CENTER FOR DEMOCRACY & TECHNOLOGY

Comment to the Privacy and Civil Liberties Oversight Board Regarding Examination of and Reforms to Section 702 of the Foreign Intelligence Surveillance Act

November 4, 2022

The Center for Democracy & Technology ("CDT")[1] submits the following comments detailing the organization's views and recommendations regarding Section 702 of the Foreign Intelligence Surveillance Act ("Section 702") in response to the request of the Privacy and Civil Liberties Oversight Board ("PCLOB") for public comment as the Board continues to review Section 702.[2] With Section 702 set to expire at the end of 2023, now is a critical time to review current practices under the law, and consider potential reforms that would strengthen civil rights and civil liberties. These comments are intended to support the PCLOB by both highlighting points of factual inquiry and setting forth policy priorities that Congress should focus on ahead of the law's scheduled expiration.

Section 702 is a warrantless surveillance authority established by Congress in 2008. The purpose of Section 702 is to collect foreign intelligence information abroad; surveillance pursuant to the law must be targeted at those believed to be non-U.S. persons located outside of the United States. Unlike Executive Order 12333—under which the President may pursue surveillance abroad absent any Congressional limits based on their commander-in-chief authority—Section 702 allows the government to compel production of communications and data by U.S. companies, as well as their technical assistance in facilitating surveillance authorized by the law. And, although targets are meant to be non-U.S. persons located outside of the United States, Section 702 surveillance involves significant incidental collection of U.S. persons' communications.

PCLOB issued a report on Section 702 in 2014, amid the height of public and Congressional concern over overbroad national security surveillance that was shrouded in secrecy.[3] That report became the best source of public information about how Section 702 operated, and involved the declassification of a significant number of facts that helped enhance public understanding of how the law was interpreted and utilized. PCLOB plays a key role in promoting transparency and improving public understanding of,

[1] The Center for Democracy & Technology is a 501(c)3 nonpartisan nonprofit organization that works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice. Among our priorities is preserving the balance between security and freedom.
[2] See, Federal Register Vol. 87, No. 185, *Notice of the PCLOB Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act (FISA)*. https://www.govinfo.gov/content/pkg/FR-2022-09-26/pdf/2022-20415.pdf.
[3] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014. https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf. Hereinafter, *PCLOB 702 Report*.

and discourse on, national security surveillance issues; we expect and encourage PCLOB to continue this role in its upcoming report on Section 702.

Our comment examines six key areas regarding Section 702: 1) the scale and impact of collection; 2) purposes for which collection is authorized; 3) queries that return the communications and data of U.S. persons; 4) domestic law enforcement use; 5) the collection technique referred to as "Abouts Collection;" and 6) providing notice to defendants. For each area, we recommend the PCLOB make factual inquiries to better inform the public debate, policy changes, or both.

I. Section 702 is a massive and powerful surveillance system, yet lawmakers and the public lack key information about how it affects civil rights and civil liberties

A. The scale of collection under Section 702 is immense, with little explanation of its expansion or clarity on how it affects U.S. persons

Section 702 is the only statutory federal surveillance authority that permits monitoring of communications content in the absence of judicial approval of the target of surveillance. This has opened the door to surveillance that is massive in scale, and appears to be growing at an alarming rate.

In 2014, when the PCLOB released its first comprehensive report on Section 702,[4] there were 89,138 targets according to the most recently available data.[5] In 2018, when Congress last reauthorized Section 702, available data indicated there were 106,469 targets.[6] Yet today, according to the most recently available data, there are 232,432 targets.[7] This represents an astounding 118% increase in the number of known targets since the last time Congress considered whether to reauthorize Section 702, and a 161% increase in the number of known targets since PCLOB last reviewed this surveillance authority. This growth of Section 702 surveillance inevitably increases the scale of incidental collection, whereby U.S. persons and individuals across the globe with no connection to foreign intelligence needs have their communications monitored.

---

[4] *PCLOB 702 Report*.
[5] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2013*, June 26, 2014. https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf
[6] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2016* (April 2017). https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf.
[7] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2021* (April 2022). https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf

PCLOB should investigate the causes of this increase and its impact. Has the basis for designating targets changed, or become more lax in ways that would lead to such an increase? Are there more categories of information — or types of individuals and organizations — that are now subject to targeting? There may be entirely legitimate reasons for the increase, such as shifting national security priorities and increased use of different communications platforms. But, given the magnitude of this increase, added clarity is important for stakeholders and lawmakers to assess what new rules and limits may be needed for Section 702 surveillance.

> ***Inquiry Recommendation #1: We recommend the PCLOB investigate and report on the causes for the significant increase in Section 702 targets in recent years, as well as the degree to which this increase has amplified incidental or mistaken collection of communications disconnected from foreign intelligence.***

In addition to the lack of information on why Section 702 surveillance is increasing, the public still has no information on how broadly this system monitors U.S. persons' private communications. Given the scale of targets, it is virtually certain that a large number of U.S. persons have their texts and emails swept up in Section 702 incidental collection, all without the warrant process that any communications monitoring involving U.S. persons typically requires. Yet, after decades of debate and multiple reauthorizations of the law, the number of U.S. persons affected is still hidden.

This is especially frustrating given the intelligence community's explicit commitment to transparency in this area. In 2016, the Office of the Director of National Intelligence (ODNI) assured Congressional leaders that it would provide an estimate of how many U.S. persons' communications were collected pursuant to Section 702, and do so numerous months before the scheduled expiration of the law in 2017.[8] Several months after making this commitment, ODNI refused to honor it, leaving members of Congress in the dark as to how Section 702 affects their constituents, even as the intelligence community pressed Congress to reauthorize the law.[9] The public has never received an adequate explanation for this about-face, and the intelligence community has not signaled publicly any renewed efforts to estimate the number of U.S. persons swept up in Section 702 surveillance. This information

[8] *Letter from House Judiciary Members to Director of National Intelligence James Clapper on discussions regarding Section 702 surveillance transparency*, December 16, 2016. https://judiciary.house.gov/sites/democrats.judiciary.house.gov/files/documents/letter%20to%20director%20clapper%20(12.16.16).pdf

[9] Dustin Volz, "NSA backtracks on sharing number of Americans caught in warrant-less spying," *Reuters*, June 9, 2017. https://www.reuters.com/article/us-usa-intelligence/nsa-backtracks-on-sharing-number-of-americans-caughtin-warrant-less-spying-idUSKBN19031B.

would be of vital importance to the public debate around Section 702, and every effort should be made to provide it.[10]

> ***Inquiry Recommendation #2: We recommend the PCLOB report on why the Office of the Director of National Intelligence reversed its commitment to estimating the number of U.S. persons affected by Section 702. We recommend the PCLOB advocate in the strongest terms possible for such an estimate to be publicly released before the Section 702 expiration.***

B. The public lacks basic knowledge about the degree to which Section 702 surveillance disproportionately harms marginalized communities

Not only does the public have little information on how many individuals in the United States Section 702 sweeps up, it also has shockingly little knowledge of which communities it most affects. In assessing the costs of Section 702 and what new safeguards are most needed, understanding whether it disproportionately collects private communications of already over-surveilled communities is essential. Yet the public has practically no information on FISA's level of impact on marginalized groups, such as racial and religious minorities.[11]

Inquiry in this area is especially important given how often surveillance conducted in the name of national security has disproportionately affected — and often intentionally focused on — marginalized communities. Following the September 11 attacks, counterterrorism surveillance was fraught with anti-Muslim bias and improper treatment of Muslim communities. With federal support, the New York Police Department invasively monitored Muslim communities for over a decade; standard life activities, student groups, community centers, and Mosques were all kept under watch, while informants who government officials labeled "Mosque crawlers" were pressed to gather information on their peers.[12] In

---

[10] See, Sharon Bradford Franklin, New America's Open Technology Institute, "Statement to the Privacy and Civil Liberties Board Regarding Exercise of Authorities Under The Foreign Intelligence Surveillance Act (FISA)," August 31, 2020. https://d1y8sb8igg2f8e.cloudfront.net/documents/Sharon_Bradford_Franklin_Comments_to_PCLOB_on_FISA_8-31-20.pdf ("The PCLOB should hold the NSA to its promise to develop substitute measures that will provide some insight into the scope and scale of collection of U.S. person information under Section 702").

[11] See Jake Laperruque, The Project On Government Oversight, "In Support of Research and Reporting on the Disparate Use and Impact of FISA," April 8, 2019. https://www.pogo.org/testimony/2019/04/in-support-of-research-and-reporting-on-the-disparate-use-and-impact-of-fisa; see also also, Sharon Bradford Franklin, New America's Open Technology Institute, "Statement to the Privacy and Civil Liberties Board Regarding Exercise of Authorities Under The Foreign Intelligence Surveillance Act (FISA)," August 31, 2020. https://d1y8sb8igg2f8e.cloudfront.net/documents/Sharon_Bradford_Franklin_Comments_to_PCLOB_on_FISA_8-31-20.pdf.

[12] The American Civil Liberties Union, "Factsheet: The NYPD Muslim Surveillance Program." https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program; see also, Adam Goldman and Matt Apuzzo,"With cameras, informants, NYPD eyed mosques," *Associated Press*, February 23, 2012, https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques; Matt Apuzzo and Joseph Goldstein, "New York Drops Unit That Spied on Muslims," *New York Times*, April 15, 2014. https://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-is-disbanded.html.

prior decades, national security surveillance has also been coopted to monitor racial minorities, activists, and dissidents.[13]

In order to truly understand the impact of Section 702 — and, in particular, the impact that incidental collection has on individuals in the United States — it is key not just to have an estimate of the overall quantity of persons affected, but also how that surveillance is distributed among different groups.

Congress has previously shown interest in this goal. In 2020, both the House and Senate passed versions of the USA FREEDOM Reauthorization Act that tasked the PCLOB with researching and issuing a public report on "the extent to which [First Amendment-protected] activities and protected classes … are used to support targeting decisions in the use of authorities pursuant to [FISA] and (2) the impact of the use of such authorities on [First Amendment-protected] activities and protected classes."[14] While this bill did not become law due to disputes over unrelated amendments and disruptions prompted by the COVID-19 pandemic, its inclusion in bills passed in both chambers shows strong Congressional interest. And, independent of any Congressional mandate, it is a topic well worth PCLOB's examination.

> ***Inquiry Recommendation #3: We recommend the PCLOB investigate and report on methodologies the intelligence community could use to better understand and report on the degree to which Section 702 incidental collection—as well as other components of FISA—disproportionately affects racial and ethnic minorities, religious minorities, immigrants, and other marginalized communities. We further recommend PCLOB investigate and report on the degree to which First Amendment-protected activities and membership of protected classes such as race, ethnicity, and religion affect targeting decisions.***
>
> ***Policy Recommendation #1: We recommend the PCLOB support legislative reforms that significantly limit the degree to which membership of protected classes or exercise of First Amendment-protected activities can be the basis of FISA targeting designations.***

II. Section 702 permits individuals to be targeted for purposes far beyond national security priorities, needlessly placing individuals at risk of invasive surveillance

Section 702 permits warrantless surveillance in a troublingly broad manner. *Any* non-U.S. person located abroad can be designated as a target, so long as a significant purpose is to acquire foreign

[13] See, The Martin Luther King, Jr. Research and Education Institute, "Federal Bureau of Investigation (FBI)." https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi; see also, U.S. Senate, Select Committee to Study Government Operations with Respect to Intelligence Activities, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate: together with additional, supplemental, and separate views*, April 26, 1976.
[14] H.R.6172, Sec. 405(a), (2020).

intelligence information. The term "foreign intelligence information" is defined broadly, and includes "information with respect to a foreign power or foreign territory that relates to … the conduct of foreign affairs."[15]

This creates the potential for large-scale targeting of individuals who are in no way connected to security threats or foreign powers. As CDT has previously noted, if programs of the U.S. State Department and other U.S. foreign projects "relate to the foreign affairs" of the U.S. (and it seems they should), Section 702 surveillance could include efforts to collect information regarding topics as mundane and commonplace as animal conservation, international sports logistics and planning, cultural and historic events, wildlife tracking, humanitarian aid missions, music and art events, consumer product standards, and environmental research and preservation efforts.[16]

Non-U.S. persons can become Section 702 targets for engaging in innocuous activities such as journalism, activism, or international business.[17] Such broad surveillance harms human rights, endangers the sustainability of key U.S.-EU data protection agreements, and makes it more likely that U.S. persons communicating with innocent individuals abroad will be swept up in warrantless surveillance.

Fortunately, there are several ways to address this issue. One reform would be to require that, when the purpose of designating a target is only to collect information that relates to national security or conduct of foreign affairs (subclause 2 of "foreign intelligence information," codified at 50 USC 1801(e)), the target must be an agent of a foreign power.[18] This proposal would still allow targeting as occurs now (without any showing that the target is an agent of a foreign power) when the purpose of the surveillance is to collect information that relates to attacks, sabotage, international terrorism, the international proliferation of weapons of mass destruction, or clandestine intelligence activities by a foreign power (subclause 1 of the "foreign intelligence information" definition).[19]

---

[15] 50 USC 3365(2).
[16] Mana Azarmi, The Center For Democracy & Technology, "Urgent Fix Needed: USA Liberty Act Needs To Better Focus Surveillance Under FISA 702," October 20, 2017. https://cdt.org/insights/urgent-fix-needed-usa-liberty-act-needs-to-better-focus-surveillance-under-fisa-702/. Hereinafter, Azarmi, "Urgent Fix Needed."
[17] One potential limit on this is the restriction imposed in Presidential Policy Directive 28, which states that the U.S. "shall not collect signals intelligence for *the* purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion." The White House, "Presidential Policy Directive -- Signals Intelligence Activities," January 17, 2014 (emphasis added). https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. However, because this rule merely states that this must not be *the* purpose, the government could likely incorporate such factors as a purpose of targeting decisions in combination with foreign intelligence purposes, such as acquiring information with respect to a foreign territory that relates to the conduct of foreign affairs.
[18] Azarmi, "Urgent Fix Needed."
[19] Azarmi, "Urgent Fix Needed."

CENTER FOR DEMOCRACY & TECHNOLOGY

Inquiry Recommendation #4: We recommend the PCLOB examine and report on the extent to which limiting Section 702 surveillance to attacks, sabotage, international terrorism, WMD proliferation and clandestine intelligence activities of a foreign power (subclause 1 of the "foreign intelligence information definition) would hamper national security

Another option for preventing overbroad surveillance under Section 702 would be to build from limits that the Administration itself has already embraced. On October 7, President Biden issued a new Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities ("Signals Intelligence EO").[20] This order requires that signals intelligence collection be conducted only if in pursuit of one or more of the following 12 broad and flexibly-described purposes:

1. Understanding the capabilities, intentions, and activities of foreign governments, militaries, factions, and political organizations in order to protect national security;
2. Understanding the capabilities, intentions, and activities of foreign organizations that pose a threat to national security;
3. Understanding transnational threats that affect security, such as climate change, public health risks, humanitarian threats, political instability, and geographic rivalry;
4. Protecting against foreign military capabilities and activities;
5. Protecting against terrorism and hostage-taking;
6. Protecting against espionage, sabotage, assassination, or other intelligence activities;
7. Protecting against development, possession, or proliferation of weapons of mass destruction;
8. Protecting against cybersecurity threats;
9. Protecting personnel of the United States and its allies;
10. Protecting against transnational criminal threats;
11. Protecting the integrity of elections and political processes, government property, and United States infrastructure; and
12. Advancing collection or operational capabilities in furtherance of the previous 11 objectives.[21]

The Signals Intelligence EO also prohibits signals intelligence from occurring for the following purposes:

1. Suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;
2. Suppressing or restricting legitimate privacy interests;
3. Suppressing or restricting a right to legal counsel; or

[20] The White House, "Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities," October 7, 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities. Hereinafter "Signals Intelligence EO."
[21] For full verbatim text of permissible purposes, see, "Signals Intelligence EO."

4. Disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.[22]

The Signals Intelligence EO does not specify whether these four purposes cannot be the *sole* purpose for collection, the *primary* purpose for collection, or merely *a* purpose of the collection. Relatedly, the Signals Intelligence EO authorizing provision requiring that surveillance be conducted "in pursuit" of the enumerated goals is vague, and subject to flexible interpretations. Further clarity is necessary to know if these limits and prohibitions will be effective; we encourage the PCLOB to examine and provide public insight on how these provisions are interpreted.

The Signals Intelligence EO currently restricts the intelligence community from engaging in Section 702 beyond those purposes;[23] there should be no objection to codifying such a rule into law. Many of these purposes are extremely broad. In its consideration of them, PCLOB should determine which are impermissibly broad and the extent to which they could be narrowed.

Inquiry Recommendation #5: We recommend the PCLOB examine and report on whether the new Signals Intelligence EO bars any surveillance activities previously conducted pursuant to Section 702, or if the purposes authorized in the Signals Intelligence EO fully encompass the existing purposes for which Section 702 is used.

Policy Recommendation #2: We recommend the PCLOB support legislative reforms to limit the purposes for Section 702 surveillance. Specifically, the PCLOB should support either 1) requiring that targets can only be designated pursuant to the purpose limits in the Signals Intelligence EO, narrowed to the extent possible, or 2) requiring that whenever targets are designated solely for the purpose of collecting information that relates to national security or conduct of foreign affairs (subclause 2 of the "foreign intelligence information" definition), there must be reasonable suspicion to believe those targets are agents of a foreign power.

III. Warrantless U.S. person queries of Section 702-acquired communications are improperly invasive, repeatedly involve mass compliance violations, and lack effective limits and oversight

[22] Text is verbatim from Executive Order. The Executive Order also provides a clarifying detail that, while business information is subject to collection for the enumerated national security reasons, such information cannot be collected solely to provide a competitive business advantage.

[23] The Signals Intelligence EO does give the president the authority to freely add new purposes for which signals intelligence collection is authorized. The PCLOB may want to consider how a statutory set of authorized purposes for Section 702 collection could ensure the government has the ability to respond to any new types of threats in a timely manner.

One of the most significant problems with Section 702 is the practice of conducting U.S. persons queries — meaning looking for communications and data about a U.S. person from databases of Section 702-acquired information — absent necessary limits and safeguards. This system bypasses basic Fourth Amendment rights and protections for surveillance of U.S. persons, and has resulted in mass compliance violations. The existing rules are riddled with loopholes and have proven ineffective, reflecting a need for significant reform.

While civil liberties advocates often refer to the system of U.S. person queries as the "backdoor search loophole," the intelligence community has long argued that these queries do not constitute a "search" under the Fourth Amendment to the U.S. Constitution because the process applies to data already in possession of the government. However — while raising an important legal question — the claim that U.S. person queries are technically not searches misses the point of the critique. U.S. person queries are "backdoor searches" because they achieve the *same effect as a search* — U.S. government officials deliberately seeking out, reviewing, and using U.S. persons' private communications — without ever going through the court approval process that is required for searches. Individuals face the same harm to their privacy rights as with a search of data not already possessed, but without any of the protections.

The rules that do exist for U.S. person queries are wholly inadequate. While the 2018 reauthorization of Section 702 did require a warrant to conduct certain U.S. person queries in limited circumstances,[24] it suffers from a series of exceptions so broad that they subsume the rule.

First, the warrant requirement only applies to U.S. person queries conducted "in connection with a predicated criminal investigation."[25] This excludes a multitude of situations when government officials may conduct U.S. person queries. As New America's Open Technology Institute has previously noted, "as reflected in the FBI's Section 702 minimization procedures, 'it is a routine and encouraged practice' for the FBI to run searches through collected 702 data even during preliminary investigative stages. Thus, [the law] would permit the FBI to continue to conduct unlimited warrantless searches through 702 data during early investigative stages, so it would never need to seek a warrant at the later predicated investigation phase."[26] Queries for activities such as assessments and background checks also elude the warrant requirement in current law. Ironically, situations where the FBI has the *least* suspicion of wrongdoing are the areas where it has *most* freedom to conduct U.S. person queries without court review.

[24] See 50 USC 1881a(f).
[25] 50 USC 1881a(f)(2)(A).
[26] Sharon Bradford Franklin, Just Security, "The House Intelligence Committee's Section 702 Bill is a Wolf in Sheep's Clothing," January 9, 2018. https://www.justsecurity.org/50801/house-intelligence-committees-section-702-bill-wolf-sheeps-clothing/.

Next, the warrant rule does not apply to any U.S. person queries conducted for investigations that "relate to the national security of the United States."[27] This term is undefined, and could be interpreted broadly, excluding a wide range of queries from court review. Additionally, the warrant requirement in current law does not apply to any U.S. person queries "designed to find and extract foreign intelligence information."[28] This could exempt not only queries focused solely on foreign intelligence, but also those that are primarily centered on domestic law enforcement, but have some foreign nexus.

Finally, the warrant rule does not apply to any U.S. person queries in which the FBI "determines there is a reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm."[29] This exception does not require threats to be imminent; it applies whenever a query could provide *any* assistance to mitigating such a threat. In effect, this exception removes the warrant requirement for U.S. person queries conducted to investigate any potential or recurring instances of most violent crimes.[30]

> ***Inquiry Recommendation #6: We recommend the PCLOB examine and report on how the government interprets each of these exceptions to the warrant requirement for U.S. person queries.***

The current system governing U.S. person queries of the Section 702 database is not only inconsistent with Fourth Amendment values and riddled with loopholes, it has proven disastrous for compliance. Over the past several years, the Foreign Intelligence Surveillance Court ("FISC") has documented an astounding number of serious violations of querying rules.

In an October 2018 opinion, the FISC documented mass abuse of the system through a process of "batch queries," whereby large numbers of queries were lumped together and conducted en masse. This included "a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime." In March 2017, FBI conducted queries on

[27] 50 USC 1881a(f)(2)(A).
[28] 50 USC 1881a(f)(2)(A).
[29] 50 USC 1881a(f)(2)(E)
[30] Surprisingly, despite the breadth of this exception, the government did not appear to invoke it when the FISC cited problematic queries related to investigations at would likely fit within the exception, such as domestic terrorism, gang violence, and organized crime. See, Memorandum Opinion and Order (FISA Ct. Nov. 18, 2020) (Boasberg, J.) available at https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, hereinafter, *FISC November 2020 Opinion.*
There may have been other problems associated with this particular queries that would have made invocation of the exception insufficient, but the PCLOB may benefit from investigating why the government did not defend its warrantless U.S. queries as justified by the 50 USC 1881a(f)(2)(E) exception.

70,000 identifiers related to individuals with access to FBI facilities. Later that year, the FBI conducted over 6,800 U.S. person queries in a single day.[31]

These problems continued in subsequent years. In a 2020 opinion, the FISC found that the FBI had conducted dozens of U.S. person queries to access Section 702-acquired data for predicated criminal investigations, while flaunting the narrow warrant rule even when it was meant to apply. The FISC also highlighted how over several months in 2019, the FBI conducted over 100 U.S. person queries as background checks that returned Section 702-acquired information. These were not to investigate threats, but rather to monitor "business, religious, civic, and community leaders" applying to the FBI's Citizen Academy program, crime victims, and maintenance staff working at field offices. Such practices may not have involved a predicated criminal investigation, but do appear to have violated an FBI Querying Procedure rule that queries be reasonably likely to return either foreign intelligence information or evidence of a crime.[32] These incidents were drawn from sample examinations rather than a comprehensive review, leading the FISC to conclude that there were "widespread violations of the querying standard" and that "similar violations of Section 702(f)(2) likely hav[ing] occurred across the [FBI]."[33]

> ***Inquiry Recommendation #7: We recommend the PCLOB examine and report on U.S. person queries since the most recent Section 702 reauthorization, and any compliance problems beyond those identified and discussed by the FISC in publicly available materials.***

In the absence of consistent, front-end judicial review for U.S. person queries, the fundamental problem the FISC identified will remain: "a misunderstanding of the querying standard—or indifference to it."[34] The cost will be regular invasion of individuals' privacy; past compliance issues have shown this means both the privacy of investigative targets who are entitled to due process, as well as individuals that are in no way suspected of wrongdoing or connected to investigations. The only way to remedy this problem is to enact a clear rule: all U.S. person queries should be subject to judicial approval, with

---

[31] See, Memorandum Opinion and Order (FISA Ct. Oct. 18, 2018) (Boasberg, J.) available at https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, hereinafter, *FISC October 2018 Opinion*; see also, Liza Goitein, *Just Security*, "The FISA Court's Section 702 Opinions, Part II: Improper Queries and Echoes of 'Bulk Collection,'" October 16, 2019. https://www.justsecurity.org/66605/the-fisa-courts-section-702-opinions-part-ii-improper-queries-and-echoes-of-bulk-collection/.

[32] "Querying Procedures Used by the Federal Bureau of Investigations in Connection With Acquisition of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended," September 16, 2019. https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Querying%20Procedures_10.19.2020.pdf

[33] *FISC November 2020 Opinion*; See also, Jake Laperruque, Just Security, "Key Takeaways From Latest FISA Court Opinion on Section 702 and FBI Warrantless Queries" (April 28, 2021). https://www.justsecurity.org/75917/key-takeaways-from-latest-fisa-court-opinion-on-section-702-and-fbi-warrantless-queries/.

[34] *FISC October 2018 Opinion*.

judges verifying that proper cause exists and procedures have been followed before Section 702-acquired communications of U.S. persons can be accessed.

> ***Policy Recommendation #3: We recommend the PCLOB support legislative reforms so that all U.S. person queries require a warrant. Specifically, if such queries return FISA-702 acquired information, that information would be blocked from review until the government obtains FISC approval that there is probable cause the relevant individual committed a crime or is an agent of a foreign power.***

IV. Section 702 was meant to focus on foreign intelligence, but absent effective use limits, this warrantless surveillance system has crept into the realm of domestic law enforcement.

Section 702 was enacted with the clear intent of establishing a foreign-focused system for gathering foreign intelligence and combating international threats. It was this separation from domestic law enforcement—where warrants are required for surveillance as a Fourth Amendment safeguard—that made Section 702 acceptable to Congress.

Yet, in practice, the fruits of Section 702 surveillance have crept into the realm of domestic law enforcement. According to the FISC's November 2020 opinion highlighting problematic U.S. person queries, an oversight review discovered dozens of queries were in support of predicated domestic criminal investigations.[35] These investigations focused on crimes such as health care fraud, gang violence, organized crime, public corruption, bribery, and domestic policing issues that appear completely disconnected from the foreign intelligence purposes for which Section 702 is supposed to exist.[36] Indeed, the FISC stated, "none of these queries [were] related to national security."[37]

Because these incidents were discovered as part of a limited internal review, it is likely that there are many other similar instances of Section 702-acquired data being used for domestic policing.

> ***Inquiry Recommendation #8: We recommend the PCLOB investigate and report on the full range of domestic law enforcement investigations in which Section 702 data has been queried or used, and how frequently information collected under Section 702 is used for domestic policing.***

---

[35] *FISC November 2020 Opinion*; See also, Jake Laperruque, Just Security, "Key Takeaways From Latest FISA Court Opinion on Section 702 and FBI Warrantless Queries" (April 28, 2021). https://www.justsecurity.org/75917/key-takeaways-from-latest-fisa-court-opinion-on-section-702-and-fbi-warrantless-queries/.
[36] *FISC November 2020 Opinion*, at 42.
[37] *FISC November 2020 Opinion*, at 42.

Efforts have been made to place use limits on Section 702 to prevent mission creep into the realm of domestic policing, but they have been wholly inadequate. In 2015, ODNI announced a new policy whereby Section 702-acquired information would only be used as evidence in court for a set of "enumerated serious crimes."[38] When Section 702 was reauthorized in 2018, a similar measure was included in the legislation and codified. Specifically, it requires that Section 702 information "not be used in evidence against that United States person … in any criminal proceeding unless" it involves certain serious offenses.[39]

These measures recognize the principle that Section 702 should largely be separated from domestic policing, but do so in an ineffective manner: By only applying the limit to *criminal court proceedings*, these rules allow Section 702-acquired information to serve as a major part of the *investigation* for any domestic criminal offense. Section 702-acquired information can be used to initiate any domestic investigation, can be used to designate persons of interest and suspects, can be the foundation for advancing such designees towards prosecution, and can be used to derive other evidence that is integral to court proceedings. Law enforcement's longstanding use of parallel construction shows how easily this loophole could be exploited to have Section 702-acquired information serve as significant value to domestic investigations in these ways without running afoul of the existing use limits.[40] The rule also fails to address the significant portion of prosecutions that end in plea bargains rather than going to court.

In order for use limits to be effective, they must apply to *all* components of domestic policing and investigations, not simply be tacked onto the tail end when the damage is already done.

Another serious problem with existing use limits is how permitted uses are framed. Specifically, current law permits use for any crime that "affects, involves, or is related to the national security of the United

[38] The offenses included in this set of "serious crimes" were: "(A) criminal proceedings related to national security (such as terrorism, proliferation, espionage, or cybersecurity) or (B) other prosecutions of crimes involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e); (vi) cybersecurity; (vii) transnational crimes; (or (vii) human trafficking."
See, Office of the Director of National Intelligence, IC On The Record, "VIDEO: ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," February 4, 2015.
https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on

[39] Use of Section 702 for criminal proceedings is authorized when "(I) the criminal proceeding affects, involves, or is related to the national security of the United States; or (II) the criminal proceeding involves— (aa) death; (bb) kidnapping; (cc) serious bodily injury, as defined in section 1365 of title 18; (dd) conduct that constitutes a criminal offense that is a specified offense against a minor, as defined in section 20911 of title 34; (ee) incapacitation or destruction of critical infrastructure, as defined in section 5195c(e) of title 42; (ff) cybersecurity, including conduct described in section 5195c(e) of title 42 or section 1029, 1030, or 2511 of title 18; (gg) transnational crime, including transnational narcotics trafficking and transnational organized crime; or (hh)human trafficking." See, 18 USC 1881e(a)(2).

[40] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (January 2018).
https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf.

States," as determined by the Attorney General. This framing could be interpreted as opening the door to using Section 702 for a huge range of offenses, such as if an investigation for any low-level offense might be used to leverage an individual to become an informant.

> ***Policy Recommendation #4: We recommend the PCLOB support legislative reforms that close existing loopholes, and properly limit use of Section 702 for domestic law enforcement. Use limits should focus on a narrow set of national security and public safety priorities, be clearly enumerated rather than subject to broad interpretation by the Executive, and apply to all stages of domestic law enforcement activities and investigation, rather than just court proceedings.***

V. Section 702 should not permit collection of communications other than those to and from targets.

Section 702 was designed to allow surveillance of designated targets. As with all forms of communications surveillance, the clear impetus underlying this was to authorize collecting communications to and from targets. Yet, as new details of how Section 702 operated came to light in 2013, it was revealed that the government was conducting surveillance far beyond this traditional meaning.[41] In addition to collecting communications to and from targets, the government was also collecting communications that merely *mentioned* targets or that specifically mentioned a unique selector associated with the target, such as an email address or username.

This system, now commonly referred to as "Abouts Collection," has proven calamitous in terms of law, policy, and technical feasibility. Abouts Collection has been paused since 2017 due to compliance problems, but Abouts Collection could freely resume upon notification to Congress that the FISC has given the necessary certification.[42]

From a legal standpoint, Abouts Collection goes beyond what Congress intended to authorize when it established Section 702. There is no clear authorization of this authority in the text of the law, nor were there mentions of it in Congressional debate, hearings, or public discourse around the law as it was passed.[43] Abouts Collection takes the basic concept that underpins our entire system of search and

[41] Charlie Savage, *New York Times*, "N.S.A. Said to Search Content of Messages to and From U.S.," August 8, 2013. https://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html.
[42] Charlie Savage, *New York Times*, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets," April 28, 2017. https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html?smid=tw-share&_r=2.
[43] In its 2014 report on Section 702, the PCLOB stated that "PRISM collection is clearly authorized by the statute," but did not state the same regarding Abouts Collection, instead maintaining only that "the statute can permissibly be interpreted as allowing such collection." *PCLOB 702 Report*, at 9.

seizure — that such activities should be based on cause — and flips it on its head. For Abouts Collection, the fruits of a search themselves become the justification for that search. Indeed, in 2014 the PCLOB declared that Abouts Collection "push[es] the entire [Section 702] program close to the line of constitutional reasonableness."[44] Similarly, the FISC has described Abouts Collection as the component of Section 702 collection "presenting the Court the greatest level of constitutional and statutory concern."[45] This type of content-based collection sets an extremely dangerous precedent that, if not directly challenged, will likely continue to expand in use with other automated scanning and computer analysis tools.

From a practical standpoint, Abouts Collection is highly fraught. In 2016, the government disclosed to the FISC that it had engaged in what the court labeled "significant noncompliance," and described issues as "an institutional lack of candor on NSA's part" that represented "a very serious Fourth Amendment issue."[46] In order to remedy these compliance problems, and assure the FISC that it could operate Section 702 in a functional manner, the NSA was forced to discontinue Abouts Collection in early 2017.[47] In the more than five years since then, the government has been unable to remedy these problems, or not seen sufficient value in attempting to do so. For all the danger Abouts Collection poses, its pause has come with no indication of key intelligence needs being lost, indicating that this controversial practice offers little benefit for an unacceptably high cost.

Despite the dysfunction of Abouts Collection, Congress failed to act on the problem when it last reauthorized Section 702, instead merely requiring notification to certain Congressional committees if this system resumed.[48] Such a measure is insufficient: Abouts Collection should be prohibited.

> ***Policy Recommendation #5: We recommend the PCLOB support a legislative prohibition on Abouts Collection.***

VI. Individuals are not properly notified when Section 702 is used to investigate them, nor given fair opportunities to challenge this surveillance system in court.

The justification for the legality of Abouts Collection accepted by the FISC was not based on Congressional debate or public discourse contemporaneous to the passage of Section 702, but rather by citing to a 1978 Congressional report (H.R. Rep. 95-1283, at 73 (1978)) that targets are " the individual or entity . . . about whom or from whom information is sought." *PCLOB 702 Report*, at 36-37, (citing *In re Sealed Case*, 310 F. 3d 717, 740 (FISA Ct. Rev. 2002))

[44] *PCLOB 702 Report*, at 97.

[45] See, Memorandum Opinion and Order (FISA Ct. Apr. 26, 2017) (Collyer, J.) available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf, hereinafter, *FISC April 2017 Opinion*.

[46] *FISC April 2017 Opinion* at 4, 19 (internal quotes omitted).

[47] Charlie Savage, *New York Times*, "N.S.A. Halts Collection of Americans' Emails About Foreign Targets," April 28, 2017. https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html?smid=tw-share&_r=2.

[48] Pub. L. 115–118, title I, §103(b), Jan. 19, 2018, 132 Stat. 10.

In general, and especially in light of the evidence of Section 702 surveillance creeping into domestic law enforcement, it is important that defendants receive notice when this surveillance power was used to investigate them. This is an important check against misconduct, and crucial to individuals' Fifth Amendment due process rights, yet notice to defendants is extremely rare.[49]

One important factor likely obstructing due notice to defendants when Section 702 is used is how the government interprets the term "derive." The government is required to give notice whenever FISA 702-acquired information is used as evidence in court (which almost never occurs), or when any evidence used in court is *derived* from Section 702-acquired information. However the Department of Justice does not disclose how it interprets this term, creating the potential that an unnaturally narrow definition is being employed to skirt notice requirements.[50] This would represent a problematic return to the type of "secret law" that plagued the FISC prior to the reforms of the USA FREEDOM Act.

> ***Inquiry Recommendation #9: We recommend the PCLOB investigate and publicly report on the definition of "derive" that the Department of Justice uses to determine its notice obligation to defendants.***

Augmenting the problem of inadequate notice is the practice of parallel construction, whereby information discovered from one source — such as Section 702 — is artificially rediscovered via another method so the true source can be obfuscated. Parallel construction has been used in a systematic manner by federal law enforcement to hide intelligence surveillance as the true source of investigative leads and activities.[51]

> ***Policy Recommendation #6: We recommend the PCLOB support legislative reforms to define the term "derive" in a reasonable manner that cannot be circumvented by parallel construction as it applies to disclosure of use of FISA.***

---

[49] See, Patrick Toomey, *Just Security*, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?" December 11, 2015. https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/#_edn1.

[50] See, Patrick Toomey, *Just Security*, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?" December 11, 2015. https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/#_edn1; see also, Greg Nojeim and Mana Azarmi, Center For Democracy & Technology, "Revised USA FREEDOM Reauthorization Act of 2020 Improves FISA; More Improvements Are Needed," March 11, 2020. https://cdt.org/insights/revised-usa-freedom-reauthorization-act-of-2020-improves-fisa-more-improvements-are-needed/.

[51] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases* (January 2018). https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf; See also, John Shiffman and Kristina Cooke, *Reuters*, "Exclusive: U.S. directs agents to cover up program used to investigate Americans," August 5, 2013. https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805

CENTER FOR
DEMOCRACY
& TECHNOLOGY

***

Section 702 has a tremendous impact on the privacy and civil liberties of individuals both in the United States and across the world. With the expiration of this authority approaching, we expect Congress and the public will diligently examine potential reforms in the coming months. PCLOB has an important role to play; its research, public reporting, and policy recommendations will meaningfully influence the debate ahead. We are eager to support the PCLOB in its work on this and other important issues. Please let us know if there are any supplemental materials or other assistance we can provide.

Thank you,

Jake Laperruque

Deputy Director, Project on Security and Surveillance
The Center For Democracy & Technology