PPSA
PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY

CENTER FOR DEMOCRACY & TECHNOLOGY

Debunking Myths on the National Security Impact of Warrants for U.S. Person Queries

Warrantless queries of Americans' communications obtained via Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702") are antagonistic to the basic principle of the Fourth Amendment. Deliberately seeking to read Americans' private communications – but without ever showing evidence of wrongdoing or obtaining independent approval from a judge – violates the Constitution, disrespects American values, and opens the door to abuse.

Opponents of FISA reform nonetheless oppose requiring a warrant for U.S. person queries by claiming these queries provide huge value that would be disrupted by a warrant requirement. ***These claims are false – in reality a warrant rule has been carefully designed to account for the limited value that such queries provide.***

MYTH #1: *U.S. person queries are immensely important in a broad array of situations, making it dangerous to place restrictions on this important tool.*

> **REALITY: Queries only provide value in a limited set of situations, and the warrant rule proposed in 2024 during the 118th Congress provides exceptions to account for all of them.**

Opponents of reform frame U.S. person queries as frequently valuable across a wide set of national security goals and investigations, but the 2023-2024 debate over FISA 702 proved this was false: The Intelligence Community testimony, the President's Intelligence Advisory Board, and the Privacy and Civil Liberties Oversight Board (PCLOB) uncovered only a few distinct scenarios in which U.S. person queries provided value.[1] And the proposed warrant rule includes exceptions that account for all of them.

Under the 2024 proposal, a warrant would not be required 1) when there is consent, 2) to track malware, or 3) for metadata queries:

- *Cyber Attacks*: Queries were most useful in the cybersecurity context, helping the government detect warning signs of future attacks and trace attacks back to their sources. But queries focused on cyberthreat signatures are explicitly exempt. Much of the cybersecurity value of queries focused on network traffic patterns; this involves metadata rather than content, and metadata queries are also exempt from the warrant rule. Most importantly, any U.S. company or critical infrastructure entity targeted for a cyberattack can simply consent to a query.

[1] For additional details, see The Government's Objections to FISA 702 Reform Are Paper Thin | Lawfare; see also Unpacking the President's Intelligence Advisory Board FISA 702 Report | Lawfare.

- *Foreign Plots*: Queries were also described as useful in detecting and responding to foreign assassination and kidnapping plots. But once again, the consent exception directly accounts for this need. A targeted American will obviously gratefully accept such a query to enable government protection.[2]
- *Foreign Recruitment*: Defenders of the status quo cited limited cases in which queries helped the government discover suspicious foreign contacts, assisting the government in investigating whether the U.S. person was a foreign target or foreign agent. But because metadata queries are exempt, a warrant rule would not inhibit the government's ability to identify these contacts. The government *has never shown one instance* in which content queries were critical to advancing an investigation against a foreign agent.[3] Besides, reading the private emails of an American being criminally investigated is exactly what warrants are required for.

MYTH #2: *U.S. person queries need to be done quickly and efficiently, and a warrant rule would slow the process down in a manner that endangers Americans' lives.*

> **REALITY: The government has never shown queries provide time-sensitive responses, and the warrant rule's exceptions account for such a scenario if it ever did emerge.**

A common argument against surveillance reform is the "ticking time bomb" hypothetical in which there simply isn't time to abide by due process and obtain court approval. But the government has never shown a situation in which query results were needed so quickly that obtaining a warrant would be infeasible.[4]

- If a time-sensitive emergency ever did occur, the warrant rule explicitly accounts for it by including an exception for exigent circumstances. Contrary to this complaint's framing, the government has indicated that query results are used primarily during the *early* stages of investigations, or with queries run on targeted victims--in which cases the consent exception makes a warrant unnecessary.

---

[2] In addition to the consent exception addressing this issue, the warrant rule can be satisfied by a probable cause showing that the query *would produce evidence of a crime*; so long as that standard is satisfied it is not necessary to prove that the query subject is a suspected criminal or foreign agent. Therefore, so long as the government can demonstrate probable cause that a query focused on the target of a foreign plot will uncover details of that plot, such a query would receive necessary judicial sign off. The government has regularly obtained warrants for digital searches focused on victims, and there is no reason to expect they could not do so in the context of queries as well. For more information, see Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries | CDT.

[3] Notably the two independent reviews of FISA 702 only cite *one instance* when a queried individual was later discovered to be a nefarious actor, and this discovery was the product of an "independent investigation" for which the government successfully obtained a warrant. See PIAB FISA 702 Report, p. 36; see also, PCLOB FISA 702 Report.

[4] Intelligence officials sometimes reference the significant length of FISA Title I warrant applications and time spent developing them as the basis to claim that US person query warrants would be equally slow and onerous. But this is not an apt comparison because the warrant proposal allows the government to conduct queries by obtaining either a standard Title III criminal wiretap order *or* a FISA Title I warrant.

In short, the exigent circumstances, consent and metadata exceptions to the proposed warrant requirement almost certainly address and legitimate concerns about the government's ability to respond to threats quickly.

MYTH #3: ***Warrants are not feasible given the scale of U.S. person queries conducted; adding this rule would overwhelm intelligence agencies and the courts.***

> **REALITY: By permitting warrantless metadata queries, the warrant rule ensures the government will not need to go to court frequently.**

In 2023, the most recent year for which data is available, the FBI conducted queries for over 57,000 unique U.S. person terms, reflecting unacceptable government overreach and fishing efforts. However, most of these queries do not produce responsive results. Because the proposed warrant requirement would apply only when the government sought to access a communication's content, it would weed out impropriety without straining intelligence agencies or the courts.

- Only 1.58 percent of the FBI's U.S. person queries resulted in personnel accessing content, according to the FBI.[5] Thus, even if queries continued to be conducted at the prior rate of 57,000 annually – an unlikely prospect, given that many of these queries were improper or broad fishing efforts – a warrant would be potentially applicable to less than 1,000 queries a year, less than 3 per day on average. And because the proposed warrant rule would permit warrantless metadata queries (and only require court approval to *access content*), agencies would be able to confirm when a query will yield a "hit" before devoting any time and effort to seeking a warrant.

And even as to these 2-3 queries per day, most would fall under one of the exceptions to the warrant requirement described above. The FBI usually wouldn't need 2-3 warrants each day; more likely it would need to obtain consent of 2-3 entities to help prevent a future cyberattack or foreign plot. And if adding a warrant requirement on this limited level would be too onerous for intelligence agencies or the courts, the solution would be to add personnel to cover that need, not to reject an important constitutional safeguard against abuse.

Americans' basic rights should not be secondary to bureaucratic hurdles and staffing limits. The exceptions and exemptions built into the 2024 warrant proposal would allow the government to remain within the boundaries of the Constitution while also having the means to protect national security.

For additional information, please contact Gene Schaerr (gschaerr@schaerr-jaffe.com), General Counsel at the Project on Privacy and Surveillance Accountability, and Jake Laperruque (jlaperruque@cdt.org), Deputy Director of the Security and Surveillance Project at the Center for Democracy & Technology.

[5] See PCLOB FISA 702 Report, fn. 35.