years have included: Peaceful protesters, a batch of over 19,000 donors to a Congress campaign, journalists, political commentators, Members of Congress, a state judge that contacted the FBI to report civil rights violations, and individuals an analyst matched with in an online dating app.

Key Fact #2: The Base Bill is Grossly Insufficient to Stop This Abuse, and is Designed Simply to Preserve the Status Quo

- The key "reform" to U.S. person queries in the bill is to codify internal FBI rules, but evidence has proven relying on this type of self-policing won't stop abuse:
  - In 2022—even after these measures were put into effect—the FBI conducted an estimated 4,000 improper U.S. person queries, *an average of over 10 improper queries every single day.*
  - These measures have merely reduced noncompliance from an astronomical level (in 2020-2021 there were an estimated 278,000 improper queries) to an intolerably high level. Labeling this status quo as sufficient is the equivalent of drinking a spoonful of poison instead of a ladle and calling it healthy.
- The bill prohibits a set of U.S. person queries, but only does so for queries conducted solely to return evidence of a crime, which *virtually never occur*: In 2022, only 2 U.S. queries that fall within this prohibition returned communications content, less than one thousandth of one percent of the 200,000+ queries the FBI conducted.

KEY FACT 3: The Warrant Rule Has Been Carefully Designed to Meet Operation and Security Needs.

- Warrants are a standard law enforcement practice for investigations, and can be rapidly obtained when probable cause is established.
- The amendment (based on text from the Protect Liberty Act, which passed out of the House Judiciary Committee 35-2) is carefully crafted to include exceptions to meet security needs. It includes an exception based on consent, facilitating queries to aid targets and victims of foreign plots. These *victim queries would not require a warrant as soon as consent is obtained*, and according to Privacy and Civil Liberties Oversight Board (PCLOB) Chair Sharon Bradford Franklin, *"Outside of the category of 'victim' or 'defensive' queries, [the] FBI has been unable to identify any cases in which a Section 702 U.S. person query provided unique value in advancing a criminal investigation."*
- The warrant rule also includes an exception for queries of malware, which (as well as the consent exception) will ensure queries related to cybersecurity will generally be exempt. Finally, the rule includes an exception for exigent circumstances, alleviating any risk of a warrant application taking too much time during an emergency.
- The amendment only requires a warrant for queries that return the content of communications, and does not apply to metadata queries. Metadata queries can yield valuable information such as web traffic that provides key information related to cyberattacks and contact networks of suspects.
- Ability to conduct metadata queries addresses the concern from intelligence agencies that they will be bogged down by the need to court tens of thousands of times. Agencies would be able conduct metadata queries as standard preliminary step to confirm when a content query will yield a "hit" before seeking a warrant. In 2022, only 1.58 percent of FBI queries returned content, less than 3,300 total.

For more info, contact Jake Laperruque, Deputy Director, Security and Surveillance Project, at jlaperruque@cdt.org.