November 4, 2022

Privacy and Civil Liberties Oversight Board
2100 K Street NW, Suite 500
Washington, DC 20427

Comment of the American Civil Liberties Union Regarding the PCLOB Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act

ACLU
AMERICAN CIVIL LIBERTIES UNION

National Office
125 Broad Street
18th Floor
New York, NY 10004
aclu.org

Deborah N. Archer
President

Anthony D. Romero
Executive Director

Dear Privacy and Civil Liberties Oversight Board Members,

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with over two million members, activists, and supporters nationwide, we are pleased to provide comments regarding the Privacy and Civil Liberties Oversight Board's (PCLOB) project examining Section 702 of the Foreign Intelligence Surveillance Act (FISA).[1]

I. Introduction

The enactment of Section 702 in 2008 radically altered the rules for conducting foreign intelligence surveillance of Americans' international communications—even opening the door to forms of surveillance that were unanticipated by Congress and the public at the time. Five years later, disclosures by former NSA contractor Edward Snowden about the breadth of Section 702 surveillance generated immense controversy and debate. Those disclosures also raised a host of additional questions about what, exactly, the executive branch was doing pursuant to the statute. In 2014, PCLOB's landmark Section 702 oversight report answered several of those key questions, shedding much-needed light on the operation of this surveillance.[2] The report has continued to be indispensable for anyone seeking to understand how Section 702 surveillance works in practice—including legislators, journalists, judges, civil society organizations, and the public at large.

---

[1] PCLOB, Notice & Request for Public Comment, 87 Fed. Reg. 58393 (Sept. 26, 2022) (Notice PCLOB-2022-03).

[2] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702*, July 2, 2014 ("PCLOB Report"), https://bit.ly/3sUWLxL.

More than eight years have passed since PCLOB's report, and the ACLU welcomes the Board's interest in examining how Section 702 surveillance has expanded and evolved in the interim. Given the statute's sunset date in December 2023 and the upcoming public and legislative debate around its reauthorization, the Board's review is especially timely. As the ACLU has explained elsewhere, Section 702 surveillance is unconstitutional. While the focus of this comment is on a broader set of policy recommendations, the ACLU's legal analysis is set out more fully in our March 19, 2014 submission to PCLOB, and in legal briefs filed with the Court of Appeals for the Tenth Circuit, which we incorporate by reference here.[3]

In short, Section 702 violates the Fourth Amendment because it permits the government to conduct large-scale warrantless surveillance of Americans' international communications—communications in which Americans have a reasonable expectation of privacy. No exception to the warrant requirement authorizes these suspicionless searches of Americans' communications. The government often argues that Americans' communications are intercepted only "incidentally" in the course of targeting foreigners abroad, but the Supreme Court has never recognized an incidental-overhear exception to the warrant requirement. Likewise, even if there were a foreign-intelligence exception to the warrant requirement, it would not be broad enough to render Section 702 surveillance constitutional. The surveillance also violates the Fourth Amendment's reasonableness requirement. It lacks the core safeguards that courts require when assessing the reasonableness of electronic surveillance. Indeed, the government's procedures actually *encourage* the warrantless exploitation of Americans' communications, including through warrantless queries of Section 702 databases. These warrantless queries—and the surveillance as a whole—are unreasonable. Importantly, the government has alternatives that would allow it to collect foreign intelligence while protecting Americans' private communications, including through safeguards proposed by then-Senator Barack Obama and by the President's Review Group.[4]

Against this backdrop, the ACLU urges PCLOB to examine and report publicly on several issues pertaining to (1) Section 702 collection; (2) Section 702 querying; and (3) notice and disclosure to criminal defendants of Section 702 surveillance. At bottom, the ACLU's recommendations are designed to provide the public with basic information about the scope and purposes of collection and querying; the impact of Section 702 surveillance on Americans; and the executive branch's misuse of secrecy to thwart adversarial court review of this surveillance. In the wake of the Snowden disclosures, the intelligence agencies

[3] Submission of Jameel Jaffer, ACLU, PCLOB Public Hearing on Section 702 of the FISA Amendments Act (2014), https://bit.ly/3ftrK0N; Defendant's Opening Brief, *United States v. Muhtorov*, No. 18-1366 (Sept. 30, 2019) ("Muhtorov Opening Br."), https://bit.ly/3U0F4bQ; Defendant's Reply, *United States v. Muhtorov*, No. 18-1366 (Apr. 7, 2020) ("Muhtorov Reply"), https://bit.ly/3zCMdH8.

[4] *See* Muhtorov Opening Br. 13–51.

acknowledged that concealing the overall nature and scope of their surveillance activities undermined their legitimacy, and they vowed to expand transparency. But over the years, those efforts have fallen short—particularly with respect to transparency about the fundamentals of Section 702 surveillance, such as information about its overall scope, its impact on Americans, and its use in criminal proceedings.

Because the intelligence agencies have failed to provide this essential information to Congress and the public, the ACLU calls on PCLOB to push for an accounting of Section 702's scope and effects, and to seek declassification of as much information as possible concerning Section 702 programs. Discussing PCLOB's 2014 report, then-Chair David Medine explained: "The Board pushed hard to declassify a great deal about the Section 702 program, and this effort was largely successful: our report led to the declassification of a substantial amount of information regarding the program's operation."[5] We hope that PCLOB's current oversight project will likewise result in the declassification of key facts about the surveillance, and that it will play a similarly important role in informing Congress and the public.

II. Section 702 Collection

A. Background

Official government disclosures, including PCLOB's July 2014 report, show that the government uses Section 702 to conduct at least two types of surveillance: "Upstream" surveillance and "PRISM" (also known as "downstream") surveillance.[6]

PRISM surveillance involves the acquisition of communications content and metadata directly from U.S. Internet and social media companies like Facebook, Google, and Microsoft.[7] The government identifies the user accounts it wishes to monitor, and then orders the provider to disclose to it all communications and data to and from those accounts. Through PRISM surveillance, the U.S. government acquires both real-time and stored communications.[8]

---

[5] David Medine, *The PCLOB Report and Eight Questions About Section 702*, Just Security (July 22, 2014), https://bit.ly/3FACzZH.

[6] *See, e.g.*, PCLOB Report 33–41; Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://bit.ly/3U9EtoE (describing "downstream" surveillance).

[7] *See* PCLOB Report 33–34; [*Redacted*], No. [Redacted], 2011 WL 10945618, at *9–10 & n.24 (FISC Oct. 3, 2011); *NSA Program Prism Slides*, The Guardian, Nov. 1, 2013, https://bit.ly/3DzUPiZ (slide describes "Collection directly from the servers" of U.S. service providers).

[8] *NSA Program Prism Slides*, The Guardian, Nov. 1, 2013, https://bit.ly/3DzUPiZ.

Upstream surveillance involves the mass copying and searching of Internet communications flowing into and out of the United States. With the compelled assistance of telecommunications companies like Verizon and AT&T, the NSA taps directly into the Internet backbone inside the United States—the physical infrastructure that carries the communications of hundreds of millions of persons around the world. To conduct this surveillance, the NSA searches the metadata and content of international Internet communications transiting the links that it monitors.[9] The agency searches for key terms, called "selectors," that are associated with its many non-U.S.-person targets. Selectors used in connection with Upstream surveillance include identifiers such as email addresses or phone numbers. The Department of Justice appears to have secretly authorized the NSA to use IP addresses and certain malware signatures as selectors as well.[10] Through Upstream surveillance, the NSA has broad access to the content of communications, as it indiscriminately copies and then searches the vast quantities of personal metadata and content passing through its surveillance devices.[11] Following the mass searching of communications, those to and from selectors—as well as those that happen to be bundled with them in transit—are retained on a long-term basis for further analysis and dissemination.[12]

B. The Scale of Section 702 Collection

The U.S. government uses Upstream and PRISM to access and retain huge volumes of communications. In 2011, Section 702 surveillance resulted in the retention of more than 250 million Internet communications—a number that does not reflect the far larger quantity

---

[9] *See, e.g.*, [*Redacted*], 2011 WL 10945618, at *10, *15 (describing the government's concession to the FISC that the NSA "*will acquire* a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA" (emphasis added)); PCLOB Report 35–41; Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. Times, Apr. 28, 2017, https://nyti.ms/3Nt5jVU; Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013, https://nyti.ms/3E4fBZT.

[10] *See, e.g.*, Charlie Savage, *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border*, N.Y. Times, June 4, 2015, https://nyti.ms/3WrFmu5.

[11] *See, e.g.*, PCLOB Report 35–39, 41, 111 n.476; [*Redacted*], 2011 WL 10945618, at *10–11. Although data in transit may be encrypted, that would not prevent the NSA from copying, examining, and seeking to decrypt the intercepted data through Upstream surveillance. When the agency collects encrypted communications under Section 702, it can retain those communications indefinitely, and public disclosures indicate that the NSA has succeeded in circumventing encryption protocols in various contexts. *See, e.g.*, *Inside the NSA's War on Internet Security*, Der Spiegel, Dec. 28, 2014, https://bit.ly/3UhCxKm.

[12] *See, e.g.*, Mem. Op. & Order at 23–30, [*Redacted*] (FISC 2017), https://bit.ly/3TY3PW5; PCLOB Report 35–41.

of communications whose contents the NSA searched before discarding them.[13] Although the government has not disclosed the overall number of communications retained under Section 702 today, PCLOB observed in 2014 that "[t]he current number is significantly higher."[14] Given the rate at which the number of Section 702 targets is growing, the government today likely collects over a billion communications under Section 702 each year. In 2011, the government monitored approximately 35,000 "unique selectors";[15] by contrast, in 2021, the government targeted the communications of 232,432 individuals, groups, and organizations—most of whom are undoubtedly associated with multiple Internet accounts or "unique selectors."[16] Whenever the communications of these targets—who may be journalists, academics, or human rights advocates abroad—are sent to the United States or stored by U.S. companies, they are subject to interception and retention by communications providers under Section 702.

In surveilling hundreds of thousands of Section 702 targets, the government "incidentally" collects the communications of Americans and others in contact with those targets—including an immense volume of communications that have nothing to do with foreign intelligence. According to an analysis of a large cache of Section 702 interceptions provided to the *Washington Post*, nine out of ten account holders in the NSA's surveillance files "were not the intended surveillance targets but were caught in a net the agency had cast for somebody else."[17] Although many of the files were "described as useless by the analysts," they were nonetheless retained—including "medical records sent from one family member to another, resumes from job hunters and academic transcripts of schoolchildren. . . . Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risqué poses in shorts and bikini tops."[18] That these communications were acquired through the use of selectors demonstrates that even "targeted" surveillance under Section 702 involves the collection and retention of vast amounts of non-targets' private information.

Notably, the executive branch has refused to provide Congress with an estimate of the number of Americans' communications subject to Section 702 surveillance. In 2011,

---

[13] *See* [*Redacted*], 2011 WL 10945618, at *9–10; PCLOB Report 111 n.476.

[14] PCLOB Report 116.

[15] Glenn Greenwald, *No Place to Hide*, 111 (2014), https://bit.ly/3fr2cBx (referencing NSA documents showing that 35,000 "unique selectors" were surveilled under PRISM in 2011).

[16] Off. of the Dir. of Nat'l Intel., *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities* at 17 (Apr. 2022) ("2022 ODNI Transparency Report"), https://bit.ly/3Wt6Qj2.

[17] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014, https://wapo.st/3FHOpRJ.

[18] *Id.*

senators serving on the Senate Intelligence Committee asked the Inspectors General of the intelligence community and the NSA to provide such an estimate.[19] After years of advocacy by civil society and continued requests from Congress, DNI James Clapper eventually committed to providing the estimate.[20] However, in 2017, the Trump administration reneged on that commitment.[21] If the intelligence community had conducted its promised accounting, its statistics would have played an important role in the 2017–18 debate over the reauthorization of Section 702 by illuminating the breadth of the government's surveillance under the statute.

Recommendations to Examine and Report on the Scale of Section 702 Collection

The ACLU urges PCLOB to:

- **Report publicly on the scale of Section 702 collection today, in terms of the total volume of communications collected and the total volume scanned by the NSA or at the NSA's direction.**
- **Call on ODNI to produce and disclose a good-faith estimate of the number of U.S. person communications collected under Section 702, as ODNI previously committed to do.**
- **Report publicly on the number of electronic communication service providers receiving directives under Section 702, broken down by the type of Section 702 surveillance at issue.**
- **Assess whether ODNI's published figure of 232,432 targets under Section 702 fairly corresponds to the number of individuals (as opposed to organizations and entities) targeted for surveillance, and report publicly on the findings.**

C. Upstream Collection and "About" Surveillance

Under Section 702, the government claims the authority to gather not only communications to and from the selectors associated with its foreign intelligence targets, but

[19] Letter from Rep. John Conyers et al. to the Hon. James R. Clapper, Director, ODNI (Apr. 22, 2016), https://bit.ly/3sT2OTn.

[20] Dustin Volz, *U.S. To Disclose Estimate of Number of Americans Under Surveillance*, Reuters, Dec. 16, 2016, https://reut.rs/3fAw3Y2.

[21] Ellen Nakashima & Karoun Demirjian, *Intelligence Officials Rogers and Coats Said They Won't Discuss Specifics of Private Conversations with Trump*, Wash. Post, June 7, 2017, https://wapo.st/3Wpb4Is; Letter from Rep. Bob Goodlatte & Rep. John Conyers to the Hon. Daniel Coats, Director of National Intelligence, ODNI (June 27, 2017), https://bit.ly/3UfljgM.

also the communications of any person *about* those selectors. For many years, the government engaged in this collection—known as "about" collection—as part of Upstream surveillance. In 2014, PCLOB recognized that "[a]t least some forms of 'about' collection present novel and difficult issues regarding the balance between privacy and national security," but concluded that it was "largely unfeasible to limit 'about' collection without also eliminating a substantial portion of upstream's 'to/from' collection, which would more drastically hinder the government's counterterrorism efforts."[22]

However, in March 2017, the NSA informed the FISC that it would change how it conducts "about" collection under Section 702, following its systemic failure to comply with FISC-imposed restrictions on queries of Upstream data.[23] Specifically, NSA analysts had "used U.S.-person identifiers to query the results of Internet 'upstream' collection, even though NSA's Section 702 minimization procedures prohibited such queries."[24] The FISC ascribed the government's failure to timely disclose these violations to "an institutional 'lack of candor' on NSA's part" and emphasized that this was a "very serious" issue.[25] As a result of the resulting change in its policy, the NSA "collects" or "acquires" for the government's long-term retention and use only those Internet communications that are to or from a target, and not those that are merely "about" a target. Yet there is no indication that the NSA has stopped copying and searching the full contents of communications as they pass through its Upstream surveillance devices prior to what the government calls "acquisition" or "collection"—*i.e.*, prior to the NSA's retention, for long-term use, of communications to or from its targets.

The executive branch claims the legal authority to resume Section 702 "about" collection in the future, following FISC approval of revised targeting and minimization procedures.[26] Congress's 2018 modifications to Section 702 allow the NSA to restart the practice if it obtains FISC approval, and if Congress does not pass legislation prohibiting the practice within a one-month period. *See* 50 U.S.C. § 1881a(b)(5), (j)(1)(B); Sec. 103(b) of the FISA Amendments Reauthorization Act of 2017, 132 Stat. 10.

---

[22] PCLOB Report 145.

[23] Mem. Op. & Order at 23–30, [*Redacted*] (FISC 2017) ("2017 FISC Op."), https://bit.ly/3T3xiwA.

[24] *Id.* at 15.

[25] *Id.* at 19 (quoting hearing transcript).

[26] *See, e.g.*, Press Release, NSA, *NSA Stops Certain Section 702 "Upstream" Activities*, Apr. 28, 2017, https://bit.ly/3U9EtoE.

Recommendations to Examine and Report on "About" Surveillance

The ACLU urges PCLOB to:

- **Examine whether the NSA has complied with the prohibition on "about" surveillance; and**
- **Publicly explain how the NSA has implemented this prohibition, given its earlier claims about technical infeasibility.**

D. New Section 702 Collection Methods and Purposes

In the years since Edward Snowden's disclosures and PCLOB's July 2014 report, Section 702 collection has undoubtedly expanded and evolved, but the public lacks critical information about the extent of this expansion and evolution.

For example, in 2017, the government released a heavily redacted 2014 FISC opinion in a challenge brought by an unknown U.S. communications company.[27] The company had resisted an apparently novel form of Section 702 surveillance—potentially related to Virtual Private Network (VPN) traffic—and the FISC ultimately ordered the company to comply with the contested directive.[28] Yet the nature of challenge remains opaque.

In addition, there are indications that the FISC has been closely considering novel issues related to the government's Section 702 certifications since late 2020, including the appointment of amici to assist in that process. As ODNI's recent statistical transparency report explains, the FISC "chose to extend its review of the 2021 certification application package" and "did not issue any Section 702 orders in 2021."[29]

Other evidence suggests that the purposes of Section 702 collection have likely evolved over the past decade. For instance, President Biden's October 7 executive order, "Enhancing Safeguards for United States Signals Intelligence Activities," identifies 12 legitimate objectives for signals intelligence, including a novel reference to "understanding or assessing transnational threats that impact global security," such as "climate and other

---

[27] Mem. Op., [*Redacted*] (FISC 2014), bit.ly/3T1LhmS; Charlie Savage, *Company Lost Secret 2014 Fight Over 'Expansion' of N.S.A. Surveillance*, N.Y. Times, June 14, 2017, https://nyti.ms/3WoKEqc.

[28] Marcy Wheeler, *Did NSA Start Using Section 702 to Collect from VPNs in 2014?*, Emptywheel, July 3, 2017, https://bit.ly/3T4kaHE.

[29] 2022 ODNI Transparency Report 16.

ecological change" and "public health risks."[30] While these may be legitimate government objectives in general, the public remains in the dark about the extent to which warrantless Section 702 surveillance is being conducted for these and other purposes.

Recommendations to Examine and Report on New Collection Methods and Purposes

The ACLU urges PCLOB to:

- **Examine how Section 702 collection methods have expanded and changed since PCLOB's July 2014 report, and how that has impacted the scope and volume of collection, including the incidental collection of Americans' communications;**
- **Examine how the authorized purposes for Section 702 surveillance have expanded and changed since PCLOB's July 2014 report, and how that has impacted the scope and volume of collection, including the incidental collection of Americans' communications; and**
- **Call on the intelligence community to declassify current and historical facts about the methods and purposes of Section 702 collection that could appropriately be declassified today.**

E. Section 702 Targets

Since the enactment of Section 702 in 2008, the ACLU has expressed serious concerns about the breadth of potential targets under the statute. Section 702 allows agency analysts to collect communications of *any* non-U.S. person abroad where a "significant purpose" of the surveillance is "foreign intelligence" collection. *See* 50 U.S.C. § 1881a(a), (h)(2)(A)(v).

As Congress debates the reauthorization of Section 702 next year, it will be necessary for both Congress and the public to understand the implications of various proposals to narrow the scope of this surveillance, including proposals to limit surveillance to foreign powers and individuals reasonably suspected by agency analysts of being "agents of a foreign power." *See* 50 U.S.C. § 1801(b). At present, however, there is no public data about the categories of individuals who are in fact targeted under the law. This information would help advance discussions about practical ways to narrow Section 702 collection; provide examples of people targeted for this surveillance who are not agents of a foreign power (*e.g.*, journalists, dissidents, academics, lawyers, technology-sector employees); and could shed light on the categories of U.S. persons incidentally swept up in Section 702 collection.

[30] Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022), https://bit.ly/3WsZSua.

Recommendation to Examine and Report on Section 702 Targets

The ACLU urges PCLOB to review a sample of Section 702 targets to provide more information to Congress and the public about the categories of individuals targeted for surveillance and whether they would qualify as "agents of a foreign power" under 50 U.S.C. § 1801(b).

III. Section 702 Queries

The U.S. government's querying of Section 702 information should be a central element of PCLOB's review. Warrantless Section 702 queries of U.S. person information are a substantial intrusion on Americans' private communications, and are directly at odds with the government's insistence that Section 702 surveillance is "targeted" at foreigners abroad. The scale of these intrusions is vast, with FBI agents alone conducting millions of U.S. person queries each year.[31] The ACLU has written extensively about Section 702 queries elsewhere, and we understand other organizations are addressing these important issues in depth, so we address only three essential points for the purposes of this submission.[32]

First, and most importantly, PCLOB should recommend a warrant requirement for U.S. person queries of Section 702 databases, given that they are deliberate intrusions on Americans' constitutionally protected communications. Second, PCLOB should provide critical information about the overall scope and purpose of U.S. person queries, which would enable greater public oversight. Third, PCLOB should provide information about the government's querying practices in criminal investigations and prosecutions. This information would facilitate meaningful adversarial review in criminal proceedings, which the government has largely thwarted for years.

A. Protections for U.S. Person Queries

Warrantless querying of Americans' private communications should be subject to far stronger safeguards—including, for example, a requirement that agents and analysts obtain a warrant before reviewing the contents of an American's communication. These communications are indisputably protected by the Fourth Amendment, and no recognized

---

[31] 2022 ODNI Transparency Report 20.

[32] Muhtorov Opening Br. 13–47; Muhtorov Reply 1–12; Amicus Brief of the ACLU & Electronic Frontier Found. at 9, *United States v. Hasbajrami*, 945 F.3d 641 (Oct. 23, 2017) (No. 15-2684), https://bit.ly/3U9Q4nG; Jennifer Stisa Granick & Ashley Gorski, *How to Address Newly Revealed Abuses of Section 702 Surveillance*, Just Security (Oct. 18, 2019), http://bit.ly/3Wnx32B; Submission of Jameel Jaffer, ACLU, PCLOB Public Hearing on Section 702 of the FISA Amendments Act (Mar. 19, 2014), http://bit.ly/3h98dTE.

exception to the warrant requirement applies.[33] Yet, at the FBI, CIA, and National Counterterrorism Center (NCTC), agents and analysts around the country can generally search for and read through U.S. persons' private communications without needing to obtain even a supervisor's approval.[34] (The NSA, which requires Office of General Counsel approval, is an outlier.[35]) The querying procedures have largely been written to give agents seamless, unencumbered access to communications that ordinarily would be shielded by a warrant.

Federal courts are divided over how to analyze the lawfulness of querying under the Fourth Amendment. But both approaches support requiring individualized court approval for queries, given that the government does not obtain a warrant prior to collecting these protected communications.[36] Moreover, regardless of what the Fourth Amendment itself requires, stronger safeguards are necessary to protect Americans' well-established privacy interests in the content of their phone calls, texts, emails, and myriad online communications.

The FISC has analyzed the government's querying procedures as part of the overall Fourth Amendment "reasonableness" of the Section 702 program. This approach involves examining Section 702 surveillance procedures and practices under "the totality of the circumstances"—from collection, to minimization, to querying—to weigh the degree of intrusion on Americans' privacy alongside the government's interests in conducting these searches.[37] Applying this framework, the FISC held in 2018 that the FBI's Section 702 surveillance violated the Fourth Amendment.[38] The FISC's decision was based on the FBI's "maximal" use of backdoor searches to investigate Americans, and the absence of even

---

[33] *See* Muhtorov Opening Br. 27–36; Muhtorov Reply 12–24; Orin Kerr, *The Surprisingly Weak Reasoning of Mohamud*, Lawfare (Dec. 23, 2016), https://bit.ly/2PfkPWx ("There is no 'targeting' doctrine in Fourth Amendment law."); Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in Mohamud*, Just Security (Dec. 8, 2016), http://bit.ly/3zFH7Kk (explaining that the "incidental overhear" doctrine is not an exception to the warrant requirement); *cf.* PCLOB Report 90 n.411 (observing that "it is not necessarily clear that the Section 702 program would fall within the *scope* of the foreign intelligence exception" recognized by courts).

[34] *See* FBI Section 702 Querying Procedures (Sept. 17, 2019), https://bit.ly/3WqpOXA; CIA, Section 702 Querying Procedures (Sept. 17, 2019), https://bit.ly/3U3c6bw; NCTC Section 702 Querying Procedures (Oct. 19, 2020), https://bit.ly/3fuzHCP.

[35] NSA Section 702 Querying Procedures (Oct. 19, 2019), https://bit.ly/3FMmCjf.

[36] *See generally* Muhtorov Reply 1–12.

[37] *See Samson v. California*, 547 U.S. 843, 848 (2006); FISC, Mem. Op. & Order 33–34 (Nov. 18, 2020) ("2020 FISC Op."), https://bit.ly/3hbssQD.

[38] [*Redacted*], 402 F. Supp. 3d 45, 73–88 (FISC 2018). The FISC has found Section 702 surveillance unreasonable on at least one other occasion. [*Redacted*], 2011 WL 10945618, at *23–28 (FISC Oct. 3, 2011).

rudimentary safeguards.[39] Although the FBI subsequently made extremely modest changes to its procedures to obtain FISC approval, the procedures used by the FBI and other agencies continue to enable widespread warrantless searches through Americans' protected communications.

In contrast to the FISC, the Second Circuit has held that the government's querying of an American's communications under Section 702 is a "separate Fourth Amendment event" that must independently satisfy constitutional requirements. *United States v. Hasbajrami*, 945 F.3d 641, 670 (2d Cir. 2019). Under this approach, the lawfulness of a given query is assessed separately from the government's initial collection of the communications at issue, much as cell phone searches can require a warrant even when police officers have warrantlessly seized a phone incident to arrest. *See id.* (citing *Riley v. California*, 573 U.S. 373, 400–01 (2014)).[40] The Second Circuit's decision places a critical focus on the constitutional status of querying, especially in light of advancing surveillance technologies. But the court did not decide the lawfulness of the government's Section 702 queries in *Hasbajrami*, leaving further factual development to the district court. *Id.* at 669–73. As explained below, however, adequate factual development has proven a dire challenge across Section 702 criminal cases, with the government repeatedly using secrecy to thwart adversarial court review of its Section 702 queries. *See* Section IV, *infra*.[41]

Since PCLOB's last review of Section 702 in 2014, the arguments supporting a warrant requirement for U.S. person queries have only grown stronger. Whether evaluated under the totality of the circumstances or as independent Fourth Amendment events,

---

[39] *See id.* at 80, 87–88 ("The government is not at liberty to do whatever it wishes with those U.S.-person communications.").

[40] Similarly, when agents are warrantlessly targeting a foreign embassy on U.S. soil under FISA and inadvertently intercept the communications of an American, they must stop and obtain an order from the FISC to retain and use those protected communications. 50 U.S.C. § 1801(h)(4). The special rules for embassy wiretaps exist because Congress recognized in FISA that it would be unlawful for the government to collect, retain, and use Americans' communications under the guise of targeting foreign powers. *See* H.R. Rep. No. 95-1720, at 24–26 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048.

[41] Significantly, in practice, the Second Circuit's framework may invite the government to raise an extra secrecy obstacle for defendants seeking to challenge the querying of their communications. That is because the government has argued that a defendant must establish the evidence at trial was "obtained or derived from" *the specific Section 702 queries in dispute*. Although defendants who receive Section 702 notices are invariably subject to warrantless queries—because FBI agents query Section 702 databases whenever they open a new national security assessment or investigation—executive branch secrecy has made it exceedingly difficult for a defendant to show that trial evidence was obtained or derived from a particular query or queries. In contrast, under the FISC's approach, a defendant who receives a Section 702 notice may challenge the reasonableness of the querying procedures as part of the "totality of the circumstances" of the Section 702 surveillance to which he was subject.

Section 702 queries raise three central concerns: the immense scale of these searches, their intrusiveness, and glaring weaknesses in the agencies' existing rules. All of these concerns are especially pronounced with respect to the FBI.

First, recent disclosures confirm the immense scale of the agencies' backdoor searches and their impact on Americans, not just foreigners. According to ODNI's most recent transparency report, FBI agents conducted up to 3.4 million warrantless U.S. person queries in a single year.[42] The agency sought to downplay that number when it was disclosed, but the FBI's policy has long been to encourage "maximal querying of Section 702 information."[43] The government has even likened the FBI's querying of its Section 702 databases to "[the] FBI's Google."[44] Meanwhile, CIA, NSA, and NCTC analysts reported using 8,790 U.S. person query terms over a similar period—a much smaller number on its face, but one that masks the total number of communications returned by these U.S. person queries.[45] As the scale of Section 702 collection has grown, sweeping up more and more targets and communications, the number of U.S. person communications susceptible to these queries has almost certainly expanded as well.

Second, as the FISC has underscored, the privacy interests implicated by Section 702 queries are "substantial"—precisely because the government acquires the "full contents" of vast numbers of communications under Section 702, and queries allow agents and analysts to sift through that trove of information for the communications of particular Americans.[46] The FBI's queries are especially intrusive because it can use them to probe for evidence of criminal activity, repurposing Section 702 into a tool for all manner of domestic investigations.[47] Although Section 702 is nominally targeted at more than 232,000 foreigners, FBI agents routinely use queries to focus on Americans instead—including at the earliest "assessment" stages of unrelated investigations.[48] Without any showing of suspicion, an FBI agent can type in an American's name, email address, or phone number, and pull up whatever communications the FBI's Section 702 collection has vacuumed into its databases over the past five years. Queries are a free pass for accessing protected communications that, otherwise, would be off-limits.

Third, chronic weaknesses in the agencies' rules have undermined the protections for Americans still further. The standards are extremely permissive and the searches—which can include so-called "batch queries" using hundreds of U.S. person querying terms at a time—are extremely broad. To search for an American's communications in the pool of

---

[42] 2022 ODNI Transparency Report 21.

[43] 402 F. Supp. 3d, at 78.

[44] Tr. at 34:15, *In re* [*Redacted*], No. [Redacted] (FISC Oct. 20, 2015), https://bit.ly/2Nu4cou.

[45] 2022 ODNI Transparency Report 18.

[46] [*Redacted*], 402 F. Supp. 3d at 75, 87–88.

[47] *See id*. at 75, 87.

[48] *See* 2022 ODNI Transparency Report 17; [*Redacted*], 402 F. Supp. 3d at 80.

Section 702 data, agents or analysts must simply have a "reasonable basis to believe" that the query is "likely" to return foreign intelligence information—a vague and elastic standard.[49] In the case of the FBI, agents may also conduct U.S. person queries whenever they have a reasonable basis to believe that the query is "likely" to return evidence of a crime, significantly expanding the universe of queries permitted by the procedures. While the NSA requires Office of General Counsel approval for U.S. person query terms, at the FBI, CIA, and NCTC, no supervisory approval whatsoever is required for most queries. At the FBI, an agency attorney must approve "batch queries" involving 100 or more query terms, but no such approval is required for "batch queries" using 99 or fewer terms.[50]

Predictably, the push for "maximal" querying, combined with lax controls, has led to large numbers of unauthorized backdoor searches.[51] For example, across thousands of queries, FBI agents have sought information about Americans that was not reasonably likely to result in foreign intelligence information or evidence of a crime, including searches for information concerning relatives, potential witnesses, and potential informants.[52]

Although Congress has recognized that certain U.S. person queries require a court order, the existing requirement is plainly insufficient to protect Americans' privacy. Congress has mandated court approval of queries in one vanishingly narrow scenario: where the FBI seeks to review the results of a U.S. person query in a predicated criminal investigation unrelated to national security. *See* 50 U.S.C. § 1881a(f)(2). But the FBI has apparently never sought such an order from the FISC, and it has violated that prohibition on numerous occasions.[53] Even if the FBI had a record of compliance, this provision would be patently inadequate, as a significant proportion of U.S. person queries occur at the earliest "assessment" stage of investigations, and therefore evade the court-order requirement. The provision is also illogical: it allows agents to conduct intrusive U.S. person queries at the assessment stage, when agents need not have *any* facts supporting criminal suspicion; but it requires a court order once agents have gathered enough evidence to open a predicated investigation, including evidence obtained through any Section 702 queries they *already* conducted at the assessment stage.

The court-order requirement should be expanded to provide consistent protection to Americans whose communications were collected under Section 702 without a warrant.

---

[49] [*Redacted*], 402 F. Supp. 3d at 76.

[50] DOJ & ODNI, *Semiannual Assessment of Compliance with Procedures & Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 57–58 (Sept. 2021), https://bit.ly/3Dxdb4b.

[51] *See* Elizabeth Goitein, *The FISA Court's Section 702 Opinions, Part II: Improper Queries and Echoes of "Bulk Collection,"* Just Security (Oct. 16, 2019), http://bit.ly/3FHpCwZ.

[52] [*Redacted*], 402 F. Supp. 3d at 76–78, 87 (finding that "the FBI has conducted tens of thousands of unjustified queries of Section 702 data"); *see also* 2020 FISC Op. 38–51.

[53] *See, e.g.*, 2020 FISC Op. 42–44; 2022 ODNI Transparency Report 22.

Agencies that conduct thousands or millions of U.S. person queries each year may claim that a court-order requirement would be too onerous and that the magnitude of their querying is already far too great to require individualized court approval. But the agencies' rush to encourage "maximal" querying and their eagerness to warrantlessly sift through Americans' communications is not controlling, nor is the general assertion that it is more expedient to forgo court review. Intelligence and law enforcement agencies will invariably prefer their own procedures to a judicial process. *See Riley*, 573 U.S. at 398 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols."). If anything, the scale of today's U.S. person queries is further evidence that Section 702 surveillance does not simply represent an "incidental" or "de minimis" intrusion on Americans' privacy interests, as the government has long claimed. Rather, U.S. person queries have become a fixture across all the agencies that participate in Section 702 surveillance, and they should be regulated as deliberate searches of Americans' communications. After more than a decade of experimentation and expansion, largely in secret, it is time for a fundamental reevaluation of these practices.

A warrant requirement will not put Section 702 queries off-limits for intelligence and law enforcement agencies. It will simply require that the agencies justify those intrusions using a familiar probable-cause standard, or point to another well-established exception to the warrant requirement—like exigent circumstances—where they seek to bypass court approval.

Recommendation to Strengthen Protections for U.S. Person Queries

The ACLU urges PCLOB to call on Congress to expand the court order requirement to encompass all Section 702 queries of U.S. persons' communications, similar to the longstanding requirement in 50 U.S.C. § 1801(h)(4).

B. Scope and Purpose of U.S. Person Queries

As PCLOB did in its 2014 report, the Board should also provide the public and Congress with important information about the agencies' querying practices today and their impact on U.S. persons. This information should be both quantitative, where possible, and qualitative. For example, PCLOB should push for an estimate of the number of U.S. person communications returned in response to queries. These kinds of statistics would provide a fuller picture of the intrusion on U.S. persons' private communications, and they would provide a common baseline for comparison across all of the relevant agencies, which is currently lacking.

Recommendation to Report on the Scope and Purpose of U.S. Person Queries

The ACLU urges PCLOB to examine how the FBI, NSA, CIA, and NCTC are using Section 702 queries today, including the quantity of U.S. person communications returned, the kinds of information sought, and the justifications for these queries.

- **Scope: How many communications are returned by each agency's U.S. person queries in a year?**
- **Purpose: What are some of the most common uses of U.S. person queries, including batch queries?**
- **Justification: Within each agency, does the querying standard function as a significant protection for U.S. persons against fishing expeditions or not? Are the written justifications supporting the agencies' queries specific and credible, or boilerplate and speculative?**
- **Batch Querying Procedures: What requirements apply to batch queries and how do agents document their justification for each of the individual U.S. person terms used?**
- **Illegal Querying: Why has the FBI repeatedly failed to seek a court order to access the results of certain U.S. person queries in predicated criminal investigations, as Congress required in 50 U.S.C. § 1881a(f)(2)?**
- **Cyber Querying: The FBI has reported that it conducted approximately 1.9 million queries related to potential victims of attempts to compromise U.S. critical infrastructure by foreign cyber actors. What was the specific purpose of these millions of queries, how was the use of each querying term justified, and how was the resulting information used?**

C. Use of U.S. Person Queries in Criminal Investigations and Prosecutions

One of the most glaring gaps in the public's understanding of Section 702 is the government's use of U.S. person queries in criminal investigations and prosecutions. The Board should provide information critical to understanding the Section 702 "lifecycle" in criminal investigations and prosecutions, including those that have a nexus to national security and those that do not.

Apart from the Board's prior report in 2014, neither the public nor criminal defendants have basic information about how the government relies on U.S. person queries in criminal investigations; how it tracks and documents its use of Section 702 throughout the investigative process; and how it determines whether to provide defendants with notice and discovery so that they have a fair opportunity to seek court review of this warrantless surveillance. In a number of cases, the government has thwarted efforts to obtain court review of U.S. person queries by making secret, one-sided claims that its evidence at trial

was not "derived from" its backdoor searches of defendants' communications.[54] Defendants have been unable to fully or fairly contest these claims because the government has insisted that all of the underlying investigative information is classified and has refused to disclose the relevant facts even to security-cleared counsel. Several courts appear to have accepted vague or conclusory assertions advanced in ex parte filings.[55] This breakdown in the adversarial process has made it virtually impossible for defendants to challenge U.S. person queries and has insulated these searches from review in the public courts.

More generally, the public lacks basic data about how widely U.S. person queries are used in criminal investigations unrelated to national security. The FISC has provided some examples—including investigations involving public corruption, bribery, healthcare fraud, violent gangs, and transnational crime—but its description was anecdotal and incomplete.[56] This information is essential because the use of Section 702 queries in criminal investigations unrelated to national security is a profound departure from the government's justification for this warrantless surveillance, which is predicated on the targeting of foreigners abroad for foreign intelligence purposes.

Recommendation to Report on the Use of U.S. Person Queries in Criminal Investigations and Prosecutions

The ACLU urges PCLOB to examine and report on the Section 702 "lifecycle" in criminal investigations and prosecutions, including by:

- **Providing a detailed narrative account of how U.S. person queries are typically used and tracked in criminal investigations from the earliest investigative stages to the conclusion of any prosecution. This review should include scenarios where the FBI initially receives the results of U.S. person queries as "tips" or "leads" from intelligence agencies.**[57]
- **Reporting on whether the FBI continues to conduct warrantless queries "whenever" it opens a national security assessment or investigation.**
- **Examining the government's use of U.S. person queries in a sample of specific investigations, including (a) cases where defendants received notice of Section 702**

[54] *See, e.g., Muhtorov*, 20 F.4th 558, 673–80 (Lucero, J., dissenting).

[55] *See id.*; *United States v. Mohamud*, 843 F.3d 420, 438 (9th Cir. 2016) (cursorily stating that terrorism case involving Section 702 surveillance did not involve querying, notwithstanding FBI querying practices).

[56] 2020 FISC Op. at 42.

[57] For example, in the context of StellarWind surveillance, the Department of Justice Inspector General reported that the FBI treated information passed from the NSA as "tips" and "leads" that FBI agents could use without later disclosing the source of the information. DOJ Office of the Inspector General, *A Review of the Department of Justice's Involvement with the President's Surveillance Program* 63–70, 78–88, 347–59 (July 2009) ("StellarWind IG Report"), https://bit.ly/2PkLV35.

surveillance but the government later insisted that its evidence was not "derived from" any queries of the defendant's communications; and (b) cases where defendants did *not* receive notice of Section 702 surveillance but the FBI maintains that its queries made a valuable contribution to its investigation.

- **Providing a more complete accounting of the quantity and types of criminal investigations unrelated to national security—including assessments—where the FBI has used U.S. person queries.**
- **Reviewing a representative sample of the justifications that FBI agents provided to support their belief that a U.S. person query was "reasonably likely" to return evidence of a crime. In particular, the Board should assess whether those justifications are specific and credible or are boilerplate and speculative.**

IV. Section 702 Notice and Disclosure to Criminal Defendants

In enacting Section 702, Congress required that DOJ provide notice to a person when it intends to use "any information obtained or derived from an electronic surveillance of that aggrieved person" in the course of an official proceeding. 50 U.S.C. §§ 1806(c), 1881e(a)(1). Because Section 702 surveillance is conducted in secret, notice is vitally important to criminal defendants and their ability to seek suppression of evidence obtained through unreasonable searches and seizures. FISA's notice requirement also performs the important function of allowing the public to learn about government surveillance practices and ensuring that this surveillance is reviewed not only in secret by the FISC, but also in adversarial court proceedings. Indeed, because the government has repeatedly blocked civil challenges to Section 702 surveillance, criminal cases have been the *sole* avenue by which our public courts are able to review a surveillance program affecting millions.

Unfortunately, DOJ has a long record of failing to give notice in criminal cases, thereby concealing the use of Section 702 surveillance and insulating it from review. Although DOJ gave a handful of Section 702 notices to criminal defendants beginning in 2013—following misrepresentations to the Supreme Court in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013)—those notices seem to have disappeared altogether in recent years.

Compounding this problem, even when a criminal defendant has received notice of Section 702 surveillance, DOJ blocks defense counsel from obtaining *any* discovery related to the surveillance. As in every other FISA case over the past 40 years, DOJ has repeatedly filed boilerplate claims asserting that every shred of information related to the surveillance is secret—notwithstanding the government's many public disclosures related to Section 702 surveillance in other contexts. These blanket claims are not credible, and they deprive defendants of information "necessary" for courts to accurately and fairly determine the lawfulness of the challenged surveillance. 50 U.S.C. § 1806(f).

PCLOB has an essential role to play in protecting the rights of individuals facing criminal proceedings and in ensuring the public courts' ability to rigorously review Section 702. PCLOB can advance these civil liberties and privacy interests by pushing for greater transparency and urging DOJ to change its practices with respect to both notice and disclosure.

A. Lack of Notice

From 2008 to 2013, DOJ did not give a single criminal defendant notice of Section 702 surveillance. In 2012, when the Supreme Court heard argument in *Clapper v. Amnesty International USA*, the Solicitor General assured the Court that criminal defendants would receive notice.[58] Unbeknownst to the Solicitor General, however, DOJ had an undisclosed policy that in practice concealed Section 702 surveillance from criminal defendants (and consequently, from the public at large). Following this revelation, DOJ revised its internal notice policy and undertook a review of prosecutions to identify those where notice should have been provided.[59] Between October 2013 and the end of 2014, a total of six defendants received belated notice of Section 702 surveillance.[60] Between 2014 and 2018, DOJ provided notice to five additional individuals.[61] Since mid-2018, DOJ does not appear to have provided any Section 702 notices whatsoever.

Given the FBI's routine reliance on Section 702 in criminal and foreign intelligence investigations, and its "maximal" querying of Section 702 databases, the vanishingly small number of Section 702 notices is striking—and implausible. FBI agents query Section 702 databases in virtually every national security investigation. Since 9/11, DOJ has prosecuted 979 individuals for terrorism-related charges, and PCLOB's July 2014 report stated that Section 702 surveillance contributed to "well over 100 arrests on terrorism-related offenses."[62] While not every Section 702 query will produce evidence that contributes to the

---

[58] Tr. of Oral Argument at 27–55, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013) (No. 11-1025).

[59] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, https://nyti.ms/3Wwl1Uk.

[60] *See United States v. Zazi*, No. 1:09-cr-00663 (E.D.N.Y. Sept. 23, 2009); *United States v. Mohamud*, No. 3:10-cr-00475 (D. Or. Nov. 29, 2010); *United States v. Mihalik*, No. 2:11-cr-00833 (C.D. Cal. Aug. 30, 2011); *United States v. Hasbajrami*, No. 1:11-cr-00623 (E.D.N.Y. Sept. 8, 2011); *United States v. Muhtorov*, No. 1:12-cr-00033 (D. Colo. Jan. 23, 2012); *United States v. Khan*, No. 3:12-cr-00659 (D. Or. Dec. 28, 2012).

[61] *See United States v. Mohammad*, No. 3:15-cr-00358 (N.D. Ohio Sept. 30, 2015); *United States v. Al-Jayab*, No. 1:16-cr-00181 (N.D. Ill. Mar. 17, 2016); *United States v. Kandic*, No. 1:17-cr-00449 (E.D.N.Y. Aug. 17, 2017).

[62] *Trial and Terror*, The Intercept (updated Aug. 17, 2022), https://bit.ly/3FFgs4j; PCLOB Report 110.

government's case at trial, the available data strongly suggests that DOJ is once again improperly withholding notice in criminal cases.

The disappearance of Section 702 notices may be the product of several developments within the executive branch. But all of them relate to how DOJ and the FBI assess a key question: whether the trial evidence in a case is "derived from" Section 702 surveillance. Section 1806(c) requires DOJ to provide notice to defendants when the government uses information "obtained or derived from" Section 702 surveillance in a proceeding. When DOJ improperly withheld notice from 2008 to 2013, it was because it had secretly adopted an interpretation of "derived from" that eliminated its notice obligation.[63] DOJ issued new internal guidance on the meaning of "derived from" in 2016, but it has refused to release that memo publicly.[64] In the years since, DOJ may have revised its notice policy once again behind closed doors, adopting an interpretation so narrow that it produces no Section 702 notices at all. Alternatively, DOJ and the FBI may have started structuring investigations in a way designed to insulate Section 702 surveillance from the "derived from" requirement—for example, by treating Section 702 information as "tip" or "lead" information and/or by "scrubbing" it from subsequent warrant applications.[65] Finally, the FBI may not be closely tracking agents' use of Section 702 information in investigations, making it difficult for officials to trace the role Section 702 information played once a case reaches the prosecution stage.

Because DOJ refuses to publicly disclose its notice policy and governing memo on the meaning of "derived" evidence, criminal defendants and the public at large can only guess at how prosecutors are interpreting and implementing Section 702's notice requirement.

The Classified Information Procedures Act (CIPA) may also play a role in concealing this surveillance. 18 U.S.C. app. III. Even if a defendant knows or suspects he was subject to Section 702 surveillance in absence of affirmative notice by the government, and requests information regarding that surveillance in discovery, the government may rely

---

[63] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, https://nyti.ms/3Wwl1Uk (describing how DOJ's National Security Division had "long used a narrow understanding of what 'derived from' means to avoid providing notice).

[64] In November 2016, DOJ distributed a 32-page memorandum to all prosecutors entitled, "Determining Whether Evidence is 'Derived From' Surveillance under Title III or FISA." It has refused to disclose that controlling guidance publicly. *See ACLU of Nor. Cal. v. U.S. Dep't of Just.*, No. 17-cv-03571, 2019 WL 2619664 (Apr. 15, 2019).

[65] "Scrubbing" is one of the tactics that DOJ used to avoid disclosure of StellarWind surveillance in criminal cases, as described in the groundbreaking Inspector General report on that surveillance program. StellarWind IG Report 78–88.

on CIPA to improperly withhold Section 702 information from the defense.[66] In particular, the government may use ex parte filings under CIPA to argue that although it collected or queried a defendant's communications under Section 702, its evidence was not "derived from" that surveillance. *See* 18 U.S.C. app. 3 § 4. On the basis of those secret, one-sided claims minimizing the role of Section 702, the court may deny the defendant's request for discovery, leaving the defendant in the dark as to the role Section 702 surveillance played in his case—and giving him no chance to challenge or cross-examine the government's version of events. This is precisely how the government concealed warrantless StellarWind surveillance in criminal cases.[67] Similarly, this use of CIPA prevents criminal defendants from challenging both the surveillance and the government's unilateral (and often self-serving) determination that its evidence was not derived from Section 702 collection.

Obscuring the use of Section 702 surveillance in these ways, and then withholding notice as a result, denies criminal defendants due process and does not comport with FISA's requirements. The Supreme Court's test for what count as "derived evidence"—or "fruit of the poisonous tree"—is a flexible and expansive one, precisely because investigations unfold in many different ways. Evidence is considered derivative even when it was "acquired as an indirect result" of an earlier search, up to the point at which the connection to that surveillance becomes "so attenuated as to dissipate the taint."[68] If the government has relied on Section 702 surveillance—even indirectly—in gathering its evidence, the defendant is entitled to notice of that surveillance. If need be, the parties can then litigate, in an *adversarial* proceeding, the factual and legal question of what specific evidence was derived from the electronic surveillance, consistent with the Supreme Court's decision in *Alderman v. United States*, 394 U.S. 165, 182–83, 184 (1969). But the government cannot avoid giving notice by putting artificial distance between its surveillance and its evidence, or simply by reobtaining identical information using techniques like parallel construction.

At a minimum, criminal defendants and the public deserve to know what standards the DOJ is applying in deciding whether to provide Section 702 notice. Without transparency about DOJ policy, there can be no evaluation from anybody outside of DOJ as to whether its interpretation of the law is constitutional.

---

[66] *Cf.* Muhtorov Opening Br. 81–86; ACLU Amicus Br. 7–8, *United States v. Song*, No. 21-10095, 2021 WL 4434714 (9th Cir. July 28, 2021).

[67] StellarWind IG Report 333–35, 347–59.

[68] *Murray v. United States*, 487 U.S. 533, 537 (1988) (quoting *Nardone v. United States*, 308 U. S. 338, 341 (1939)).

Recommendations to Strengthen Section 702 Notice

The ACLU urges PCLOB to:

- **Examine DOJ's notice policies and practices to identify why so few Section 702 notices have been provided in criminal cases, and publicly report on how DOJ determines whether to provide notice of Section 702 surveillance.**
- **Recommend that DOJ provide Section 702 notice in any case where there is a colorable argument that its evidence was "derived from" Section 702 surveillance, so the "fruit of the poisonous tree" issue can be resolved in a fair, adversarial litigation suppression proceeding before the court.**
- **Ensure that the FBI and DOJ are reliably tracking the use of Section 702 surveillance in investigations, so the role of that information can be accurately traced for purposes of providing notice.**
- **Recommend that DOJ provide an annual accounting of how many Section 702 notices it has given and in which specific cases, as part of its regular transparency reporting.**

B. Inadequate Disclosure of Section 702 Information

Even in the rare cases where criminal defendants receive a Section 702 notice, the government uses blanket claims of secrecy to deprive the defense of any further information about the surveillance. The notice itself is a short, boilerplate filing that provides no specific information about the surveillance or querying at issue. DOJ has consistently refused to provide defendants or their security-cleared lawyers with any discovery about the surveillance beyond the initial notice. Defendants' inability to obtain discovery, even with special safeguards, prevents them from presenting fully informed challenges to Section 702 surveillance. The absence of a fair, adversarial process undermines courts' ability to accurately determine the lawfulness of this complex surveillance.

For example, in *United States v. Muhtorov*, the government refused the defense's requests for basic information such as which communications the FBI obtained under Section 702; whether they were phone calls, emails, Skype video calls, or web pages the defendant visited; and how his communications were used in the government's investigation.[69] It refused to provide the defense with its surveillance applications, the supporting affidavits, the FISC orders that granted those applications, or the targeting and minimization procedures that applied at the time the defendant's communications were

[69] Muhtorov Opening Br. 26.

collected.[70] Nor did it tell Mr. Muhtorov what search terms or other methods agents used to locate his communications in the government's Section 702 databases.[71]

Deprived of relevant information, Mr. Muhtorov, and other defendants like him, have been unable to make the full range of legal, factual, and technological arguments that a court must analyze in reviewing the complexities of Section 702 surveillance. Full and fair litigation of Fourth Amendment cases involving novel surveillance methods often turn on precisely how a search is conducted. In absence of such information, courts have been unable to fairly and accurately review of the legality of the warrantless surveillance and querying used in the handful cases where DOJ has provided notice of Section 702 surveillance. As the Second Circuit has put it, courts cannot evaluate the Fourth Amendment issues inherent in Section 702 surveillance without knowing, at minimum, "what databases were queried by whom, for what reasons, what (if any) information was uncovered by such queries, or what (if any) use was made of any information uncovered." *United States v. Hasbajrami*, 945 F.3d 641, 672–73 (2d Cir. 2019); *see Muhtorov*, 20 F.4th 558, 673–80 (Lucero, J., dissenting) (stating that the court's review was "almost immediately stymied by the [classified] record's silence on multiple facts that are crucial to the derivative evidence inquiry").

DOJ has justified its refusal to provide discovery by submitting a boilerplate declaration from the Attorney General asserting that disclosure of *any* Section 702 information would endanger national security.[72] The Attorney General appears to have filed such a declaration in every FISA case over the past forty years. But it is increasingly clear that, even if some information is genuinely sensitive, the claimed need for blanket secrecy is not credible. The government has made numerous public disclosures of Section 702 materials without harm to national security,[73] yet it refuses to give even security-cleared counsel access to comparable information about the surveillance used in defendants' individual cases.[74]

DOJ's failure to disclose key information regarding its surveillance and querying violates FISA, which requires disclosure of materials to counsel when disclosure is

---

[70] *Id.*

[71] *Id.*

[72] *See* 50 U.S.C. § 1806(f)*;* Decl. of Att'y Gen., *United States v. Muhtorov*, No. 12-cr-00033-JLK (May 9, 2014) (ECF No. 559-1).

[73] *See, e.g.*, NSA Section 702 Minimization Procedures (2011), https://bit.ly/2KL3Bzp; FBI Section 702 Targeting Procedures (2015), https://bit.ly/2LOvuJS; Certification of DNI & Attorney General Pursuant to FISA Subsection 702(g) (July 2015), https://bit.ly/2KmCMBx; Affidavit of Admiral Michael Rogers, Director, NSA (July 2015), https://bit.ly/3387jLR.

[74] *See* Muhtorov Opening Br. 66–68.

"necessary" for an "accurate determination of the legality" of the surveillance. 50 U.S.C. §§ 1806(f), 1825(g), 1881e. In enacting FISA, Congress sought to "strik[e] a reasonable balance" between "mandatory disclosure" and "an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself."[75] The congressional reports also describe factors that Congress expected courts to consider when assessing whether disclosure is "necessary": the "complex[ity]" of the legal questions at issue; "indications of possible misrepresentations of fact"; and the "volume, scope, and complexity" of the surveillance materials.[76] Disclosure is "necessary" when these factors are present.[77]

If there were any uncertainty as to whether FISA requires disclosure, the statute must be construed consistent with the Fourth and Fifth Amendments, which require disclosure. Under the Fifth Amendment's Due Process Clause, defendants must have a meaningful opportunity to pursue suppression of evidence obtained in violation of the Fourth Amendment's guarantees.[78] Against this constitutional backdrop, FISA must be construed to require disclosure of Section 702 information under appropriate security measures whenever such disclosure is "necessary" for "an accurate determination of the legality" of the surveillance, 50 U.S.C. §§ 1806(f), 1825(g), 1881e. As courts have repeatedly recognized—especially in the suppression context—adversarial litigation is essential to fair and accurate judicial decision-making.[79]

Reliance on one-sided submissions from the government in complex surveillance litigation carries an unacceptably high risk of error.[80] Declassified FISC opinions underscore the complexity of the government's Section 702 and FISA surveillance—and the inherent limitations of ex parte proceedings in cases involving novel surveillance techniques.[81] These opinions show that the government has made a series of incomplete or inaccurate representations in its surveillance applications, and that it has repeatedly failed to comply with restrictions imposed by the FISC.[82] These widespread problems have revealed a persistent blind spot in the ex parte process by which FISA applications are reviewed:

---

[75] S. Rep. No. 701, 95th Cong., 2d Sess. at 64, *reprinted in* 1978 U.S.C.C.A.N. 4033.

[76] *Id.*

[77] *See, e.g.*, *United States v. Belfield*, 692 F.2d 141, 147–48 (D.C. Cir. 1982).

[78] *See Wong Sun v. United States*, 371 U.S. 471, 487 (1963).

[79] *See Alderman*, 394 U.S. at 182–83, 184; *Franks v. Delaware*, 438 U.S. 154, 169 (1978).

[80] *See ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

[81] *See*, *e.g.*, 2017 FISC Op. at 19–23, 68–95; *Redacted*, 2011 WL 10945618, at *9; *cf. In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

[82] *See also, e.g.*, DOJ OIG, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019), https://bit.ly/2sOu8H4.

neither the FISC, nor any other court, is in a position to singlehandedly assess whether the government's applications are accurate and complete.

Greater disclosure to defense counsel is necessary to ensure that courts can fairly and accurately determine the legality of Section 702 surveillance used in criminal cases.

Recommendations to Strengthen Section 702 Disclosure

The ACLU urges PCLOB to:

- **Examine and report on the obstacles to fair and accurate court review that inadequate disclosure creates in criminal cases involving Section 702 surveillance.**
- **Propose legislative reforms that will ensure defendants and their counsel receive access to critical discovery concerning Section 702 surveillance and querying used in their cases.**

We appreciate the opportunity to present our views to PCLOB as it formulates its oversight project on Section 702 surveillance and examines the impact of this surveillance on privacy and civil liberties. We look forward to further collaboration with the Board. For more information, please contact Patrick Toomey at ptoomey@aclu.org or Ashley Gorski at agorski@aclu.org.

Sincerely,

Patrick Toomey
Ashley Gorski
Sarah Taitz
National Security Project
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
ptoomey@aclu.org
212.549.2500