epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the Privacy and Civil Liberties Oversight Board

on

Notice of the PCLOB Oversight Project Examining

Section 702 of the Foreign Intelligence Surveillance Act (FISA)

87 Fed. Reg. 58393

November 4, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Privacy and Civil Liberties Oversight Board's (PCLOB) Notice of the PCLOB Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act (FISA).[1] EPIC applauds the PCLOB's decision to examine FISA Section 702 ahead of its reauthorization deadline at the end of 2023. The PCLOB's investigations and recommendations are of vital importance to the American public and Congress in determining whether to renew Section 702 and, if it is renewed, what additional safeguards are necessary.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has particular interest in issues related to national security and surveillance. EPIC has engaged with the PCLOB since it was first formed in 2004. During that time, EPIC has provided extensive comments to the Board on EO 12333, FOIA

[1] 87 Fed. Reg. 58393, https://www.govinfo.gov/content/pkg/FR-2022-09-26/pdf/2022-20415.pdf.
[2] *See* About EPIC, EPIC.org, https://epic.org/epic/about.html.

procedures, and "defining privacy," among other topics.[3] EPIC has long argued that a full-strength, independent PCLOB is necessary for effective oversight of government surveillance programs, including Section 702.[4]

EPIC here provides specific recommendations to the Board to investigate the scope of Section 702 "abouts" collection and recommend Congress prohibit the practice; to review Section 702's use in cybersecurity investigations; to encourage Congress to prohibit warrantless backdoor searches; and to push for inclusion of additional safeguards in Section 702, including strengthening the role of FISC amici, codifying privacy protections for both U.S. and non-U.S. persons, ensuring that the government cannot circumvent notice requirements in criminal cases, and bolstering transparency requirements.

I. The PCLOB should investigate the scope of "abouts" collection and recommend that Congress prohibit the practice.

The National Security Agency (NSA) has persistently failed to bring its "abouts" collection activities into compliance with statutory and constitutional privacy requirements. Despite these failures, the NSA has restarted "abouts" collection, relying on advanced surveillance techniques that have improved and multiplied since the PCLOB's last report. Therefore, the PCLOB should

[3] Comments of the Electronic Privacy Information Center to the Privacy and Civil Liberties Oversight Board, Request for Public Comment on Activities Under Executive Order 12333 (June 16, 2015), https://epic.org/privacy/surveillance/12333/EPIC-12333-PCLOB-Comments-FINAL.pdf; Jeramie D. Scott, Nat'l Sec. Counsel, EPIC, Prepared Statement for the Record Before the Privacy and Civil Liberties Oversight Board (Jul. 23, 2014), https://epic.org/news/privacy/surveillance_1/EPIC-Statement-PCLOB-Review-12333.pdf; Comments of the Electronic Privacy Information Center to the Privacy and Civil Liberties Oversight Board, Freedom of Information, Privacy Act, and Government in the Sunshine Act Procedures (July 15, 2013), https://epic.org/open_gov/EPIC-PCLOB-FOIA.pdf; Letter from Marc Rotenberg, EPIC President, & Khaliah Barnes, EPIC Administrative Counsel, to PCLOB on "Defining Privacy," at 4 (Nov. 11, 2014), available at https://epic.org/open_gov/EPIC-Ltr-PCLOB-Defining-Privacy-Nov-11.pdf.

[4] *See* Letter from Coalition of Civil Liberties Organizations to President Joseph R. Biden, Jr. on PCLOB Vacancies (Sept. 7, 2021), available at https://cdt.org/wp-content/uploads/2021/09/2021-09-07-PCLOB-Vacancies-Coalition-Letter.pdf.

investigate and clearly define the current scope of "abouts" collection and recommend that Congress prohibit "abouts" collection altogether.

As opposed to other surveillance techniques that collect communications that are *to* or *from* a target, "abouts" collection sweeps in communications that merely *reference* a target—meaning that when two U.S. persons (who cannot be targeted under Section 702) reference the targeted selector (e.g., a non-U.S. person target's email address), that wholly domestic communication may be acquired.[5] As the PCLOB and the Foreign Intelligence Surveillance Court (FISC) have both emphasized, the sheer breadth of "abouts" collection—and the extent to which incidental collection is part and parcel of "abouts" collection—results in substantial privacy violations for the individuals whose personal information the government incidentally collects.[6]

Because of the uniquely invasive nature of "abouts" collection, the NSA has adopted special procedures limiting the use of the method, but the Agency has repeatedly failed to comply with even these minimal safeguard requirements. Since 2011, the NSA's own minimization procedures have "prohibited the use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702."[7] Only the NSA may receive this raw upstream-collected information; however, once the NSA has passed this information through its minimization procedures, it may share it with

---

[5] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115–118, §§ 103(a)(3)(5), 702(b)(5), 132 Stat. 3, 10 (2018) (codified at 50 U.S.C.A. § 1881a(b)(5) (West)).

[6] *See* PRIV. & CIV. LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 88 (2014) [hereinafter PCLOB SECTION 702 REPORT], https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf; *In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 19 (FISA Ct. Apr. 26, 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf (noting that the removal of "abouts" collection "eliminates the types of communications presenting the Court the greatest level of constitutional and statutory concern").

[7] *In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 19 (FISA Ct. Apr. 26, 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf; *see also* PCLOB SECTION 702 REPORT, *supra* note 6, at 7 (comparing how upstream collection functions in relation to downstream—then called PRISM—collection).

the FBI and CIA.[8] Therefore, the NSA's minimization procedures are a purported safeguard against abuse of upstream-collected information. However, for years, NSA personnel queried data collected through the Section-702 upstream program using U.S. person identifiers, despite the express prohibition against the use of these identifiers in the NSA's own minimization procedures.[9] In a 2017 opinion, the FISC deemed these queries "significant noncompliance" and a "very serious Fourth Amendment issue."[10] Ultimately, the NSA determined that it could not remedy the noncompliance and therefore decided to end "abouts" collection and purge all previously collected upstream data.[11]

Properly addressing "abouts" collection requires understanding its current scope. In 2017, after the NSA ended "abouts" collection, Congress enacted the FISA Amendments Act, which did not codify a prohibition on "abouts" collection but required the government to obtain FISC approval and notify Congress prior to resuming the practice.[12] In 2018, the government submitted its annual certifications and procedures, which appear to include some new form of "abouts" collection.[13] In its October 2018 opinion, the FISC disagreed with the appointed amicus and concluded that certain novel surveillance practices did not constitute "abouts" collection, thus triggering restrictions imposed by Congress.[14] Given this disagreement, it is crucial that the PCLOB investigate and clearly define the scope of current "abouts" collection.

---

[8] PCLOB SECTION 702 REPORT, *supra* note 6, at 7.
[9] *In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 19 (FISA Ct. Apr. 26, 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[10] *Id.*
[11] *Id.* at 23.
[12] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118 § 103, 132 Stat. 3, 10–13 (2018).
[13] *In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 31 (FISA Ct. Oct. 18, 2018), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.
[14] *Id.*

Given the history of persistent and significant noncompliance relating to "abouts" collection, the PCLOB should:

- Investigate and clarify the current scope of "abouts" collection; and
- Recommend that Congress prohibit "abouts" collection altogether.

II. The PCLOB should review the use of 702 collection in cybersecurity investigations.

The Intelligence Community has dramatically increased use of Section 702 in cybersecurity investigations over the last five years. That purported justification for expanding use of 702 warrants close inspection. The government has repeatedly highlighted its use of Section 702 in the context of its cybersecurity investigations. The NSA claims it has used Section 702 to identify cybersecurity information relating to hostile foreign governments and foreign adversaries, including identifying specific foreign individuals and their tactics, techniques, and procedures;[15] to protect U.S. government networks by bolstering understanding of specific cyber vulnerabilities and infrastructure;[16] to identify the scope of malicious cyber activities to warn and protect U.S. victims.[17]

While the government claims that Section 702 has played an important role in cybersecurity investigations, there is not enough public information to corroborate whether Section 702 is necessary to accomplish these goals, and whether special safeguards are necessary in the cyber context. The use of Section 702 as part of cybersecurity efforts raises privacy and civil liberties concerns given the potential breadth of collection and querying. According to the ODNI's Statistical Transparency Report for 2021, the FBI conducted batch queries related to "attempts to compromise

---

[15] *"Section 702" Saves Lives, Protects the Nation and Allies*, NAT'L SEC. AGENCY (Dec. 12, 2017), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1627009/section-702-saves-lives-protects-the-nation-and-allies/.
[16] *Id.*
[17] *Section 702 Overview*, OFFICE OF THE DIR. OF NAT'L INTEL. 10, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

U.S. critical infrastructure by foreign cyber actors."[18] These queries included approximately 1.9 million query terms—more than all reported queries over the previous year—related to potential victims, including U.S. persons.[19]

Given this exponential increase, the PCLOB should investigate and report on the use of Section 702 in the cybersecurity context. Such review is within scope for the PCLOB because national security agencies assert that cyber-attacks are frequently a vector for attacks with terroristic motives, and therefore claim that cyber is an integral part of U.S. counterterrorism programs.[20] U.S. government officials have repeatedly emphasized the growing threat of cyber-enabled terrorism.[21] These officials have also emphasized the need to meet cyber-enabled threats with the same approach as traditional counterterrorism, using a "whole-of-government" and "all-tools" approach, including reliance on intelligence tools.[22]

It is vital that the public understand the scope of surveillance systems used in cybersecurity investigations and whether additional privacy and civil liberties protections are necessary to ensure

[18] OFFICE OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2021 20 (Apr. 2022).
[19] *Id.*
[20] PCLOB's enabling statute authorizes it to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties," and to "ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation from terrorism." 42 U.S.C. § 2000ee(c).
[21] *See* Leon Panetta, U.S. Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012) (transcript available at https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity) (emphasizing that a cyber-attack by violent extremist groups "could be as destructive as the terrorist attack on 9/11" and could "virtually paralyze the nation"); Press Release, *Global Disruption of 3 Terror Finance Cyber-Enabled Campaigns* https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns (quoting several U.S. officials emphasizing the need to counter terrorist groups' adaptation of their finance activities in the cyber age); Lisa Monaco, Assistant Att'y Gen. for Nat'l Sec., Remarks to the 2012 Cybercrime Conference (Oct. 25, 2012) (transcript available at https://www.justice.gov/nsd/justice-news-2) (outlining the threat posed by cyber-enabled terrorism and the U.S. approach to countering cyber-attacks) [hereinafter Assistant Att'y Gen. Monaco Remarks].
[22] Assistant Att'y Gen. Monaco Remarks, *supra* note 21.

that these investigative tools are not abused. Therefore, the PCLOB should investigate and report on the use of Section 702 collection in cybersecurity investigations, including but not limited to:

- Estimates on the scale of this use and the volume of data collected, including a specific estimate of its impact on U.S. persons;
- What if any special procedures exist for the retention, dissemination, and use of data collected in support of cyber investigations, given the scope of potential collection; and
- Whether documentation requirements relating to cybersecurity-related querying are meaningfully enforced.

III. The PCLOB should investigate the effectiveness of the role played by FISC amici in protecting privacy and civil liberties.

Since their establishment, FISA court amici have been incorporated into FISA court review on a limited basis, but—contrary to prior PCLOB recommendations—amici roles are narrowly circumscribed and lack authority to truly advocate on behalf of the public, severely limiting their value in key areas such as FISC reauthorization of programmatic surveillance. Without a strong public advocate, the secretive and non-adversarial nature of the FISA court process cannot is even more prone to abuse and unlikely to provide substantive privacy and civil liberties protections.

The USA FREEDOM Act of 2015 established a process for appointing independent amici curiae for orders before the FISC that "present[] a novel or significant interpretation of the law."[23] Notably, however, amici may only weigh in on legal issues, not the impacts of proposed surveillance on privacy and civil liberties.[24] Further, the FISC may decline to appoint amici if it deems it inappropriate.[25] Through the end of 2021, the FISC had only appointed amici on twenty-five occasions, and had never done so in any case involving an individual surveillance application. Even

[23] United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Pub. L. No. 114-23 § 401(i)(2)(A), 129 Stat. 268 (codified at 50 U.S.C. §§ 1872-1874 (2012) and 18 U.S.C. §§ 2280-2281, 2332 (2012)).
[24] *See id.* § 401(i)(4).
[25] *Id.* § 401(i)(2)(A).

where amici are appointed, they are constrained in their ability to advocate on behalf of the public because they lack all the information relevant to the matter, and they have no ability to petition to certify questions for review at the FISCR or the Supreme Court.

Throughout the last eight years, civil liberties advocates and the PCLOB have highlighted areas where the role of amici should be expanded or strengthened.[26] The PCLOB should build off its prior report and recommend that Congress meaningfully reform the FISC amicus system, including but not limited to the following areas:

- Amici should participate in a broader set of FISA court proceedings, not just those that present "novel and significant" issues. In particular, the PCLOB should recommend—in line with prior reform proposals[27]—that the amici also be authorized to participate those cases that:
    - Present "significant concerns" relating to activities protected by the First Amendment;
    - Present or involve a "sensitive investigative matter," i.e., an investigative matter involving a domestic public official or political candidate, religious or political organization, or news media;
    - Involve a request for approval of a new program, technology, or use of existing technology; or
    - Present a request to the FISC for reauthorization of programmatic surveillance.
- Amici should have full access to all government filings and information related to these matters.
- Amici should be able to petition FISCR for appellate review, or the Supreme Court after FISCR review.

[26] *See* PRIV. & CIV. LIBERTIES OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT 5–6 (Feb. 5, 2016), available at https://irp.fas.org/offdocs/pclob-assess-2016.pdf [hereinafter PCLOB RECOMMENDATIONS ASSESSMENT REPORT]; Faiza Patel & Raya Koreh, *Improve FISA on Civil Liberties by Strengthening Amici*, JUST SEC. (Feb. 26, 2020), https://www.justsecurity.org/68825/improve-fisa-on-civil-liberties-by-strengthening-amici/.

[27] *See, e.g.*, Lee-Leahy Amendment, H.R. 6172, 116th Cong. (as passed by Senate, May 14, 2020).

IV. The PCLOB should investigate the disparate impact of the use of Section 702-derived information.

Counterterrorism and surveillance programs have historically focused disproportionately on communities of color, including the Muslim community during the so-called "War on Terror." For years, civil liberties groups have expressed concerns that Section 702 and other intelligence collection activities have had a disparate impact on communities of color.[28] Beyond the inherently biased focus on certain groups in initial targeting decisions, the analysis and use of information derived from programmatic surveillance activities can contribute to discrimination by misidentifying individuals from particular social groups at higher rates than others, as well as overclassifying information as relevant to foreign intelligence based on a lack of linguistic and cultural competency. Despite calls for investigation, the U.S. government has done little to address or remedy concerns of discriminatory impact. Further, the secrecy with which these programs operate makes it difficult for civil liberties groups or the public to fully assess the scope of any disparate impacts.

The U.S. government has recognized that, given their foreign intelligence purpose, its intelligence activities are inherently discriminatory.[29] Earlier this year, in response to a directive from Congress, the ODNI began to assess disparate impact of intelligence activities in more limited circumstances. The ODNI examined the "privacy, civil liberties, and related civil rights controls, as well as related training, oversight, and avenues for the public to raise concerns regarding IC

[28] Jake Laperruque, *In Support of Research and Reporting on the Disparate Use and Impact of FISA*, POGO (Apr. 8, 2019), https://www.pogo.org/testimony/2019/04/in-support-of-research-and-reporting-on-the-disparate-use-and-impact-of-fisa.

[29] OFF. OF THE DIR. OF NAT'L INTEL., BEST PRACTICES TO PROTECT PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS OF AMERICANS OF CHINESE DESCENT IN THE CONDUCT OF U.S. INTELLIGENCE ACTIVITIES 13 (May 2022), available at https://www.dni.gov/files/CLPT/documents/ODNI_Report_on_Best_Practices_to_Protect_Privacy_Civil_Liberties_and_Civil_Rights_of_Americans_of_Chinese_Descent_in_ConductOof_US_Intelligence_Activities_May_2022.pdf [hereinafter ODNI BEST PRACTICES].

conduct."[30] The resulting report analyzed best practices to protect the privacy, civil liberties, and civil rights of Americans of Chinese descent during the course of U.S. intelligence activities.[31]

Overall, the ODNI found that while the IC's policies and procedures "reflect an appropriate focus" on protecting the privacy, civil liberties, and civil rights in the implementation of these intelligence activities, it made several recommendations, including that: (1) IC agencies "reemphasize the prohibition on conducting intelligence and related security activities based on race or ethnicity [. . .] in their training materials"; (2) IC agencies "expand unconscious bias and cultural competency training to personnel involved in intelligence collection"; and (3) privacy officers, civil rights officers, and civil liberties officers "further develop and, when relevant, highlight the potential for disparate impacts on historically disadvantaged groups of U.S. persons, including Americans of Chinese descent, when conducting analyses and making recommendations regarding intelligence and related security activities."[32]

As the ODNI noted, assessing disparate impact in the context of incidental collection is particularly difficult because "[t]he IC neither has, nor could realistically generate, demographic information regarding U.S. persons whose information has been incidentally collected."[33] However, despite this lack of data, the ODNI emphasized that "the IC does not presume that the impact of incidental collection is evenly distributed across the American public."[34] Therefore, the ODNI tasked

[30] *Id.*
[31] *Id.* at 3.
[32] *Id.* at 5. The ODNI highlighted similar mechanisms in other areas such as the ODNI's 2020 Principles of Artificial Intelligence (AI) Ethics for the Intelligence Community, which requires the IC to "take affirmative steps to identify and mitigate bias" and the accompanying AI Ethics Framework for the Intelligence Community, which further defines steps to minimize bias. *Id.* at 16.
[33] *Id.* at 13.
[34] *Id.*

the IC Civil Liberties and Privacy Council[35] with leading the development and dissemination of best practices and tools for conducting disparate impact analysis in incidental collection.[36]

While EPIC applauds the ODNI's reporting, far more information is needed to properly gauge the disparate impact of programs like those authorized under Section 702. Beyond the inherent disparate impact of foreign intelligence surveillance, biased analysis and use of Section 702-derived information causes concrete harms that will fall more heavily on certain communities if not properly mitigated.

For example, prior counterterrorism programs relying on name matching have resulted in substantial harm to individuals from communities where naming conventions result in many individuals with identical names, resulting in misidentification.[37] In *TransUnion LLC v. Ramirez*, Sergio Ramirez was denied a car purchase because he shared the same first and last name with an individual on the U.S. Treasury Department's Office of Foreign Assets Control terrorist watch list, which TransUnion incorporated into its credit report without verifying potential name matches with other sources of information.[38] Both the Treasury Department and TransUnion failed institute sufficient protections to prevent Mr. Ramirez's wrongful identification and subsequent financial hardships.

Further, monitoring communications across languages and cultures creates substantial risk of oversurveillance and wrongful surveillance which is hard to mitigate without significant linguistic and cultural competency. Processing and making meaning out of communication data from around the world requires understanding of location-specific and community-specific communication

[35] The IC Civil Liberties and Privacy Council led the development of the AI Ethics Framework for the Intelligence Community.
[36] *Id.* at 16.
[37] U.S. Gov't Accountability Off., GAO-06-1031, Terrorist Watchlist Screening: Efforts to Reduce Adverse Effects on the Public 19 (2006), available at https://www.gao.gov/assets/gao-06-1031.pdf.
[38] 141 S. Ct. 2190, 2201–02 (2021).

patterns, such as idiom, satire, and slang. Without adequate familiarity with these communication patterns, agencies may be more likely to overreach when identifying communications as relevant for foreign intelligence purposes. While agency minimization procedures reference translation support from foreign governments and other agencies, it is far from clear how bias mitigation is embedded into the processing and analysis of Section-702 derived information.

Finally, while the ODNI highlighted efforts to include bias mitigation training as part of intelligence activities, persistent compliance issues in core areas of Section 702, such as querying standards or retention and purging requirements, raise concerns that bias mitigation training, even if available, may not adequately address the disparate impact in analysis and use of Section-702 derived information.

EPIC applauds the ODNI's efforts on addressing disparate impacts resulting from intelligence activities and recommends the PCLOB build on these efforts by investigating the potential for disparate impact in Section 702 activities. Given the substantial privacy harms that arise from misidentifications or other disparate impacts of analysis and use of Section 702-derived information, it is vital that the PCLOB, members of Congress, and the American public understand how bias mitigation is incorporated into the IC's training and handling procedures. As the ODNI noted, "further examination will provide valuable perspective on whether the IC's protections provide equitable outcomes for other persons of color as well."[39] In particular, EPIC recommends the PCLOB investigate and report on:

- How the IC incorporates into its training and information handling procedures discussion of the risks of disparate impact in the use and analysis of Section 702-derived information, including but not limited to misidentification and cultural or linguistic misunderstanding.
- Whether there are particular empirical metrics—such as the demographics of those criminal defendants against whom the government relied on Section 702-derived

[39] ODNI BEST PRACTICES, *supra* note 29, at 5.

information—that shed light on any disparate impacts but do not implicate the same difficulties or risks as a top-line demographic breakdown of all U.S. persons whose information was collected through Section 702.

V. The PCLOB should review its prior analysis of the constitutional basis for 702 in light of the Supreme Court's decision in *Carpenter*.

In its last report, the PCLOB found that the core of Section 702 met the "totality of the circumstances" standard for reasonableness under the Fourth Amendment, but that certain aspects of Section 702—the scope of incidental collection, "abouts" collection, and the use of U.S. person queries—"push the program close to the line of constitutional reasonableness."[40] Since the PCLOB's report, the Supreme Court has revisited its reasonableness analysis in light of new means of government surveillance.

In *Carpenter v. United States*, the Supreme Court held that law enforcement authorities must obtain a warrant before accessing seven or more days of an individual's cell site location information (CSLI).[41] The Court's emphasis on the extent to which retroactive CSLI collection operated to give authorities "near perfect surveillance" of an individual has garnered significant attention because of its implications for other emerging surveillance technology.[42] Under *Carpenter*, highly intrusive surveillance using information gained from third parties will often be a search under the Fourth Amendment, and so can only be constitutional with a warrant supported by probable cause. However, despite this significant shift in Fourth Amendment doctrine, there is no clear indication of how—if at all—the government applies *Carpenter* to its programmatic surveillance programs like Section 702.

Within the FISC, there appears to be at least some sign of disagreement over *Carpenter*'s applicability. The FISC's 2018 certification order notes that FISC amici argued that "reviewing

[40] PCLOB SECTION 702 REPORT, *supra* note 6, at 9.
[41] *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).
[42] *Id.* at 2218.

querying as an independent Fourth Amendment event would be in line with evolving case law," including *Carpenter*.[43] Therefore, according to these amici, querying of information lawfully acquired under Section 702 requires a reasonableness determination independent of that concerning collection.[44] The FISC, however, declined to find that queries constitute a distinct Fourth Amendment event, finding that the case law cited by amici was distinguishable from the unique statutory framework of Section 702.[45]

At least one other court has recognized that the use of already-collected information for a broad range of law enforcement purposes poses significant privacy risks. In *United States v. Hasbajrami*, the Second Circuit considered the reasonableness of querying separately from the reasonableness of the collection.[46] In doing so, it noted—citing *Riley v. California*[47]—that "courts have increasingly "recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected."[48] The Second Circuit also emphasized that the program, given its sweeping breadth of collection and the broad availability for review by domestic law enforcement agencies, "begins to look more like a dragnet, and a query more like a general warrant[.]"[49] The Second Circuit further found that permitting indiscriminate warrantless querying by domestic law enforcement of information collected for foreign intelligence purposes "would be at odds with the bedrock Fourth Amendment

[43] *In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 86 (FISA Ct. Oct. 18, 2018), available at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.
[44] *Id.*
[45] *Id.* at 86–87.
[46] 945 F.3d 641, 669 (2d Cir. 2019).
[47] 573 U.S. 373 (2014). In *Riley*, the Court found that law enforcement officers need to obtain a warrant to search a cell phone, even where incident to a lawful arrest. *Id.* at 386.
[48] *Hasbajrami*, 945 F.3d at 670.
[49] *Id.* at 671.

concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search."[50]

Given the evolution of the Supreme Court's reasonableness analysis in the digital age, as well as disagreements between the FISC and amici over *Carpenter*'s applicability to Section 702, the PCLOB should review its constitutional and statutory analysis of Section 702, and in particular the current scope of incidental collection, "abouts" collection, and the use of U.S. person queries.

VII. The PCLOB should recommend a prohibition on warrantless backdoor searches.

The warrantless querying of data acquired under Section 702 circumvents essential Fourth Amendment protections and posts a significant threat to the privacy of communications. Section 702 authorizes certain electronic surveillance of foreign communications without probable cause, so long as the target of an investigation is a non-U.S. person located outside the United States. Section 702 further prohibits the targeting of U.S. persons—whether directly or through "reverse targeting." However, federal agents can search communications collected under Section 702 for information about U.S. persons, even when they could not lawfully target this information at the front end.

For years, EPIC and other civil liberties advocates have decried these warrantless "backdoor" searches as a dangerous end-run around the Fourth Amendment.[51] Oversight bodies have repeatedly questioned the use of this technique and have called on the FBI to document and review these searches. But the agency has repeatedly failed to comply with these oversight requests and even the most basic transparency requirements. For example:

---

[50] *Id.* at 672.

[51] *See, e.g.*, Complaint, *EPIC v. U.S. Dep't of Justice Nat'l Sec. Div.*, No. 17-2274 at 5–6 (D.D.C. 2017), available at https://epic.org/wp-content/uploads/foia/epic-v-NSD/1-Complaint.pdf; Michelle Richardson, *Section 702: Fixing the Backdoor Search Loophole*, CTR. FOR DEMOCRACY & TECH. (June 22, 2017), https://cdt.org/insights/section-702-fixing-the-backdoor-search-loophole/; Julian Sanchez, *Reforming Surveillance Authorities*, CATO HANDBOOK FOR POLICYMAKERS (2017), https://www.cato.org/cato-handbook-policymakers/cato-handbook-policy-makers-8th-edition-2017/11-reforming-surveillance-authorities#close-section-702-s-backdoor-search-and-about-search-loopholes.

- In 2018, as the result of a Freedom of Information Act lawsuit, EPIC obtained a report mandated by the Foreign Intelligence Surveillance Court ("FISC") due to concerns about the possible misuse of Section 702 authority by the FBI. The report shed light on FBI analysts' failure to follow internal guidance requiring notification to their superiors when they "receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[52]

- In its twenty-third semiannual review of Section 702 compliance covering the second half of 2019, the ODNI found that FBI personnel had misunderstood basic querying standards and had conducted batch queries of large numbers of identifiers, including U.S. person identifiers, without any expectation that those queries would result in foreign intelligence or evidence of a crime.[53]

- A recent DOJ Inspector General report found that the FBI and DOJ had disagreed over the proper querying standard under Section 702, with a senior NSD official stating that the FBI took a much broader approach to querying due to "a fundamental misunderstanding of the standard."[54] Even after working to align the standards in 2018, the FBI continued to press—without success—for the use of Section 702 querying in vetting potential confidential informants, even where there was no basis to believe that the subject had criminal intent or was a threat to national security.[55]

- In a November 2020 opinion, the FISC reported that an audit into the FBI's Section 702 querying practices revealed that FBI personnel had made forty queries of Section 702-acquired information involving U.S. persons for use in domestic criminal investigations without court approval in 2019-2020.[56] The FISC emphasized that, because these query violations aligned with prior reported violations and were discovered through a limited audit, it was concerned about the FBI's "apparent widespread [Section 702] violations."[57]

---

[52] *See* Letter from Kevin J. O'Connor, Chief, Oversight Section, Off. of Intel., Dep't of Just., to Rosemary M. Collyer, Presiding Judge, Foreign Intel. Surveillance Ct. (Jan. 23, 2017), available at https://epic.org/wp-content/uploads/foia/epic-v-NSD/EPIC-17-05-15-NSD-FOIA-20180108-Production.pdf.

[53] DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT—REPORTING PERIOD: JUNE 1, 2019 – NOVEMBER 30, 2019 31 (Sept. 2021), https://www.intel.gov/assets/documents/702%20Documents/declassified/23rd_Joint_Assessment_of_FISA_for_Public_Release.pdf [hereinafter 23RD SEMIANNUAL 702 COMPLIANCE ASSESSMENT].

[54] DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., AUDIT OF THE ROLES AND RESPONSIBILITIES OF THE FEDERAL BUREAU OF INVESTIGATION'S OFFICE OF THE GENERAL COUNSEL IN NATIONAL SECURITY MATTERS 23 (Sept. 2022), available at https://oig.justice.gov/sites/default/files/reports/22-116.pdf.

[55] *Id.* at 24.

[56] *In re* Section 702 2020 Certification, No. [REDACTED], 42 (FISA Ct. Nov. 18, 2020), https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

[57] *Id.* at 43–44.

The government has contended that a warrant requirement would "hamper the speed and efficiency of operations, and impair the [intelligence community]'s ability to identify and prevent threats to America."[58] In particular, the government has highlighted scenarios in which a warrant requirement would be detrimental to national security. However, the government's operational concerns do not appear to have a strong foundation because most of the examples they refer to would likely fall within an exception to the warrant requirement. For example:

1. *"Using the name of a U.S. person hostage to cull through communications of the terrorist network that kidnapped her to pinpoint her location and condition[.]"*[59]

Courts have routinely upheld government searches under the exigency exception to the Fourth Amendment warrant requirement in ongoing hostage situations, even where time has passed between the initiation of the hostage-taking and the search itself.[60] Therefore, the use of a U.S. person hostage's name to query terrorist communications to ascertain the hostage's whereabouts and condition would likely be upheld under the exigency exception.

2. *"Using the email address of a U.S. victim of a cyber-attack to quickly identify the scope of malicious cyber activities and to warn the U.S. person of the actual or pending intrusion[.]"*[61]

3. *"Using the name of a government employee that has been approached by foreign spies to detect foreign espionage networks and identify other potential victims[.]"*[62]

4. *"Using the name of a government official who will be traveling to identify any threats to the official by terrorists or other foreign adversaries."*[63]

[58] *Section 702 Overview*, OFF. OF THE DIR. OF NAT'L INTEL. 10, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.
[59] *Id.*
[60] *See, e.g.*, *United States v. De Jesus-Batres*, 410 F.3d 154, 159 (5th Cir. 2005) (finding that a warrantless search of a garage suspected of containing hostages was justified by exigent circumstances).
[61] *Section 702 Overview*, supra note 58, at 10.
[62] *Id.*
[63] *Id.*

Courts have similarly upheld government relying on the consent of the person whose information is searched.[64] In these three scenarios, it appears reasonable to have the government obtain the consent of the U.S. victim or U.S. government employee to conduct searches using the individual's information for security and foreign intelligence purposes.

As these scenarios illustrate, it is far from clear how substantially a warrant requirement would interfere with the FBI's ability to execute investigations in these circumstances. Therefore, the PCLOB, in addressing the FBI's query authorities, should investigate any effect a warrant requirement would have, taking into account the warrant requirement's broad exceptions. In addition to assessing the feasibility of a warrant requirement, it is imperative that the American public, the PCLOB, and members of Congress consider the scope of the FBI's backdoor searches—as well as the scope and frequency of compliance violations—in deciding how to reform Section 702 next year. Given the FBI's history of noncompliance, the PCLOB to recommend that any reform proposal include a full fix of the backdoor search loophole requiring all agencies to obtain a warrant based on probable cause to search Section 702 data for information about U.S. citizens and residents in all investigations.

VIII. PCLOB should recommend new safeguards in Section 702 that apply across the board, regardless of nationality.

Section 702 is one of the largest scale surveillance programs and its scope calls for especially strong privacy protections that are rooted in legislative power and not merely executive fiat. The U.S. government has taken steps recently to reinforce privacy safeguards as part of its signals intelligence activities, including Section 702. However, these safeguards lack the stability of legislation and do not go far enough to promote meaningful restrictions on programmatic

[64] *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973).

surveillance programs like Section 702. Therefore, the PCLOB should recommend further legislative action codifying more robust privacy protections for both U.S. persons and non-U.S. persons.

a. Codifying protections for non-U.S. persons

Legislative reforms must be made on the provisions of Section 702 that authorize data collection on non-U.S. persons. In July 2020, the Court of Justice of the European Union (CJEU) in the case *Schrems II* struck down the EU-U.S. Privacy Shield.[65] The CJEU had previously found that there were insufficient legal protections for the transfer of European consumer data to the United States, primarily because the surveillance authority granted to the U.S. government under Section 702.[66] In *Schrems II*, the CJEU once again found that U.S. law inadequately protected European consumer data, emphasizing the insufficient strength of privacy safeguards and the lack of independent and effective redress.[67] In response, the EU and U.S. agreed to the new EU-U.S. Data Privacy Framework, which—through an implementing Executive Order—seeks to address these concerns, including by equalizing certain privacy protections—such as minimization and retention procedures—between U.S. persons and non-U.S. persons.[68] While these safeguards represent an improvement over the prior privacy framework, without reforms by Congress, the new EU-U.S. Data Privacy Framework could very well be invalidated by the CJEU.

b. Codifying more meaningful safeguards, regardless of nationality

In addition to codifying protections for non-U.S. persons, the PCLOB should recommend more meaningful safeguards governing collection, retention, and dissemination, regardless of

[65] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 168–200 (July 16, 2020).
[66] *Id.* ¶ 42.
[67] *Id.* ¶¶ 168–200.
[68] Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities § 2(c)(iii) (Oct. 7, 2022).

nationality. While the new Executive Order equalizes certain protections between U.S. persons and non-U.S. persons, these protections are only effective if they are meaningful and properly enforced.

In particular, the PCLOB should recommend:

1. *Stronger documentation requirements as part of querying procedures.*

According to the ODNI, agencies' querying procedures "require a written statement of facts justifying that the use of any such identifier as a query selection term of Section 702-acquired content is reasonably likely to retrieve foreign intelligence information or, in the instance of FBI, evidence of a crime."[69] In response to widespread compliance incidents, in 2019, the FBI amended its querying procedures to require further documentation on why a U.S.-person query met the appropriate legal standard prior to accessing the contents of the communication retrieved by the query.[70] However, even after these changes, the FISC noted that compliance issues remained.[71] Nonetheless, the FISC found that because the majority of the compliance issues occurred prior to the change in procedures, and because the government's oversight was limited by the COVID-19 pandemic, the persistent noncompliance did not undermine the updated minimization procedures as a whole.[72] Given the FISC's continued concern over the adequacy of documentation requirements, especially those of the FBI, the PCLOB should recommend stronger documentation requirements and more meaningful review of analysts' statements of reasons to identify individuals in need of further training on querying standards and prevent abuse.

[69] 23RD SEMIANNUAL 702 COMPLIANCE ASSESSMENT, *supra* note 53, at 80.
[70] *In re: Section 702 2020 Certification*, No. [Redacted] at 38 (FISA Ct. Nov. 18, 2020).
[71] *Id.* at 39–41.
[72] *Id.* at 41.

2. *More meaningful retention limits at the front end, and more restrictive exceptions to these limits.*

In general, data collected under Section 702 may be retained for five years, unless it has been identified as "foreign intelligence," in which case it may be retained indefinitely.[73] However, many agencies' minimization procedures contain exceptions to the age-off requirements. For example, the NSA's minimization procedures provide that the NSA may retain unminimized encrypted information "for a sufficient duration to permit exploitation[,]" meaning "any period of time during which the encrypted information is subject to, or of use in, cryptanalysis or deciphering secret meaning."[74] Open-ended exceptions like these create broad authority to indefinitely retain certain information. Therefore, the PCLOB should recommend shorter default retention periods and narrower exceptions to these default periods.

3. *Stricter enforcement of purging requirements, especially for improperly collected communications.*

The FISC has repeatedly found that agencies failed to timely purge Section 702-acquired information. In 2015, the FISC criticized the government after it disclosed that it had failed to purge improperly collected communications.[75] Compounding this failure to purge is the government's

[73] *See* Central Intelligence Agency, Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended § 2(a) (Sept. 17, 2019) [hereinafter CIA Minimization Procedures]; National Counterterrorism Center, Minimization Procedures Used by National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended § B(2)(a) (Oct. 19, 2020) [hereinafter NCTC Minimization Procedures]; National Security Agency, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended § 7(a)(1) (Oct. 19, 2020) [hereinafter NSA Minimization Procedures]. The FBI's default retention period for raw, unreviewed Section 702 data is five years; however, the FBI may retain information that has been reviewed but not yet determined to meet the applicable standard for indefinite retention for up to fifteen years. Federal Bureau of Intelligence, Minimization Procedures Used by the Federal Bureau of Intelligence in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended § III(D)(4)(c) (Sept. 17, 2019) [hereinafter FBI Minimization Procedures].
[74] *See* NSA Minimization Procedures, *supra* note 73, at § 7(a)(1)(a).
[75] *In re* [REDACTED], No. [REDACTED] at 58 (FISA Ct. Nov. 6, 2015).

failure to timely notify the FISC of this noncompliance. According to the FISC, "[p]erhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information."[76] The FBI and CIA have both also been reprimanded by the FISC for their own violations of purging requirements.[77]

4. *A prohibition on use of attorney-client privileged communications acquired pursuant to Section 702 for any purpose—including analytic purposes—except for technical and compliance personnel implementing the agency's attorney-client privilege segregation requirements.*

In its 2020 certification order, the FISC expressed concern that the NSA—by marking privileged communications for quarantine on the NSA's Master Purge List (MPL) but leaving them discoverable by NSA personnel—did not comply with the segregation requirements in its minimization procedures.[78] The FISC noted that the NSA continued to interpret the segregation requirement differently from the CIA and NCTC, both of which "forgo analytic use of these sensitive categories of communications and limit access to technical and compliance personnel charged with implementing the attorney-client privilege requirements of their respective procedures."[79] While the FISC ultimately approved the NSA's procedures, it warned against the potential that the NSA might disseminate privileged information to the FBI that, had the FBI sought to obtain that same information, would have to be sequestered.[80]

[76] *Id.*
[77] *See In re* [REDACTED], Memorandum Opinion and Order, No. [REDACTED] 87–89, 94–95 (FISA Ct. Apr. 26, 2017), available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[78] *In re: Section 702 2020 Certification*, No. [Redacted] at 26 (FISA Ct. Nov. 18, 2020).
[79] *Id.* at 28.
[80] *Id.* at 30.

IX. The PCLOB should recommend that Congress enact more robust notice requirements, as well as a prohibition on parallel construction.

The government has repeatedly failed to provide notice to criminal defendants that 702-derived evidence is being used against them in prosecutions. The current structure for providing notice must be revised. As civil liberties groups have documented for years, while the scope of Section 702 targeting remains significant, there have been only a handful of cases in which a criminal defendant was notified that the government intended to introduce 702-derived evidence.[81] Civil liberties groups have expressed concern that the government is concealing its reliance on Section 702 by narrowly construing its notice obligations and by engaging in "parallel construction," whereby law enforcement authorities "recreate the evidentiary trail[.]"[82] Without meaningful notification policies or protections against parallel construction, there is a great risk that much of 702-derived evidence kept out of view of the courts, hindering criminal defendants' ability to fully defend themselves.

Therefore, the PCLOB should recommend reforms to the current notice system, including but not limited to:

- Requiring that notice must be given to criminal defendants in all instances where that evidence would not have been discoverable but for the use of Section 702.
- The prohibition of parallel construction to ensure agencies cannot build criminal cases without providing notice to defendants.

[81] *See, e.g.*, Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.
[82] Laura K. Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, COUNCIL ON FOREIGN RELS. (June 26, 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law.

X. The PCLOB should recommend greater transparency measures.

The PCLOB plays an integral role in encouraging transparency about the effects that programs within its purview have on U.S. persons' privacy. Despite prior PCLOB recommendations and calls from civil liberties groups, the U.S. government has not provided key declassified information about Section 702. This opacity hinders vigorous public debate weighing the benefits and costs of these programs, especially heading into their reauthorization deadline. Therefore, the PCLOB should recommend greater transparency measures, including but not limited to:

1. The U.S. government should develop and release a reliable methodology to gauge the value of 702 collection, in line with prior PCLOB recommendations.[83] Despite promises from the US government, no such methodology has been released. Therefore, the PCLOB should again recommend that the US government release a methodology substantiating the value of 702 collection in its current form.

2. The U.S. government should develop and release a declassified estimate of the number of U.S. persons whose communications have been incidentally collected pursuant to Section 702. The PCLOB previously suggested various metrics by which U.S. government could provide estimates.[84] Since then, members of Congress and civil liberties groups have called for years for such a statistical estimate, but—despite indications that the ODNI would provide an estimate, the U.S. government later walked back those promises, citing privacy and security concerns.[85]

3. The PCLOB should recommend the further declassification of other influential FISC documents and information, including but not limited to:

    a. FISC amicus briefs; and

    b. Written findings supporting any decision to not appoint amicus curiae.

[83] PCLOB RECOMMENDATIONS ASSESSMENT REPORT, supra note 26, at 18–19.
[84] *Id.*
[85] 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-caught-in-warrant-less-spying-idUSKBN19031B.

Conclusion

EPIC applauds the Oversight Board for its continued oversight of Section 702. The PCLOB's work supports robust public debate over the efficacy and privacy implications of Section 702 ahead of its reauthorization deadline at the end of 2023. Ahead of the reauthorization deadline, EPIC believes the PCLOB should investigate the scope of Section 702 "abouts" collection and recommend Congress prohibit the practice; to review Section 702's use in cybersecurity investigations; to encourage Congress to prohibit warrantless backdoor searches; and to push for inclusion of additional safeguards in Section 702, including strengthening the role of FISC amici, codifying privacy protections for both U.S. and non-U.S. persons, ensuring that the government cannot circumvent notice requirements in criminal cases, and bolstering transparency requirements. EPIC looks forward to engaging further with the PCLOB to support its work in this vital area. For further questions, please contact EPIC Executive Director Alan Butler at butler@epic.org.

Respectfully Submitted,

Alan Butler
Alan Butler
EPIC Executive Director

Jake Wiener
Jake Wiener
EPIC Counsel

Chris Baumohl
Chris Baumohl
EPIC Law Fellow