Statement for the Record

Jake Laperruque, Deputy Director of the Security and Surveillance Project
The Center for Democracy & Technology

House Judiciary Committee
Subcommittee on Crime and Government Surveillance

"A Continued Pattern of Government Surveillance of U.S. Citizens"

April 8, 2025
(Submitted April 15, 2025)

The Center for Democracy & Technology ("CDT") is pleased to submit the following written statement to the House Judiciary Subcommittee on Crime and Federal Government Surveillance for its hearing "A Continued Pattern of Government Surveillance of U.S. Citizens." CDT is a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age. For nearly three decades, CDT has worked to ensure that rapid technological advances promote our core values as a democratic society.

A wide range of surveillance technologies and techniques are in need of more rigorous rules and safeguards. In this statement, we focus on two policy areas where loopholes have emerged that facilitate problematic warrantless surveillance, undermining Americans' privacy and risking abuse. First is the "Backdoor Search Loophole," involving warrantless U.S. person querying practices under section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"). Second is the "Data Broker Loophole," involving governmental purchases of sensitive data compelled disclosure of which would require a warrant or other court order. We also highlight the key role the Privacy and Civil Liberties Board ("PCLOB") has played in protecting privacy and promoting reform of these and other critical surveillance authorities, and the importance of ensuring that the Board can function as a strong and independent entity.

I. FISA 702 and the Backdoor Search Loophole

FISA 702 is a warrantless surveillance authority that can only be used to *target* foreigners located abroad, but inevitably involves significant surveillance of Americans who have communicated with those targeted. Disturbingly, despite past promises made to the House Judiciary Committee and others, the

intelligence community has refused to provide a public estimate of how many Americans' communications are collected warrantlessly in FISA 702 surveillance.[1]

After FISA 702 surveillance vacuums in the private communications of Americans, the FBI, CIA, and NSA query the databases of communications collected via FISA 702 to pull up Americans' emails, texts, and other private messages. Because this workaround allows agencies to deliberately seek out and read Americans' private communications without ever obtaining a warrant, it is often referred to as the Backdoor Search Loophole. This loophole is exploited on a massive scale: In 2023 (the most recent year for which data is available) the FBI conducted queries for over 57,000 unique U.S. person identifiers.[2] Such a system is an affront to Americans' privacy, and legally dubious; just this year a federal court ruled that warrantless queries violated the Fourth Amendment.[3]

Warrantless access to Americans' private communications not only disrespects American values, it opens the door to abuse. In the absence of independent court approval, U.S. person queries have been systemically misused. In recent years improper U.S. person queries have been conducted on peaceful protesters, a batch of over 19,000 donors to a Congressional campaign, journalists, Members of Congress, Congressional staff, political commentators, a state senator, a state judge that contacted the FBI to report civil rights violations, and individuals an intelligence analyst had matched with in an online dating app.[4]

Updated internal rules for U.S. person queries—adopted as agency guidelines in 2021 and early 2022[5] and largely codified for FISA 702's most recent reauthorization—have proven woefully inadequate. Some of the most egregious U.S. person queries that have been publicly reported occurred since implementation of

[1] In 2016, a bipartisan group of 11 members of the House Judiciary Committee sent a letter to Director of National Intelligence James Clapper memorializing a promise to the Members to provide an estimate within months of the number of Americans whose communications are collected via FISA 702. During his Senate confirmation hearing Director of National Intelligence Dan Coats reaffirmed this commitment, stating "I will do everything I can to work with Admiral Rogers in NSA to get you that number." In 2017 NSA Deputy Director Richard Ledgett stated an estimate would be provided before the end of the year. See, Letter to Director of National Intelligence James Clapper, Dec. 16, 2016, https://democrats-judiciary.house.gov/sites/democrats.judiciary.house.gov/files/documents/letter%20to%20director%20clapper%20(12.16.16).pdf; see also, Letter to Director of National Intelligence Dan Coats, April 7, 2017, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2017-04/040717_Letter-to-DNI-Coats.pdf; see also, Dustin Volz, *Reuters*, "U.S. lawmakers ask for disclosure of number of Americans under surveillance," April 7, 2017 https://www.reuters.com/article/world/us-lawmakers-ask-for-disclosure-of-number-of-americans-under-surveillance-idUSKBN1792I3/.

[2] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Authorities, Calendar Year 2023," April 2024, https://perma.cc/RWW7-UHK7. Hereinafter, "ODNI 2023 Transparency Report."

[3] *United States v. Hasbajrami*, No. 11-cr-00623-LDH (E.D.N.Y. Jan. 21, 2025).

[4] See, Privacy and Civil Liberties Oversight Board, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," September 28, 2023, https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf, hereinafter, PCLOB FISA 702 Report; see also "Section 702 of FISA: A 'Foreign Intelligence' Law Turned Domestic Spying Tool," https://perma.cc/MU88-45JX.

[5] See, Department of Justice, National Security Division, "Recent Efforts to Strengthen FISA Compliance," February 28, 2023, https://perma.cc/SW38-LZUF; see also, Joint Statement of Chris Fonzone, Office of the Director of National Intelligence, George Barnes, NAtional Security Agency, David Cohen, Central Intelligence Agency, Paul Abbate, Federal Bureau of Investigation, Matt Olsen, Department of Justice, before the Senate Judiciary Committee, June 13, 2023, https://www.judiciary.senate.gov/imo/media/doc/2023-06-13%20-%20Joint%20statement%20-%20ODNI,%20NSA,%20CIA,%20FBI,%20DOJ%20(1).pdf, hereinafter, Intelligence Community Joint Statement to Senate Judiciary Committee.

these rules, such as queries of a U.S. Senator, a state senator, and a judge, and online dating matches.[6] And improper queries are still alarmingly frequent. According to multiple audits, in 2022 and 2023 improper queries occurred at a 1.7 to 4.2 percent rate;[7] even the low-end non-compliance rate translates to an estimated 3,400 improper queries in 2022 and 1,000 in 2023.[8] A system in which improper queries occur on a daily basis is not a system that can be relied upon. Self-policing cannot safeguard Americans' privacy - only a warrant rule and independent court approval can prevent abuse.

A warrant rule for U.S. person queries of FISA 702 data would not only shield Americans from misconduct, it would also meet security needs. After extensive review and reporting by PCLOB and the President's Intelligence Advisory Board—as well as a rigorous defense of the status quo offered by intelligence agencies—U.S. person queries have been shown to provide value in only a limited set of situations.[9] And the warrant rule[10] has been carefully tailored to account for all of them.

The warrant rule includes exceptions when there is consent, for queries to identify malware, and for metadata queries. This accounts for the three main areas in which, based on reporting from PCLOB, the President's Intelligence Advisory Board, and the intelligence community's own testimony on FISA 702,[11] U.S. person queries have proven useful: in combating cyber attacks, foreign plots targeting Americans, and foreign recruitment for espionage. In terms of cyber attacks, queries focused on cyberthreat signatures are exempt, alerts and intelligence based on network traffic are covered under the metadata exception, and, perhaps most importantly, any US company or critical infrastructure entity being targeted for a cyber attack can simply consent to have the government run queries on that entity. The consent exception also accounts for value that has been described as stemming from querying targets of foreign assassination and kidnapping plots. In such situations an American can simply consent to queries being conducted to protect them. And, in the limited number of cases in which queries helped the government discover suspicious

---

[6] *See*, *FISA Section 702 Memorandum Opinion and Order* (April 11, 2023), 86, https://perma.cc/968W-3L7J; see also, PCLOB FISA 702 Report.

[7] See, Federal Bureau of Investigations Office of Internal Auditing, "FISA Query Audit," May 10, 2023, https://perma.cc/JNU3-2SNX (listing a noncompliance rate of 4 for queries occurring between 2021 and 2022); *see also*, *FISA Section 702 Memorandum Opinion and Order* (April 11, 2023), 84 (listing a noncompliance rate of 1.7 in 2022), *see also*, *Memorandum Opinion and Order* (April 4, 2024), 38, https://perma.cc/4VVE-EZZ7 (listing a noncompliance rate of 4.2 for January 2022 to October 2023).

[8] The FBI conducted 204,090 U.S. person queries in 2022 and queried 57,094 unique U.S. person identifiers in 2023. Based on noncompliance rates, this translates to 3,469 to 8,570 improper US person queries in 2022, and 971 to 2398 improper US person queries in 2023 (although because only the number of unique query terms rather than actual number of queries was published for 2023, we lack complete data). See, Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, "Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Authorities, Calendar Year 2022," April 2023, https://perma.cc/BKP5-ZWYC; see also, "ODNI 2023 Transparency Report."

[9] See, PCLOB FISA 702 Report; see also, The President's Intelligence Advisory Board, "President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations for Reauthorization," July 2023,https://perma.cc/2GKD-8QM7, hereinafter PIAB FISA 702 Report; see also, Intelligence Community Joint Statement to Senate Judiciary Committee.

[10] Specifically, the warrant rule proposed by Senators Lee and Durbin in the 2024 SAFE Act as well as in the amendments offered on the House and Senate floor in the 2024 April votes on legislation reauthorizing FISA 702. See, S. 3961 (2024), The Security and Freedom Enhancement (SAFE) Act, https://www.congress.gov/bill/118th-congress/senate-bill/3961/text.

[11] See, Jake Laperruque and Gene Schaerr, "Debunking Myths on the National Security Impact of Warrants for U.S.Person Queries," April 7 2025, https://cdt.org/insights/debunking-myths-on-the-national-security-impact-of-warrants-for-u-s-person-queries/; see also; PCLOB FISA 702 Report; see also, PIAB FISA 702 Report.

foreign contacts of U.S. persons to determine whether they were collaborating with hostile foreign powers, an exemption for metadata queries means the government would not need a warrant to identify these contacts. There are no documented cases in which content queries were critical to advancing an investigation against a foreign agent.[12] Even if content queries could provide this value, reading the private emails of an American to advance a criminal investigation of them is exactly when we expect warrants to be required.

FISA 702 is set to expire in just over one year; Congress should not reauthorize this law unless a warrant rule is included.

II. Warrantless Purchases and the Data Broker Loophole

If the government demanded that Verizon provide a customer's cell phone location data for the past 90 days or that Google turn over a user's browsing data, those companies would only comply if the demand was accompanied by a warrant; it would be unimaginable if a company responded to a such a demand by saying, "We'll turn over those records if you have a warrant … or if you give us $100 instead."

Yet this is in essence what the Data Broker Loophole permits. It undermines Americans' privacy by allowing law enforcement and intelligence agencies to use taxpayer dollars to circumvent court approval requirements established by the Fourth Amendment and in statute by purchasing this data from data brokers. Conditioning surveillance on independent court authorization and evidence of wrongdoing is a foundation of our democratic system. When the government bypasses these rules by simply buying Americans' sensitive information, it violates privacy rights and opens the door to abuse.

Data purchases are a common practice, with reported use by the FBI, DHS, NSA, DEA, ICE, CBP, and IRS, as well as state and local police across the country.[13] Unfortunately, its use is often shrouded in secrecy, leaving Americans with scant knowledge on how often their data is being collected by the government and for what purposes. Highly sensitive information that law enforcement and intelligence agencies purchase includes cell phone location data, Internet browsing records, purchase records, and communications metadata. These data quite often can be highly revealing even in isolation, and in combination can paint a picture of the most intimate detail of individuals' lives. This sensitivity is why compelled disclosure of some records—such as weeklong spans of cell site location information—requires a full probable cause warrant, and why all compelled disclosure of each of them generally requires court approval.

---

[12] 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, PCLOB FISA 702 Report; see also, PIAB FISA 702 Report, 36.

[13] Shenkman, C., Franklin, S.B., Nojeim, G., and Thakur, D. (2021) *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*. Center for Democracy & Technology, https://perma.cc/9SSC-KEZJ; see also, Sara Morrison, *Vox*, "A surprising number of government agencies buy cell phone location data. Lawmakers want to know why," December 20, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.

Government data purchases also circumvent the principal FISA reform that Congress enacted when it overwhelmingly passed the USA FREEDOM Act in 2015.[14] This legislation was the product of a two-year debate over the NSA's telephony metadata bulk collection program which vacuumed up the phone records of hundreds of millions of Americans with a single court order.[15] Reacting to public outrage, Congress outlawed bulk collection by requiring individualized demands for Americans' records based on a specific selection term.[16] Data purchases directly undercut this rule, allowing intelligence and law enforcement agencies to collect Americans' data in bulk. In fact, in a troubling echo of the bulk collection debate fifteen years ago, NSA data purchases include Americans' communications metadata.[17]

When Congress passed the USA FREEDOM Act, it did so to ban bulk collection of Americans' data, not to require that future bulk collection include a price tag. This legislation was the most extensive FISA reform passed in the 21st century, and Congress should not permit the Data Broker Loophole to undermine it. Congress should pass legislation, such as the Fourth Amendment Is Not For Sale Act,[18] to close this loophole and stop data purchases from undermining Americans' rights, the Fourth Amendment, and critical surveillance reform laws.

III. The Importance of PCLOB for Safeguarding Privacy and Preventing Surveillance Abuse

Guarding against surveillance abuse will require vigilant, ongoing oversight, and achieving effective surveillance reform—not only regarding the issues discussed above but the myriad of other privacy issues we face now or will confront in the future. This requires thorough assessment of surveillance activities across the intelligence community. PCLOB has for over a decade played a critical role in support of these objectives, proving invaluable to Congress and the public alike. Now Congress needs to act to ensure it can provide this service in the future by safeguarding its independence.

PCLOB had a major impact on the debate over PATRIOT Act bulk collection, debunking the frequently repeated intelligence community myth that this dragnet surveillance program had stopped numerous terrorist attacks.[19] It also made policy recommendations to end the bulk collection programs and to reform FISA Court procedures—such as requiring publication of rulings and creation of amici to defend privacy

[14] Jennifer Steinhauer and Jonathan Weisman, New York Times, "U.S. Surveillance in Place Since 9/11 Is Sharply Limited," June 2, 2015, https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.
[15] See, Jake Laperruque, Project On Government Oversight, "The History and Future of Mass Metadata Surveillance," June 11, 2019, https://ww.pogo.org/analysis/the-history-and-future-of-mass-metadata-surveillance.
[16] Id.
[17] Charlie Savage, *New York Times*, "N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says," January 25, 2024, https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html; see also, Dell Cameron, Wired, "The Pentagon Tried to Hide That It Bought Americans' Data Without a Warrant," January 26, 2024, https://www.wired.com/story/pentagon-data-purchases-wyden-letter/.
[18] H.R. 4639 (2023), the Fourth Amendment Is Not For Sale Act.
[19] Justin Elliott and Theodoric Meyer, *Pro Publica*, "Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence," October 23, 2013, https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence; What's the Lauren Kirchner, *Pro Publica*, "Evidence Mass Surveillance Works? Not Much," November 18, 2015 https://www.propublica.org/article/whats-the-evidence-mass-surveillance-works-not-much.

rights—that became law as part of the USA FREEDOM Act.[20] Its reports on FISA 702 have brought to the public essential information on how the program functions, compliance issues, and distinctions about where it does and does not provide value.[21] Many of the recommendations in PCLOB's 2023 FISA 702 report mirror those in legislation passed by the House Judiciary Committee several months later.[22]

Given the value PCLOB has provided on these and other surveillance issues, it is alarming that earlier this year President Trump fired three members of the Board. This pushes PCLOB into a sub quorum status, and far more importantly, endangers the independence that is vital to PCLOB performing in an effective manner. As CDT and over 25 other civil society organizations have highlighted,[23] if PCLOB members are subjected to at-will firing, it will be impossible as a practical matter for the Board to perform its most important tasks. Going forward, a president of either party could fire PCLOB members to block off investigations into controversial or improper surveillance activities, or to stymie the Board from issuing reports that reveal surveillance abuse and call for policy reform. The mere threat of firings would chill PCLOB from being vigilant in its duties, with the Board curtailing investigations and editing reports so as not to incur White House disfavor. As a corollary, this will undermine public trust in PCLOB and the intelligence community at large. If, for example, PCLOB reports that FISA surveillance powers are being used properly, the public and the Congress will be left to wonder if impropriety had been ignored to avoid firing. It is for precisely these reasons that Congress in 2007 removed from law a provision stating that PCLOB's members "serve at the pleasure of the President."

Until this issue is addressed, PCLOB will not be able to serve as an effective entity, even if new members are appointed and a quorum is restored. Congress should act to protect and strengthen PCLOB, including with legislative action to reaffirm and bolster PCLOB's independence.

***

This hearing marks a positive start in Congress' consideration of important surveillance reform issues. We urge Congress to continue its work to protect Americans' privacy and civil liberties, building new safeguards against abuse and closing loopholes that are being exploited to undermine Americans' rights. In particular, we recommend Congress address the three issues highlighted above in any legislation taken up within the next year to reauthorize FISA 702.

[20] See, Privacy and Civil Liberties Oversight Board, "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court," January 23, 2014, https://perma.cc/EAG6-K65F.
[21] See, PCLOB FISA 702 Report.
[22] H.R. 6570 (2023), The Protect Liberty and End Warrantless Surveillance Act.
[23] See, Coalition Letter on Firing of PCLOB Members, January 31, 2025, https://cdt.org/insights/cdt-leads-coalition-letter-condemning-pclob-firings/.