PUBLIC SUBMISSION

As of: 10/5/22, 3:07 PM
Received: September 26, 2022
Status: Pending_Post
Tracking No. l8j-cw3d-opnr
Comments Due: October 31, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0024
Comment on PCLOB_FRDOC_0001-0021

Submitter Information

Name: Anonymous Anonymous
Address: United States,

General Comment

The PCLOB should play a leading role in reviewing and critiquing the reauthorization (or non-reauthorization) of this statute. It should propose strict statutory language that clearly delineates what constitutes acceptable and unacceptable data collection so that executive agencies are not left to interpret the statute themselves (where such interpretation would be subject to deference from courts under the Chevron standard, if anyone ever had standing to sue in the first place - which is another concern). The statute should provide for strong oversight by independent agencies and, of course, Congress. Although specific details of data collection are understandably classified, the statute should require some amount of sunshine and transparency about the magnitude of collection, the nature and degree of any internal or external oversight of the data collection, and the results of any audits. Congress and the public and the PCLOB cannot weigh the costs and benefits of such a program unless they have general data about the number of crimes solved, the number of criminal conspiracies foiled, and the financial impacts of the program including direct budget, the financial implications of averted crimes, the amount spent on tracking or investigating innocent persons who were inadvertently swept into the program, etc.

PUBLIC SUBMISSION

As of: 11/1/22, 3:16 PM
Received: October 31, 2022
Status: Draft
Tracking No. l9x-m9hw-cijv
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0025
Comment on FR Doc # 2022-20415

Submitter Information

Email: bscarpelli@actonline.org
Organization: ACT | The App Association

General Comment

See attached for comments of ACT | The App Association

Attachments

ACT Comments to PCLOB re Oversight Project Examining Section 702 of FISA (31 Oct 2022)

October 31, 2022

Privacy and Civil Liberties Oversight Board
800 North Capitol Street, NW Suite 565
Washington, District of Columbia 20002

RE: ***Comments of ACT | The App Association to PCLOB on its* Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act (FISA) *[Notice-PCLOB-2022-03; Docket No. 2022-0009 Sequence No. 3]***

ACT | The App Association submits these comments in response to the notice of the Privacy and Civil Liberties Oversight Board's (PCLOB) Oversight Project, which examines section 702 of the Foreign Intelligence Surveillance Act (FISA) in connection to privacy, surveillance, and counterterrorism.[1] We note that PCLOB's continued work in the privacy space, is timely, and the App Association appreciates the opportunity to provide commentary in response to this notice in anticipation of the December 2023 sunset date for section 702 and the upcoming public and congressional consideration of its reauthorization.

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. The App Association serves as a leading resource in the privacy space for thought leadership and education for the global small business technology developer community.[2] We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and usable guidance to ease the burden of compliance.[3] Further, we are committed to promoting proactive approaches to ensure end-user privacy and supporting privacy-by-design approaches that build trust.

Consumers and businesses who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer

---

[1] 87 Fed. Reg. 58393, Notice of the PCLOB Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act (FISA), available at https://www.federalregister.gov/documents/2022/09/26/2022-20415/notice-of-the-pclob-oversight-project-examining-section-702-of-the-foreign-intelligence-surveillance

[2] ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy Fellows (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/.

[3] See e.g., ACT | The App Association, General Data Protection Regulation Guide (May 2018), available at: https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf; What is the California Consumer Privacy Act (January 2020), available at: https://actonline.org/wp-content/uploads/What-is-CCPA.pdf.

community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. For this reason, we support the Administration's goal of ensuring the United States leads the world in responsible data practices and technologies, which are critical to our economic prosperity and national security. The PCLOB has a critical role in supporting U.S. competitiveness, privacy, and security in safeguarding that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.

As regulators from across key markets abroad continue to rush to regulate the digital economy, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face great barriers to bring novel products and services to market, slowing technological innovations to the pace of government approval. Yet, the American approach to privacy is a work in progress, with Federal sector-specific regulation of privacy, along with a patchwork of state-level laws and regulations, presents a very challenging scenario for a small business innovator. Ultimately, the App Association is supportive of a new federal privacy framework that will include critical features such as the preemption of differing privacy requirements by states, a clear and certain path to compliance, and protections against unauthorized access to data.[4]

While bipartisan work towards a new federal law continues, important steps have been accomplished to protect privacy while enabling the law enforcement and intelligence communities to access needed data. For example:

- Through the passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[5] later leading to the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime.[6] The App Association worked to advance the passage of the CLOUD Act, and it now provides a path forward for law enforcement and foreign governments to resolve conflict and ambiguity in data access laws by authorizing our government to enter bilateral agreements with other countries, enabling consumers to benefit from their home countries' due process protections wherever their data may be stored.
- The Administration, through negotiations with the European Commission, has created a new legal framework necessary to support transatlantic data flows while protecting privacy.[7] This new negotiated framework represents a critical mechanism for small businesses to legally transfer personal information from the European Union (EU) to the

[4] ACT | The App Association, "The 4 Ps of Privacy: What Small Businesses Need in a Privacy Bill" (September 13, 2022), https://actonline.org/2022/09/13/the-4-ps-of-privacy-what-small-businesses-need-in-a-privacy-bill/.

[5] Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018).

[6] https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force.

[7] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

U.S. This construct replaces the EU-U.S. Privacy Shield, which was a vital means for small businesses to legally transfer personal information from the EU to the U.S. before the Court of Justice of the European Union's struck it down in the *Schrems II* case.

In its examination of the U.S. government's intelligence gathering programs, we urge that PCLOB pay particular attention to the oversight mechanisms that promote forced localization and other arduous policies that can stifle digital platforms and hinder the global flow of information technology products and services, harming American information technology companies.[8] Companies expanding into new overseas markets, especially small businesses, increasingly face regulations that force them to build and/or use local data infrastructure. These data localization requirements seriously hinder imports and exports, as well as jeopardize an economy's international competitiveness and undermine domestic economic diversification. Small app developers often do not have the resources to build or maintain infrastructure in every country in which they do business, which effectively excludes them from global commerce.

The App Association urges PCLOB to center how the Oversight Project and its findings can impact small businesses as they continue to adopt privacy-enhancing technologies (PETs). App developers are already working to adopt and implement PETs in their products, services, and features in order to meet market and cybersecurity demands and build trust with consumers despite barriers to enter the international market. Here are a few examples of PETs that our members rely on every day:

- Data Minimization. App Association members design privacy protections into the products and services they offer from the earliest stages of design, and limit the collection of information to what is directly relevant and necessary to accomplish specific purposes in order to minimize risks for their customers as well as liabilities for themselves.
- Encryption. The App Association supports fully leveraging technical protection mechanisms including end-to-end encryption to protect data broadly, enabling key segments of the economy to function—from banking to national security to healthcare—by safeguarding access to, and the integrity, of data from unwanted interlopers. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. The importance of encryption to the app economy only heightened during the COVID-19 pandemic and the increased desire to perform traditionally offline functions in the digital space due to social distancing mandates. That's why we've been strong supporters of National Institute of Standards and Technology's (NIST) efforts to support the development of encryption technologies, as well as their leadership in advancing risk-based scaled approaches to cybersecurity management in the NIST Cybersecurity Framework (which includes an emphasis on encryption as a technical protection mechanism), while opposing legislation seeking to undermine end-to-end encryption, such as the Lawful Access to Encrypted Data Act or the EARN IT Act.
- On-Device Processing. Apps utilize on-device processing for certain sensitive features to ensure that no external processing occurs and that the company cannot see or access

[8] Allan Friedman, "Cybersecurity and Trade: National Policies, Global and Local Consequences," Brookings Institution Center for Technology Innovation, September 2013, accessed October 23, 2013, http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf.

the data. To share one key use case, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log in to apps using a scan of their face from the camera app. An app developer can choose integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[9]

- App Tracking Transparency. Even as federal lawmakers debate legislation that would put new guardrails around data-sharing practices in the digital economy, app developers comply with a growing number of platform-level restrictions on certain types of data sharing with third parties. For example, Apple's App Tracking Transparency (ATT) tool creates a simple solution to the opt-in/opt-out binary by presenting users with a just-in-time push notification asking if they want to permit third-party tracking that follows them outside of the app onto the open web or even other third-party apps. This type of engineering solution has so far evaded an easy resolution in the policy world but has markedly improved user privacy outcomes along the way.[10]
- Privacy Labeling. Over the past few years, the app marketplace has seen the gradual introduction of the "privacy nutrition label" concept. The contemporary version of these labels (drawing from more than a decade of scholarship with researchers proposing similar concepts in various forms)[11] aims to perform an imperative function: making app developers' privacy practices more understandable to the average consumer. Initial research demonstrates that many app developers welcome privacy nutrition labels as a convenient, efficient, and user-friendly way for them to demonstrate their privacy practices and see it as a major improvement from the previous practice of directing users to lengthy privacy policies for similar information.[12] Though we believe the app platforms could do a better job of assisting developers in the creation and maintenance of the label, we believe the concept will help to maintain trust in the app ecosystem in the long- un.

[9] Apple, "About Face ID advanced technology", September 14, 2021, https://support.apple.com/en-us/HT208108

[10] Estelle Laziuk, "iOS 14.5 Opt-in Rate - Daily Updates Since Launch", Flurry (May 25, 2021), available at https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[11] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/1572532.1572538.

[12] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3502012.

As the PCLOB considers questions it should explore, and recommendations it should consider making, in connection with its oversight project to examine the surveillance program operated pursuant to section 702 of FISA, the App Association recommend the following:

- PCLOB's continued activities are vital to President Biden's Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, under which PCLOB is designated to review intelligence community policies and procedures to ensure that they are consistent with the Executive Order and to conduct an annual review of the European Union-U.S. Data Privacy Framework's redress process, including to review whether the intelligence community has fully complied with determinations made by the Civil Liberties Protection Officer in the Office of the Director of National Intelligence and the new Data Protection Review Court. PCLOB's efforts under the Executive Order are essential to providing the trust and transparency needed to make the new transatlantic framework functional.
- We urge the PCLOB and Congress to further advance transparency in the digital ecosystem while avoiding disruptions to law enforcement and intelligence investigations. The U.S. government can do this by permitting companies to disclose the number of government orders, and anonymized data capturing the number of individuals impacted, under Section 215 of the USA Patriot Act, Section 702 of the FISA Amendments Act, and other national security statutes; and declassifying Foreign Intelligence Surveillance Court (FISC) opinions where appropriate. Such steps would enhance public transparency and will build trust in U.S. government processes and programs. The PCLOB is well positioned to evaluate the state of transparency and recommend new ways to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties.
- PCLOB can and should support the role of strong encryption in protecting privacy through its recommendations, and should work with U.S. government to prevent the recycling of flawed proposals for mandated vulnerabilities in encryption algorithms.[13] This effort should be done in coordination with, and in support of, the National Institute of Standards and Technology's cryptographic standards and guidelines.[14]
- PCLOB should support the development of new bilateral agreements authorized by the Clarifying Lawful Overseas Use of Data (CLOUD) Act to allow each country's investigators to gain better access to vital data to combat serious crime consistent with privacy and civil liberties standards. CLOUD Act-driven frameworks give law enforcement the tools they need to keep us safe and small businesses the legal clarity they need to keep customers' data protected.
- PCLOB should support the private sector's use of data minimization practices that mitigate privacy risks for their customers in alignment with industry norms (e.g., platform practices described above) and in coordination with other U.S. government agencies.

[13] *E.g.*, https://actonline.org/2015/07/29/fbi-backdoor-means-weaker-encryption-and-data-breaches/.

[14] https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines.

The App Association appreciates PCLOB's consideration of the above views. We urge PCLOB to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matthew Schwartz
Public Policy Associate

Leanna Wade
Public Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130

PUBLIC SUBMISSION

As of: 11/8/22, 8:38 AM
Received: November 03, 2022
Status: Draft
Tracking No. la1-d7it-ifep
Comments Due: November 04, 2022
Submission Type: API

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0026
Comment on FR Doc # 2022-20415

Submitter Information

Email: kruane@wikimedia.org
Organization: Wikimedia Foundation

General Comment

The Wikimedia Foundation (Foundation) submits these comments to the Privacy and Civil Liberties Oversight Board (PCLOB) as it conducts its oversight project of Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the surveillance program conducted thereunder (Docket No. 2022-0009). The review of Section 702 could not be more timely, considering Section 702's sunset date in December of 2023 and Congress' planned debate surrounding the statute's reauthorization. The Wikimedia Foundation is an organization dedicated to privacy and deeply concerned about overbroad mass government surveillance. The Foundation welcomes PCLOB's review and hopes the Board at a minimum will recommend additional safeguards and limitations to the surveillance conducted under Section 702.

Attachments

Comments of the Wikimedia Foundation to the PCLOB Section 702 Oversight Process 2022-0009

Comments of

The Wikimedia Foundation

In the Matter of

PCLOB Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act

DOCKET ID: PCLOB-2022-0009

November 3, 2022

Introduction

The Wikimedia Foundation (Foundation) submits these comments to the Privacy and Civil Liberties Oversight Board (PCLOB) as it conducts its oversight project of Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the surveillance program conducted thereunder (Docket No. 2022-0009). The review of Section 702 could not be more timely, considering Section 702's sunset date in December of 2023 and Congress' planned debate surrounding the statute's reauthorization. The Wikimedia Foundation is an organization dedicated to privacy and deeply concerned about overbroad mass government surveillance. The Foundation welcomes PCLOB's review and hopes the Board at a minimum will recommend additional safeguards and limitations to the surveillance conducted under Section 702.

Statement of Interest

The Foundation is a charitable, nonprofit organization which hosts, and provides the technical infrastructure for twelve (12) online projects dedicated to creating and providing free knowledge to a worldwide audience. The Foundation hosts global websites that invite contributions from people all over the world and strive toward sharing the sum of human knowledge. In the course of fulfilling that mission, the contributors to the projects it hosts (i.e., Wikimedians) and the Foundation's staff communicate with one another as well as with government officials, journalists, activists, and civil society across borders.

These communications are deeply impacted by the surveillance programs operated under Section 702. We take burdensome and costly measures to attempt to protect our communications from surveillance. Because the Foundation and the community engaged in creating the projects cannot engage in domestic or international advocacy without considering the surveillance to which we might be subject, we are cautious about the content of our communications, and may edit messages or even choose to travel and communicate in person. Mass surveillance, specifically Upstream surveillance, one of the surveillance programs operated pursuant to Section 702, also reduces the likelihood that journalists, activists, experts, and others who might want to contribute their knowledge to Wikimedia projects will do so, thereby further impeding the Foundation's mission.

Research substantiates our concerns. Jonathon W. Penney of York University in Toronto, Canada, released the first original empirical study of the regulatory chilling effects associated with online government surveillance. The study, "Chilling Effects: Online Surveillance and Wikipedia Use,"[1] successfully quantified the impact of such surveillance on Wikipedia users and articles, and web traffic data more generally, resulting from the June 2013 National Security Agency (NSA) surveillance program revelations. Penney chose to focus on Wikipedia because it is an "essential source of information and knowledge online" and an "important public tool in promoting collective understanding, decision-making, and deliberation." Therefore, as he

[1] Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use,* 31 Berkeley Tech, L.J. Vol. 1, 117 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

argues, any demonstrated chilling effect on Wikipedia users has broader implications for the global free knowledge movement and democratic processes.

Because mass surveillance impedes our mission by interfering with the Foundation's relationship with the community of volunteers, imposing a chilling effect on the development and consumption of the free knowledge projects we host, and generally invading privacy and harming human rights, the Foundation has sued the NSA in federal court, challenging the legitimacy and constitutionality of Upstream surveillance. The Foundation has petitioned the Supreme Court to hear the case.

Wikimedia's Questions for PCLOB's Oversight Project

The Foundation attached as Annexure I a list of questions we urge the PCLOB to address in its review. The Foundation attached as Annexure II a list of recommendations for changes to the Section 702 program that we urge the PCLOB to make to both the executive branch and to Congress as it reconsiders Section 702 in 2023.

Thank you for the opportunity to participate in this process. Please do not hesitate to reach out to Kate Ruane, Lead Public Policy Specialist for the United States, kruane@wikimedia.org, with any questions.

Sincerely,

The Wikimedia Foundation

.

Annexure I

Questions:

- Until 2017, the NSA used Upstream surveillance to collect communications to and from targeted selectors as well as communications that were merely "about" targeted selectors. These "about" communications were not necessarily from surveillance targets, but may have simply mentioned the selectors in their text. This practice, known as "about" collection, involved the NSA searching the entire contents of international communications and then retaining those that contained any mention of the NSA's thousands of selectors. The intelligence community announced that it would cease "about" collection in 2017, after the FISA Court addressed serious violations of court-imposed rules.

  - How, if at all, has the end of "about" collection in 2017 changed the process for collecting communications via the Upstream surveillance program?

- Recently, the United States (U.S.) issued the Declaration for the Future of the Internet. The Wikimedia Foundation commended the signatory governments for their strong support for a free, open, and interoperable internet, but noted that many of the countries had failed to always live up to the principles the document espoused. In the Declaration, the government pledged that human rights should be respected online and stated that it would refrain from using unlawful surveillance that does not align with international human rights principles.

  Has Upstream surveillance or any other surveillance practice purportedly authorized by section 702 ever undergone a Human Rights Impact Assessment?

  - If so, will the assessment be made public?

  - If not, why not and will the intelligence community consider conducting such an assessment now in keeping with the pledge made in the Declaration for the Future of the Internet?

  - What chilling effect do the surveillance programs authorized by Section 702 have upon internet usage and free expression, including the abilities to both send and find information? Has any component of the United States intelligence community ever conducted a study of the impacts of its surveillance practices on free expression domestically or internationally?

- The Wikimedia Foundation is committed to protecting the privacy of the communities that create the projects the Foundation hosts. These communities are located all over the

world, including in places where contributing to the projects can lead to great personal risk, heightening the importance of ensuring privacy on Wikimedia projects. In the White House's recent executive order implementing a new European Union-United States Data Privacy Framework to replace the Privacy Shield framework struck down by the Court of Justice for the European Union (CJEU), the White House acknowledged that all people, regardless of their country of residence, have a right to privacy. Yet Section 702 surveillance programs authorize suspicionless surveillance of any foreign national.

In keeping with the new Data Privacy Framework, will the PCLOB recommend that the government narrow the scope of foreign nationals that could be targets of Section 702 surveillance?

Annexure II

Recommendations

- The PCLOB should recommend that the Section 702 surveillance programs undergo a Human Rights Impact Assessment, not only with respect to the rights of U.S. citizens, but also taking into account the impact on foreign citizens' rights, if that has not already happened. This recommendation aligns strongly with the Administration's commitments under the Declaration for the Future of the Internet. It would also help to ensure the protection of the human rights of Wikimedians around the globe.

- The PCLOB should recommend that the government follow the recommendations any human rights impact assessment produces.

- The PCLOB should recommend narrowing the scope of individuals that can be targeted for surveillance under Section 702 to "foreign powers" and "agents of foreign powers." Following this recommendation will significantly narrow the number of foreign nationals and people within the United States whose communications could be swept up in suspicionless surveillance under Section 702. These additional safeguards will support the exchange of free knowledge and the creation of reliable information on the internet.

- The PCLOB should recommend imposing additional restrictions on the retention of information collected under Section 702. Currently, information collected under Section 702 can be retained as long as five years by default. The PCLOB should recommend that the retention period be shortened to two years and that information cannot be retained past that period unless the government can demonstrate that the information is foreign intelligence information. As the Foundation has said in previous comments to the US government, data minimization is good cybersecurity practice and less data held means less data that could be used improperly.

- The PCLOB should recommend expanding the role of the amicus before the Foreign Intelligence Surveillance Court (FISC) in cases that raise heightened concerns for privacy, free expression, racial and ethnic bias, political activities, religious freedom, and academic freedom. The amicus is currently the only representative the public has in the review process for Section 702 surveillance programs. It is imperative to ensure the public has a representative in the review and authorization of Section 702 programs in all circumstances that create a significant risk to human rights.

- The PCLOB should recommend promptly identifying and purging the communications of U.S. citizens and people within the United States. If adopted, this recommendation would primarily benefit the privacy rights of people located in the United States and U.S. citizens but, by simply reducing the number of communications held under Section 702, would also benefit the privacy of any of the people involved in the communications.

- The PCLOB should recommend ending warrantless searches of Section 702's database for the communications of people located within the United States—known as "backdoor" searches. These searches are specifically designed to circumvent critical Fourth Amendment constitutional protections and are highly controversial. Moreover, the government's own transparency reports have revealed that the Federal Bureau of Investigation (FBI) frequently fails to abide by existing requirements for obtaining this data. The only solution is to limit the FBI's access to this database in the first instance.

PUBLIC SUBMISSION

As of: 11/8/22, 8:41 AM
Received: November 04, 2022
Status: Draft
Tracking No. la2-rges-44cd
Comments Due: November 04, 2022
Submission Type: API

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0027
Comment on FR Doc # 2022-20415

Submitter Information

Email: jlaperruque@cdt.org
Organization: The Center for Democracy & Technology

General Comment

See attached file(s)

Attachments

CDT Comment to PCLOB on FISA Section 702

CENTER FOR DEMOCRACY & TECHNOLOGY

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

November 4, 2022

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

CENTER FOR DEMOCRACY & TECHNOLOGY

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

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

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

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

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

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

[21] For full verbatim text of permissible purposes, see, "Signals Intelligence EO."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

[34] *FISC October 2018 Opinion*.

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

CENTER FOR
DEMOCRACY
& TECHNOLOGY

***

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

Thank you,

Jake Laperruque

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

PUBLIC SUBMISSION

As of: 11/8/22, 8:43 AM
Received: November 04, 2022
Status: Draft
Tracking No. la2-z3u8-ukks
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0028
Comment on FR Doc # 2022-20415

Submitter Information

Email: mnohr@aclu.org
Organization: American Civil Liberties Union

General Comment

See attached file(s)

Attachments

PCLOB Section 702 Comment - 4 Nov. 2022

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

PUBLIC SUBMISSION

As of: 11/8/22, 8:44 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-06qx-wrio
Comments Due: November 04, 2022
Submission Type: API

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0029
Comment on FR Doc # 2022-20415

Submitter Information

Name: Adonica Blackston
Address:
Alexandria, VA, 22305
Email: ajblackston@uchicago.edu
Phone: (773) 257-3932

General Comment

There is no way to balance the Civil Rights of US Citizens, specifically the right to Privacy under the Fourth Amendment, with the zealous pursuits of police authorities. They will always argue that the desired “End” justifies the means. No matter how much damage, destruction of lives, or people killed, when individuals seeking career advancement or just plain old recognition want to force an issue, they will. I hope we can all agree that neither career advancement nor recognition has anything to do with National Security or our protection from terrorists.

With the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA), you will be facilitating a means to continue to turn our police authorities into our terrorists. With a Sting Ray, Leon Newsome first held me under electronic surveillance without a warrant from August 2002 to June 2004, denying me the ability to become gainfully employed, demonstrating an egregious abuse of his position of authority and gross misconduct.

As documented by the Washington Post, “Democracy Dies In Darkness,” when we choose to look the other way and allow our police authorities to skirt the Constitution. In an Exclusive Investigation conducted from 2010 to 2020, the Washington Post reported, “More than $1.5 billion has been spent to settle claims of police misconduct involving thousands of officers repeatedly accused of wrongdoing.”

With the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act in 2023, these numbers will get worse.

The hidden billion-dollar cost of repeated police misconduct
https://www.washingtonpost.com/investigations/interactive/2022/police-misconduct-repeated-settlements/?itid=lb_more-on-policing-in-america_4

Attachments

Renting GM Vehicles

GMC Cargo Van - Harrassment

PUBLIC SUBMISSION

As of: 11/8/22, 8:46 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-2sbp-sdrh
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0030
Comment on FR Doc # 2022-20415

Submitter Information

Email: goiteine@brennan.law.nyu.edu
Organization: Brennan Center for Justice at NYU School of Law

General Comment

See attached file

Attachments

Brennan Center Comments to PCLOB on Section 702 11-4-22

Comments to the Privacy and Civil Liberties Oversight Board re:
Section 702 of the Foreign Intelligence Surveillance Act

submitted by:

The Brennan Center for Justice at NYU School of Law

November 4, 2022

Elizabeth Goitein
Senior Director
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue, NW
Eleventh Floor
Washington, DC 20036

Introduction

Congress's goal when it enacted Section 702 of the Foreign Intelligence Surveillance Act ("FISA") in 2008 was to give our government more powerful tools to address terrorist threats. In writing the law, however, Congress did not expressly limit Section 702 surveillance to that purpose. Instead, Congress gave significant discretion to the executive branch and the Foreign Intelligence Surveillance Court ("FISA Court" or "FISC"), trusting them to ensure that the law was implemented in a manner consistent with its objective. For instance, Congress allowed the government to target almost *any* foreigner overseas, counting on intelligence agencies to focus their efforts on those who pose a threat to our country. Congress also did not specify what minimization should look like, leaving that to the agencies and the judges of the FISA Court.

Rather than tailoring its surveillance as Congress expected, the executive branch has taken full advantage of the leeway provided in the statute. Instead of simply acquiring the communications of suspected terrorists or foreign powers overseas, the government is scanning nearly all of the international communications that flow into and out of the United States via the Internet backbone, and is acquiring hundreds of millions of these communications each year. This surveillance inevitably pulls in vast amounts of Americans' calls, texts, and e-mails.

Section 702 also has fallen victim to mission creep. A statute designed to protect against foreign threats to national interests has become a major source of warrantless access to Americans' data and a tool for ordinary domestic law enforcement. The most recent statistical transparency report issued by the Office of the Director of National Intelligence ("ODNI") revealed that the FBI conducted more than *three million* searches of Section 702 data in 2021 for the purpose of finding Americans' communications. This outcome is contrary, not only to the original intent of FISA, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

Perhaps most disturbingly, with every new release of a FISA Court opinion, it becomes increasingly clear that the rules designed to protect Americans' privacy are being honored in the breach. Agencies have repeatedly, and in some cases systemically, violated statutory or court-ordered limitations on collection, retention, querying, and dissemination. Some of these violations have rendered the operation of the program unconstitutional. When Congress last reauthorized Section 702, it sought to shore up privacy protections by requiring FBI agents to obtain a warrant before accessing Section 702 data about Americans in certain investigations. According to the government's own reports, the FBI has *never* complied with this requirement.

The concerns with Section 702 apply with even greater force to surveillance under Executive Order (EO) 12333, which is subject to far fewer constraints. Generally speaking, Section 702 applies when the collection takes place inside the United States or from a U.S. company, while Executive Order 12333 applies when the collection takes place overseas. In the digital era, however, this distinction has become artificial. Overseas surveillance can have just as great an impact on Americans' privacy as domestic surveillance, if not greater. Reforms to Section 702 will have limited effect if EO 12333 surveillance continues to be carved out of foreign intelligence surveillance legislation.

As Congress considers reauthorization of Section 702, the Privacy and Civil Liberties Oversight Board should use its authority in two ways. First, following up on its highly effective 2014 investigation into the workings of Section 702, the PCLOB should undertake three projects designed to elicit key information. The first project would entail working with the intelligence community to develop an estimate of how many communications involving U.S. persons are "incidentally" collected under Section 702. The second project would be an investigation of the government's targeting decisions under Section 702, with an eye toward making recommendations for narrowing the criteria for targeting. The third project would be an examination of how Section 702 is used for cybersecurity purposes, in light of indications that investigations into cybersecurity threats involve particularly broad surveillance.

Second, PCLOB should recommend reforms to Section 702. The core of Section 702 is the ability it gives the government to obtain the communications of foreign powers and suspected foreign terrorists without obtaining a warrant. There are several potential reforms that would leave this core intact, while adding badly needed protections for law-abiding citizens of this country and others. These reforms fall into the following categories: (1) narrowing the scope of Section 702 collection; (2) shoring up protections for "incidentally" acquired U.S. person information by requiring agencies to obtain a warrant, court order, or subpoena before running U.S. person queries of Section 702 data, and by placing stricter limits on retention; (3) modernizing FISA by establishing basic rules and requiring FISA Court oversight for EO 12333 surveillance; and (4) increasing transparency and accountability in the operations of Section 702 and EO 12333.

I. Section 702: A Massive Expansion in the Scope of Foreign Intelligence Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a decade ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.[1]

But instead of increasing safeguards for Americans' privacy as technology advances, the law has evolved in the opposite direction since 9/11. In its zeal to bolster the government's powers to conduct surveillance of foreign threats, Congress has amended surveillance laws in ways that increasingly leave Americans' information outside their protective shield (the USA FREEDOM Act being the notable exception). Section 702 is a particularly striking example.

Before 2007, if the NSA, operating domestically, sought to wiretap a foreign target's communications with an American inside the U.S., it had to show probable cause to the FISA Court that the target was a foreign power — such as a foreign government or terrorist group —

[1] *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 19–21 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.[2]

Executive officials have often argued that Section 702 was necessary to address changes in communications technology and "modernize" FISA. They note that, before 2007, the law required the NSA to obtain a FISA Court order to collect certain foreign-to-foreign e-mails stored by internet service providers inside the United States — something Congress almost certainly did not intend when it originally passed FISA. Section 702, however, went much further than was necessary to correct that problem. It did not simply allow the warrantless collection of foreign-to-foreign e-mails inside the United States; it allowed the warrantless collection of communications, both stored and in transit, between foreign targets and Americans. This state of affairs differs fundamentally from the regime Congress designed in 1978.[3]

Another critical change is that the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas.[4] The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly

---

[2] *See* 50 U.S.C. § 1881a.

[3] Some executive branch officials have suggested that Congress in 1978 intended to regulate surveillance only for purely domestic communications. They note that FISA required the government to obtain an individual court order when collecting any communications involving Americans that traveled by wire, but required an individual court order to obtain satellite communications only when all of the communicants were inside the U.S. Asserting that wire technology was the norm for domestic calls, while most international communications were carried by satellite (and were thus "radio communications"), they infer that Congress intended to require the government to obtain an order when acquiring purely domestic communications, but not when obtaining communications between foreign targets and Americans. This intent, they argue, was undermined when fiber-optic cables later became the standard method of transmission for international calls.

The problem with this theory is two-fold. First, it would have been quite simple for Congress to state that FISA orders were required for purely domestic communications and not for international ones. Instead, Congress produced an elaborate, multi-part definition of "electronic surveillance" that relied on particular technologies rather than the domestic versus international nature of the communication. Second, contrary to the factual premise of this theory, the available evidence indicates that one third to one half of international communications *were* carried by wire back in 1978. David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 3 (Brookings Inst., Working Paper, 2007), *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.pdf.

A more plausible explanation for the original FISA's complex scheme was put forward by David Kris, a former head of the Justice Department's National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day. *Id.* at 13–23. Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute's coverage of NSA's operations "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans." S. REP. NO. 95-701, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004.

[4] 50 U.S.C. § 1881a(b).

increases the number of communications involving Americans that are subject to acquisition — as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the universe of available communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[5] The inclusion of "about" in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the "selectors" associated with the target (e.g., the target's e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention Vladmir Putin, ISIS, or a wide array of other individuals and groups who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of so-called "abouts" collection.

The NSA's failure to comply with minimization rules for "abouts" collection (discussed later in these comments), which delayed the FISA Court's approval of the program in 2016, led the agency to stop the practice in April of 2017.[6] When Congress reauthorized Section 702 in early 2018, it required the government to provide 30 days' notice if it intended to restart "abouts" collection. There is no public indication that this has happened, and no FISA Court decision approving the reinstitution of "abouts" collection has been released. However, the door remains open to the NSA resuming this practice in the future.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify, on a program-wide basis, that acquiring foreign intelligence is a significant purpose of the collection.[7] FISA's definition of foreign intelligence is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[8] This could encompass everyday discussions of current events. A conversation between friends or colleagues about trade between the U.S. and China "relates to the conduct of foreign affairs," as does a conversation about whether the U.S. should do more to support Ukraine. Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether.[9] Finally, the statute requires the FISA Court to accept the government's certifications under Section 702 as long as they contain the required elements.[10] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

---

[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://www.pclob.gov/library/702-report.pdf.

[6] Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets,* N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

[7] 50 U.S.C. § 1881a(g)(2)(A)(v).

[8] 50 U.S.C. § 1801(e)(2).

[9] *In re* Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).

[10] 50 U.S.C. § 1881a(i)(3)(A).

Going forward, the expansive scope of Section 702 surveillance might be somewhat constrained by President Biden's recent executive order establishing new rules for the collection of signals intelligence. The order sets forth twelve legitimate objectives for signals intelligence collection, [11] which are more specific than the general language contained in FISA's definition of "foreign intelligence information." However, these purpose-based limitations do not necessarily translate into constraints on the scope of surveillance. For instance, one of the permissible purposes is to protect against threats to cybersecurity — a goal that could in theory justify constant monitoring of any and all Internet networks. Furthermore, the order permits the president to add to the list of objectives, and to do so secretly if the president determines that disclosure of the new objective(s) would harm national security.

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[12] The second type of Section 702 surveillance is "PRISM collection," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.[13]

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011 — the last year for which such information is publicly available.[14] Because agencies generally may store Section 702 data for at least five years, a yearly intake of 250 million communications would result in at least 1.25 billion communications residing in government databases at any given time. The actual number is almost certainly higher, as the 250 million figure does not include telephonic communications, and the number of targets today is likely much larger than in 2011. Since 2013, when the government first began reporting the number of Section 702 targets, that number has risen from 89,138[15] to 232,432.[16]

In short, under Section 702, the rules for U.S.-based surveillance of foreigners overseas were rewritten to greatly loosen restrictions on targeting and to remove any individualized oversight of targeting decisions by the FISA Court. It is no wonder that this form of surveillance has ballooned, with hundreds of millions — if not billions — of communications collected each year.

---

[11] Exec. Order 14086, § 2(b)(i)(A), 87 Fed. Reg. 62283–4 (Oct. 7, 2022).
[12] PCLOB 702 REPORT, *supra* note 5, at 36–41.
[13] *Id.* at 33–34.
[14] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[15] OFF. DIR. NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013 (Jun. 2014), *available at* https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.
[16] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2021 (Apr. 2022), *available at* https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2291-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2021.

This mass surveillance disregards the privacy rights of law-abiding foreign nationals — and that, in turn, is causing economic headaches for the United States. On two occasions, the Court of Justice for the European Union (CJEU) has struck down agreements between the United States and the European Union governing the transfer of data between EU and U.S. companies.[17] One major reason for the court's rulings is that Section 702 provides the U.S. government with ready access to EU citizens' data in the hands of U.S. companies, in contravention of European law. President Biden's recent executive order was issued to pave the way for a new data-transfer agreement, but observers doubt whether that order includes sufficient constraints on surveillance to satisfy the CJEU.[18] More than 5,000 U.S. companies rely on a U.S.-EU data-sharing agreement to do business.[19]

Beyond these economic woes, mass surveillance of foreigners overseas has inevitable and significant impacts on Americans' privacy, as discussed in the next Part.

II. The Impact of Section 702 on Americans' Privacy

Because the "target" of Section 702 surveillance must be someone reasonably believed to be a foreigner overseas, the collection of Americans' communications with those targets is described as "incidental," and the statute requires "minimization" of those Americans' information. These are terms of art that have particular legal meanings. Legal and policy defenses of Section 702 in its current form rely heavily on these terms and concepts.

The impact on Americans' privacy, however, does not. If the government is collecting tens of millions of Americans' communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or theft, it matters little — from a practical perspective — that their initial acquisition was "incidental," or that the procedures allowing them to be kept and stored include "minimization" in their title. And if FBI agents are searching this data for Americans' communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not "targets."

The government has refused to provide any information that would give Congress and Americans a sense of the volume of Americans' communications being collected and stored. We do know, however, that the rules for "minimization" allow agencies to keep this "incidentally" acquired data for five years or longer. We also recently learned that the FBI searches through Section 702 data for Americans' communications literally millions of times each year — and that

---

[17] *See* Case C-311/18, Data Protection Commissioner v. Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4231279; Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

[18] American Civil Liberties Union, *To Make Real Progress, ACLU Calls on Congress to Enact Meaningful Surveillance Reform* (Oct. 7, 2022), https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.

[19] *See* Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (Jul. 16, 2020), https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html.

it has never complied with the statutory warrant requirement that applies to some of these searches.

A. How Many Americans' Communications Does the NSA Collect?

Section 702 surveillance obtains the communications, not only of foreign targets, but of any Americans who are in contact with them. The number of Americans' communications thus collected is likely quite large: If only one out of every 250 communications involves an American, that would still add up to more than one million communications a year. But there is no official public information on how many Americans' communications are in fact swept up in Section 702 surveillance.

In 2011, Senators Ron Wyden and Mark Udall asked the Inspectors General of the Intelligence Community and the NSA to come up with a public estimate of this number.[20] They were later joined in this call by several other senators from both parties.[21] The Inspectors General responded that generating an estimate would itself violate Americans' privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed.[22] In October of 2015, however, a coalition of more than thirty advocacy groups — including many of the nation's most prominent privacy organizations — sent a letter to the Director of National Intelligence (DNI) urging that the NSA go forward with producing an estimate.[23] The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy.

In April 2016, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.[24] Eight months later, the members wrote again to memorialize their understanding, in light of interim conversations and briefings, that the DNI would provide the requested estimate "early enough to inform the debate," and with a target date of January 2017.[25] By all private and public accounts, the intelligence community was close to launching its count at the beginning of 2017.

---

[20] *See* Letter from Senators Ron Wyden and Mark Udall to The Honorable I. Charles McCullough III, Inspector General of the Intelligence Comm., and Dr. George Ellard, Inspector General, Nat'l Sec. Agency (May 4, 2011), *available at* https://www.wyden.senate.gov/download/?id=CE360936-DFF9-4273-8777-09BF29565086&download=1.

[21] *See* Ron Wyden, *Senators Seek Answers from DNI on How Many of Americans' Communications Have Been Monitored* (Jul. 12, 2012), https://www.wyden.senate.gov/news/press-releases/senators-seek-answers-from-dni-on-how-many-of-americans-communications-have-been-monitored.

[22] Letter from The Honorable I. Charles McCullough, III, Inspector General of the Intelligence Comm., to Senators Ron Wyden and Mark Udall (June 15, 2012), *available at* https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1.

[23] Letter from Brennan Ctr. for Justice, et al., to James Clapper, Dir. Nat'l Intelligence (Oct. 29, 2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[24] Letter from Rep. John Conyers, Jr., et al., to James Clapper, Dir. Nat'l Intelligence (Apr. 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

[25] *See* Press Release, U.S. House Comm. on the Judiciary Democrats, Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance (Dec. 16, 2016), *available at* https://democrats-judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance.

Following the change in administration, however, the government backed down from this commitment. In June 2017, then-Director of National Intelligence Dan Coats testified before Congress that it was technologically infeasible to generate an estimate without invading Americans' privacy — the very same claim that was addressed and seemingly resolved under the previous administration.[26] The government retreated to its 2012 assertion that there is no automated way to assess whether a particular communication is to or from an American.

The problem with this claim is that the NSA can, and routinely does, make such an assessment when it conducts upstream surveillance. The FISA Court has held that the Constitution requires the government to take certain steps to minimize the acquisition, retention, and searching of wholly domestic communications. One of these steps, as the PCLOB reported in 2014, is the NSA's use of IP addresses and "comparable technical means" to filter out domestic communications when conducting upstream surveillance of Internet transactions.[27] Both the NSA and the FISA Court consider this method of identifying the domestic-versus-foreign status of communicants sufficient for purposes of complying with the Constitution. If it is sufficient for that purpose, it is certainly adequate to give Congress and the public a rough sense of how Section 702 collection impacts Americans.

In addition, there should be no difficulty in generating an estimate of how many Americans' telephone calls are collected: The government can simply use the country code as a proxy. The method is not perfect — a cell phone's country code does not always correspond with the location or nationality of the user — but again, lawmakers are seeking a rough estimate, not an exact count.

Stored e-mails, obtained through the PRISM program, are admittedly a harder case. However, computer scientists Jonathan Mayer and Anunay Kulshrestha of Princeton University have proposed a method that would leverage information in communications providers' possession, using encryption at various stages in the process to restrict the information actually visible to the providers and to the government.[28] If that fails, the privacy community is unanimous in its conclusion that the NSA should perform a one-time limited sampling of collected communications, under conditions (such as the immediate deletion of the communications after review) that would minimize the privacy intrusion.[29]

It is worth noting that the government maintained for many years that it could not track the number U.S. person queries the FBI performed on Section 702 data, in part because doing so would require an added intrusion into the query subjects' privacy. Based on this representation, Congress excluded the FBI from a reporting requirement imposed on other agencies. In 2018, however, Congress required the FBI to keep records of its U.S. person queries, and when the FBI

---

[26] Dustin Volz, *NSA Backtracks On Sharing Number of Americans Caught in Warrant-less Spying*, REUTERS (Jun. 12, 2017), http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B.
[27] *See* PCLOB 702 REPORT, *supra* note 5, at 38.
[28] Anunay Kulshrestha & Jonathan Mayer, *Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum* (USENIX Sec. Symposium, 2022), *available at* https://www.usenix.org/system/files/sec22-kulshrestha.pdf.
[29] *See* Letter from Brennan Ctr. for Justice, et al., to James Clapper, *supra* note 23.

failed to do so, the FISA Court ordered it to comply.[30] In 2022, the ODNI's annual statistical transparency report included the number that the FBI had claimed it could not produce.[31]

If the government is truly incapable of ascertaining, even roughly, how many Americans' communications it is collecting, that fact is in itself alarming. Regardless of whether it is lawful, the "incidental" collection of Americans' communications has real and significant effects on privacy — particularly when (as discussed below) that information can be stored for years, searched, and used in legal proceedings. The government cannot simultaneously assure the public that the impact of Section 702 surveillance on Americans' privacy is minimal, while also maintaining that it has no idea — and no way to discover — how many Americans' communications it is acquiring and storing.

B. Minimization and Its Loopholes

Minimization procedures are intended to mitigate the effects of "incidental" collection. The concept behind minimization is fairly simple: The interception of Americans' communications when targeting foreigners is inevitable, but because such interception would otherwise require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[32] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[33]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its PRISM collection with the FBI, the CIA, and (as of April 2017) the National Counterterrorism Center (NCTC).[34] All four agencies generally may keep unreviewed raw data — including data about U.S. persons — for

---

[30] [Redacted], 402 F. Supp. 3d 45, 66–73 (FISA Ct. 2018).
[31] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 21.
[32] 50 U.S.C. § 1801(h)(1).
[33] 50 U.S.C. § 1801(h)(3).
[34] WILLIAM BARR, U.S. DEP'T OF JUSTICE, 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(c) (Sept. 16, 2020) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Minimization%20Procedures_10.19.2020.pdf.

five years after the certification expires;[35] they also can seek extensions from a high-level official,[36] and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications that "reasonably appear[]…to contain secret meaning."[37] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[38]

If the NSA discovers U.S. person information that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[39] The NSA, however, interprets this requirement to apply only if the NSA analyst determines "not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need."[40] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[41]

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews U.S. person information and *does not identify it* as foreign intelligence information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[42] A similar rule applies to the NCTC.[43]

---

[35] *Id.* at § 4(c)(1)-(2) (2020); WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION 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.b (Oct. 19, 2020) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Minimization%20Procedures_10.19.2020.pdf; WILLIAM BARR, U.S. DEP'T OF JUSTICE, 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. 16, 2019) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_CIA%20Minimization%20Procedures_10.19.2020.pdf; WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE 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 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NCTC%20Minimization%20Procedures_10.19.2020.pdf.

[36] PCLOB 702 REPORT, *supra* note 5, at 60; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § B.2.a.

[37] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 7(a)(1).a; FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § I.4; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at § 3.c.

[38] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at §§ 6(a)(1), 7(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.A.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at §§ 3.a, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § B.3.

[39] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at §§ 4(b)(1), 4(c).

[40] PCLOB 702 REPORT, *supra* note 5, at 62.

[41] *Id.*

[42] FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.D.4.c.

[43] [Redacted], at 40 (FISA Ct. Apr. 26, 2017), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

If any of the four agencies — all of which have access to raw data — disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[44]

In short, the NSA routinely shares raw Section 702 data with the FBI, CIA, and NCTC; and the agencies' minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are "minimized" under any common sense understanding of the term.

C. Back Door Searches

Perhaps the most glaring failure of "minimization" is the fact that all four agencies are permitted to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans' communications.[45] This practice, commonly known as "back door searches," is both constitutionally suspect and at odds with the stated purpose and design of the statute.

If the government wishes to obtain an American's communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after showing probable cause that the target is an agent of a foreign power. If the government wishes to obtain an American's communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on "reverse targeting" — i.e., targeting a foreigner overseas when the government's intent is to target "a particular, known person reasonably believed to be in the United States." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans.

And yet, immediately upon obtaining the data, all four agencies may sort through it looking for the communications of particular, known Americans — the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans' communications absent a significant foreign intelligence purpose, the FBI may — and, "with some frequency,"[46] does — search the Section 702 data for Americans' communications to use in criminal proceedings having no foreign

---

[44] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 7(b); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § IV.A.1–2; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § D.1–2. In addition, the FBI may disseminate unminimized Section 702 data to the NSA, CIA, and in some cases the NCTC. FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § IV.E.

[45] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 4(b)(4); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.D.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at § 4; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § C.1.

[46] PCLOB 702 REPORT, *supra* note 5, at 59.

intelligence dimensions whatsoever.[47] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment's warrant requirement.

For years, the FBI resisted calls to disclose how many backdoor searches it performs each year. But after Congress and the FISA Court forced the FBI to track those queries, the government lost its excuse to withhold the number. In 2022, the ODNI's annual statistical transparency report revealed that the FBI had conducted up to *3.4 million* U.S. person queries in 2021 alone.[48] The report notes that the figure likely overstates the number of Americans affected, in part because there could be multiple searches relating to a single individual. But even if the figure is off by an order of magnitude, that still means that every day, nearly a thousand Americans are subject to a warrantless search for their personal communications.

Indeed, on some days, that number is much higher. The FBI has adopted a practice of "batch queries," in which it runs hundreds or thousands of queries under a single justification. In March 2017, against the advice of its Office of General Counsel, the FBI performed a batch query for 70,000 people — most of whom were presumably U.S. persons, given that the targets of the query were people with access to FBI facilities.[49]

In the past, some have defended back door searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. This legal defense entirely misses the point. The staggering figure of 3.4 million U.S. person queries per year,[50] even with all the government's caveats, makes clear that there is nothing "incidental" about Section 702's impact on Americans. Warrantless access to Americans' communications has become a core feature of a surveillance program that purports to be solely foreign-focused.

In any event, the argument that Section 702 data may lawfully be used for any purpose ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: As Judge Bates of the FISA Court has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[51]

---

[47] ROBERT S. LITT, OFF. DIR. NAT'L INTELLIGENCE, PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: AN OVERVIEW OF INTELLIGENCE COLLECTION (July 18, 2013), https://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

[48] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 21.

[49] [Redacted], 402 F. Supp. 3d 45, 76 (FISA Ct. 2018).

[50] Although the FBI is by far the most prolific user of back door searches, other agencies also make use of them. In 2021, the NSA, CIA, and NCTC performed U.S. person queries of communications *content* on 8,790 occasions. The NSA and CIA further conducted U.S. person queries of communications *metadata* 3,958 times. OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 18–19.

[51] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011). In cases involving the so-called "foreign intelligence exception" to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government's national security interest against the privacy intrusion. While the surveillance scheme (*cont'd*)

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant.[52] Moreover, if a different agency wishes to search the seized data for a different purpose, it must obtain a separate warrant for that search.[53] The fact that the government lawfully obtained and is in possession of the computer's contents does not give it license to conduct any search it wishes.

Compounding the constitutional harm of back door searches, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. Before 2013, the government interpreted "obtained or derived from" so narrowly that it notified no one. In the nine years since the government's approach reportedly changed,[54] the government has provided notification in fewer than ten known cases, even though the PCLOB reports that the FBI searches Section 702 every time it conducts a national security investigation and there have been nearly two thousand terrorism and national security convictions during this time.[55]

There is reason for concern that the government is avoiding its notification requirements by engaging in "parallel construction" — i.e., recreating the Section 702 evidence using less controversial means.[56] This is a well-documented practice that the government has used in a

---

should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest. This is one of several errors in the FISA Court's 2015 decision upholding the constitutionality of back door searches. *See* Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider,* JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

[52] *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *rev'd en banc on other grounds,* 824 F.3d 199 (2d Cir. 2016).

[53] *See* United States v. Hulscher, 2017 WL 657436 (D.S.D. February 17, 2017).

[54] For more background, see 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.

[55] *See* Brief for the Brennan Ctr. for Justice et al. as Amicus Curiae at 23 n.23, *Wikimedia v. Nat'l Sec. Agency*, No. 22-190 (2022); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2021 at 14 (133 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2020 at 14 (172 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2019 at 14 (181 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2018 at 14 (185 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2017 at 14 (196 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2016 at 14 (210 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14 (273 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 14 (265 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60 (290 guilty dispositions).

[56] *See* Toomey, *supra* note 54; John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans,* REUTERS (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805#X7BeCQSb0GrEDTJX.97.

variety of settings, including foreign intelligence surveillance cases.[57] Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be "derived from" Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to "the wall." Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama's Review Group on Intelligence and Communications Technologies — a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) — unanimously recommended closing the "back door search" loophole by prohibiting searches for Americans' communications without a warrant.[58]

III. Violations of Statutory and Court-Ordered Privacy Protections

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than they were during the period of J. Edgar Hoover's worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is limited evidence of intentional abuse of foreign intelligence surveillance authorities.[59] But the government's record of non-compliance with statutory, constitutional, and court-ordered requirements is extensive and alarming. Notably, this includes cases in which the government did not detect the non-compliance for years, and external overseers (including the FISA Court) had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was *not* trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide.

---

[57] *See* Human Rights Watch, *Dark Side: Secrets Origins of Evidence in US Criminal Trials* (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

[58] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 29 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[59] *See, e.g.*, [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018) (noting "[a] small number of cases in which FBI personnel apparently conducted queries for improper personal reasons — for example, a contract linguist who ran queries on himself, other FBI employees, and relatives"); Letter from Dr. George Ellard, Inspector Gen., Nat'l Sec. Agency, to Sen. Charles E. Grassley (Sept. 11, 2013), *available at* http://www.privacylives.com/wp-content/uploads/2013/09/09262013-NSA-Surveillance-09-11-13-response-from-IG-to-intentional-misuse-of-NSA-authority.pdf (detailing 12 instances of intentional abuse of NSA bulk surveillance data, most involving employees searching for information on their romantic partners).

In any event, inadvertent failures to adhere to privacy protections are a concern in their own right, especially when they are as persistent and pervasive as they are here. They can result in Americans being investigated without proper legal basis; sensitive information falling into the hands of people who could misuse it; information being improperly retained and thus subject to hacking or theft; and a range of other harms. The knowledge that information is being improperly collected, stored, and accessed also creates a chilling effect on free and open communication[60] — particularly among marginalized communities who are more likely to be the victims of abusive surveillance practices.

A. FBI Violations of Limitations on U.S. Person Queries

Since Section 702 was last reauthorized, it has emerged that the FBI has widely disregarded the modest limits on U.S. person queries imposed by Congress and the FISA Court. There is every reason to believe that these violations have occurred since the program's inception, and no indication that the FBI is putting a stop to them.

In the vast majority of cases, the only substantive restriction on the FBI's use of U.S. person identifiers to query Section 702 data is the standard set forth in its querying procedures. Congress required agencies to develop these procedures when it reauthorized Section 702 in 2018. Although agencies' minimization procedures already had some limits on queries,[61] the

---

[60] After Edward Snowden revealed the NSA's bulk collection program in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., "dirty bomb" or "CIA"). A control list of popular search terms or other types of sensitive terms (such as "abortion") did not show the same change. *See* Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Apr. 29, 2015), *available at* http://dx.doi.org/10.2139/ssrn.2412564. Similarly, after the Associated Press reported on the New York City Police Department's surveillance activities, Muslims reported a decline in mosque attendance and Muslim Student Association participation, as well as a marked reticence to speak about political matters in public places or to welcome newcomers into the community. *See* MUSLIM AMERICAN CIVIL LIBERTIES COALITION (MACLC) ET AL., MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[61] For instance, the FBI's 2016 minimization procedures provided that, "[t]o the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime." LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § III.D (Sept. 21, 2016), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf. The 2016 minimization procedures for both the CIA and NCTC required queries to be "reasonably likely to return foreign intelligence information, as defined in FISA." WILLIAM BARR, U.S. DEP'T OF JUSTICE, 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 § 4 (Sept. 21, 2016), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_CIA_Section_702_Minimization_Procedures_Se_26_2016.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE 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 § C.1 (Sept. 21, 2016) , *available at* https://www.dni.gov/files/documents/icotr/51117/2016_NCTC_Section_702_Minimizatio_Procedures_Sep_26_2016.pdf.

new requirement clarified that this was a mandatory aspect of minimization and that the constraints must be set forth in detail. The querying procedures must be approved by the FISA Court, and the Court's annual approval of Section 702 surveillance is predicated on compliance with these and other court-approved procedures.

The FBI's querying procedures provide that "[e]ach query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures."[62] This is a fairly low bar, to be sure. Even so, FISA Court opinions issued in recent years show that the FBI has repeatedly failed to meet it.

In an October 2018 opinion, the FISA Court noted that, "[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime."[63] These included multiple one-off incidents of FBI personnel running U.S. person queries accidentally or for improper personal purposes. (In a frank statement that reveals why limits on access are a poor substitute for adequate limits on collection, the FISA Court commented that it was less concerned about personal misuses of the data, because "[i]t would be difficult to completely prevent personnel from querying data for personal reasons."[64]) They also included several incidents indicative of more systemic problems, including:

- In March 2017, the FBI, against the advice of the FBI's Office of General Counsel, conducted queries using 70,000 identifiers "associated with" people who had access to FBI facilities and systems.
- On a single day in December 2017, the FBI conducted over 6,800 U.S. person queries using Social Security Numbers.
- Between December 7-11, 2017, an FBI official improperly reviewed raw FISA information resulting from 1,600 U.S. person queries.
- On more than one occasion, the FBI conducted dozens of U.S. person queries to gather information about potential informants.[65]

The government told the FISA Court that these errors stemmed from "fundamental misunderstandings by some FBI personnel [about] what the standard 'reasonably likely to return foreign intelligence information' means."[66] This is a remarkable admission, given that the standard essentially carried forward a limitation that had been in place for a decade in the FBI's minimization procedures,[67] and given the government's repeated assurances to the FISA Court

---

[62] [Redacted], 402 F. Supp. 3d 45, 75 (FISA Ct. 2018).
[63] *Id.* at 76.
[64] *Id.* at 78.
[65] *Id*. at 76–7.
[66] *Id*. at 77.
[67] Specifically, the FBI's 2008 minimization procedures provided that, "[t]o the extent reasonably feasible, authorized users must design such queries to find and extract foreign intelligence information or evidence of a crime…" MICHAEL MUKASEY, U.S. DEP'T OF JUSTICE, STANDARD MINIMIZATION PROCEDURES FOR FBI SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

during this time that access to Americans' data was restricted to personnel who were carefully trained in the applicable limits.

The Court expressed "serious concern" about "the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it."[68] The Court posited that the reported violations were likely the tip of the iceberg. It noted that some FBI offices field offices go for periods of two years or more between oversight visits, and ultimately, Justice Department overseers "review only a small portion of the queries conducted."[69] It also observed that "the documentation available to [overseers] lacks basic information that would assist in identifying problematic queries."[70] Given these limitations on existing oversight mechanisms, the Court wrote, "it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court."[71]

The Court was equally disturbed by the FBI's use of "batch queries." The FBI's querying procedures require that "[e]ach query" must be reasonably likely to retrieve foreign intelligence information or evidence of a crime. The government, however, took the position that "an aggregation of individual queries" — also referred to as a "batch query" — "can satisfy the querying standard, even if each individual query in isolation would not be reasonably likely to return foreign-intelligence information or evidence of a crime."[72] So, for instance, if the FBI has information that an employee at a particular company is planning illegal actions, but the FBI has no knowledge of who the employee is, the Bureau would be justified (according to the government's argument) in running queries for *every employee at that company*. The Court rightly expressed skepticism that such an approach could be reconciled with the text of the FBI's querying procedures.

The Court held that the extent of improper querying rendered the FBI's procedures, as implemented, inconsistent with Section 702's "minimization" requirement. It also held that the FBI's practices ran afoul of the Fourth Amendment. Weighing the privacy interests at stake against the government's interests, the Court found the privacy interests to be substantial: "The goal of the Fourth Amendment is to protect individuals from arbitrary governmental intrusions on their privacy…The FBI's use of unjustified queries squarely implicates that purpose: the FBI searched for, and presumably examined when found, private communications of particular U.S. persons on arbitrary grounds."[73] Although the Court found the government's interest in acquiring foreign intelligence information to be "particularly intense," it quoted a decision by the Foreign Intelligence Surveillance Court of Review stating that if "the protections that are in place for individual privacy interests are . . . insufficient to alleviate the risks of government error and

---

§ III.D (Oct. 22, 2008), *available at* https://www.aclu.org/sites/default/files/field_document/2017.5.8_savage-nyt-foia-fbi-2008-09-fisa-standard.pdf.

[68] [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018).

[69] *Id*. at 79.

[70] *Id.*

[71] *Id*. at 79–80.

[72] *Id*. at 81.

[73] *Id.* at 89.

abuse, the scales will tip toward a finding of unconstitutionality."[74] The Court concluded: "Here, there are demonstrated risks of serious error and abuse, and the Court has found the government's procedures do not sufficiently guard against that risk."[75]

To cure these defects, the Court recommended — and the FBI ultimately adopted, after the government's unsuccessful appeal to the Foreign Intelligence Surveillance Court of Review — a remedy proposed by *amici*. Specifically, any time the FBI runs a U.S. person query that returns Section 702 data, FBI personnel are not permitted to view the content (although they may still view non-content "metadata") unless they first document the reasons why they believed the query was likely to return foreign intelligence or evidence of a crime.

When the Court next signed off on Section 702 surveillance, however, there had been no improvement. In a December 2019 opinion, the Court observed that "there still appear to be widespread violations of the querying standard by the FBI."[76] The list of violations compiled in the Court's opinion includes (among others) queries of college students participating in a "Collegiate Academy"; queries of police officer candidates; and one case in which the FBI ran 16,000 U.S. person queries — for a purpose that remains classified — of which only seven were justified.[77] The Court nonetheless approved Section 702 for another year, reasoning that the FBI had not been given sufficient time to fully implement the remedy previously imposed by the Court.

A year later, in a November 2020 opinion, the FISA Court reported that "the FBI's failure to properly apply its querying standard" was "more pervasive than … previously believed."[78] The targets of the improper queries included people who came to the FBI to perform repairs; victims who approached the FBI to report crimes; and business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy."[79] Moreover, when conducting batch queries, the FBI had failed in many cases to document the justifications for the queries, due to a "system failure [that] went undetected or unreported for nearly a year."[80] As the Court noted, "[t]he failure to require a written justification for a bulk query involving a U.S.-person query term is particularly concerning given the indiscriminate nature of such queries."[81]

Once again, however, the Court approved Section 702 surveillance. This time, it reasoned that government office closures resulting from the Covid-19 pandemic had prevented the

---

[74] *Id*. at 86–7 (quoting *In re* Directives Conducted Pursuant of Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)).
[75] *Id*. at 88.
[76] [Redacted], at 65 (FISA Ct. Dec. 6, 2019), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1060343/gid_c_00282.pdf?sequence=1&isAllowed=y.
[77] *Id.* at 66–7.
[78] [Redacted], at 39 (FISA Ct. Nov. 18, 2020), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1061209/gid_c_00289.pdf?sequence=1&isAllowed=y.
[79] *Id*. at 39–40.
[80] *Id*. at 51.
[81] *Id.* at 50.

oversight necessary to determine whether the new training and record-keeping requirements implemented by the FBI in late 2019 and early 2020 had made any difference. As the Court stated, "While the Court is concerned about the apparent widespread violations of the querying standard… it lacks sufficient information at the time to assess the adequacy of the FBI system changes and training, post-implementation."[82]

The Court's repeated excuses for the FBI's behavior amount to an admission that the FBI's systems, procedures, and training have been inadequate since Section 702's inception — which means the improper queries have likely occurred from the outset. Throughout this period, the government has touted these same systems, procedures, and training, portraying them as robust protections for Americans' privacy. The notion that the FBI simply needs a little more time to get its house in order is far too dismissive of the constitutional rights that have been violated for at least five years (and probably closer to fourteen). Moreover, there is little reason to expect that additional record-keeping requirements or training sessions will solve the problem.

Indeed, even the most robust procedural protection of all — a warrant requirement — has proven insufficient to constrain the FBI. In 2018, Congress required the FBI to obtain a probable-cause order from the FISA Court before reviewing the results of U.S. person queries in a small subset of cases, i.e., predicated criminal investigations unrelated to national security.[83] According to the ODNI's statistical transparency reports, this requirement has been triggered on more than 100 occasions over the past four years.[84] This figure is almost certainly a substantial undercount, given that it measures the number of days on which queries that require warrants were performed rather than the number of queries. Incredibly, the FBI did not obtain a FISA Court order in a *single one* of those cases.

Addressing this issue in its December 2019 opinion, the FISA Court noted that "*[s]ome* violations resulted *in part* from the manner in which FBI systems displayed information in response to queries" (emphasis added).[85] Specifically, systems would display query results in a summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. Of course, FBI agents still could have obtained FISA Court orders before opening the results to see more than the 100 characters. According to the Court, however, "FBI personnel are known to have taken further steps in response to such displays (e.g., opening "products" containing contents returned by a query), thereby accessing Section 702-acquired contents beyond what was initially displayed to them."[86] In any event, this feature of the FBI systems did not account for all of the violations.

---

[82] *Id.* at 44.
[83] 50 U.S.C. § 1881a(f)(2)(A). The PCLOB has reported that the FBI routinely performs U.S. person queries at the "assessment" stage, which happens before the FBI has sufficient information to open a predicated investigation. PCLOB 702 REPORT, *supra* note 5, at 59.
[84] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2020 at 21 (Apr. 2021); OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 22.
[85] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 69.
[86] *Id*. at 70.

It is stunning that the FBI has ignored a statutory warrant requirement for four years, and equally astonishing that the FISA Court has permitted Section 702 surveillance to continue despite this fact. Promises that the FBI will fix these violations in the future ring empty given its long record of systemic non-compliance. At a minimum, because the Court itself has determined that the FBI's non-compliance with querying limitations renders the surveillance unreasonable under the Fourth Amendment, it seems clear that the surveillance — or, at least, the FBI's access to Section 702-acquired data — should be suspended until the FBI can prove that its queries of already-collected data are fully compliant with the law and the Constitution.

B. Other Violations

On multiple other occasions in the past fourteen years, the FISA Court has had occasion to rebuke the government for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, access, dissemination, and retention. It is instructive to review some of the Court's comments in these cases. The following statements are excerpted from nine opinions spanning the years 2009 through 2020:

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[87]
- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[88]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[89]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[90]
- "[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last."[91]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the

[87] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10–11 (FISA Ct. Mar. 2, 2009).
[88] *Id.* at 6.
[89] *Id.* at 10.
[90] *Id.* at 15.
[91] *Id.* at 16.

government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[92]

- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[93]
- "As far as can be ascertained, the requirement was simply ignored."[94]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[95]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[96]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[97]
- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition…presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[98]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor."[99]
- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[100]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[101]

---

[92] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[93] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]), *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[94] *Id.* at 19.
[95] *Id.* at 20.
[96] *Id.* at 21.
[97] *Id.* at 22.
[98] *Id.* at 77.
[99] *Id.* at 95.
[100] *Id.* at 115.
[101] [Redacted], at 48–49 (FISA Ct. Nov. 6, 2015), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/official-statement/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

- "The Court was extremely concerned about these additional instances of non-compliance."[102]
- "Perhaps 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 . . . ."[103]
- "The Court did not find entirely satisfactory the government's explanations of the scope of [its] segregation errors and the adequacy of its response to them . . . ."[104]
- "[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data."[105]
- "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those [Inspector General] and [NSA Office of Compliance for Operations] reviews at the October 4, 2016 hearing to an institutional lack of candor on NSA's part and emphasized that this is a very serious Fourth Amendment issue."[106]
- "Beginning in October 2016, while the 2016 Certifications were pending before the FISC, the government reported that NSA had violated that querying prohibition much more frequently than had been previously disclosed."[107]
- "The quarterly reports also revealed that in several of these incidents the CIA or the FBI was responsible for conducting post-targeting content review but did not conduct timely reviews."[108]
- "It must be noted . . . that the government has unjustifiably disregarded the current reporting requirement . . . . It should be unnecessary to state that government officials are not free to decide for themselves whether or to what extent they should comply with Court orders."[109]
- "The government has not reported such instances [of non-compliance] in timely fashion. Rather, they have been reported to the Court belatedly, usually after they were uncovered during oversight reviews."[110]
- "The FBI's handling of the Carter Page applications, as portrayed in the OIG report, was antithetical to the heightened duty of candor . . . . The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable."[111]
- "[T]he OIG expressed a 'lack of confidence that the Woods Procedures are working as intended' — i.e., 'as a means toward achiev[ing]' the FBI's professed policy 'that FISA

---

[102] *Id.* at 50.
[103] *Id.* at 58.
[104] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 80.
[105] *Id.* at 82.
[106] *Id*. at 19 (internal quotation marks omitted).
[107] [Redacted], 402 F. Supp. 3d 45, 56 (FISA Ct. 2018).
[108] *Id.* at 104.
[109] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 44–5.
[110] *Id.* at 72.
[111] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 3 (Dec. 17, 2019), *available at* https://www.fisc.uscourts.gov/sites/default/files/MIsc%2019%2002%20191217.pdf.

> applications be "scrupulously accurate."' . . . It would be an understatement to note that such lack of confidence appears well founded. None of the 29 cases reviewed had a Woods File that did what it is supposed to do: support each fact proffered to the Court. For four of the 29 applications, the FBI cannot even find the Woods File . . . . For three of those four, the FBI could not say whether a Woods File ever existed."[112]

A particularly notable Section 702 compliance failure, discussed in the FISA Court's April 26, 2017 opinion, was the NSA's widespread use of U.S. person identifiers to query certain data obtained through upstream collection. The FISA Court had prohibited such queries in 2011, in response to its discovery that the NSA had for years been pulling in substantial numbers of wholly domestic communications by virtue of "abouts" collection. The Court had found the NSA's handling of this data unconstitutional, and the ban on U.S. person queries of upstream data was one of the key remedies adopted to cure the constitutional defect.

In January 2016, however, the NSA Inspector General reported internally that agency analysts were not fully complying with this limitation, based on an examination of three months of audit data from early 2015. The Inspector General and the NSA's Office of Compliance for Operations began studies of other time periods, and "preliminary results [suggested] the problem was widespread during all periods under review."[113] In other words, at no point during the operation of upstream collection — either in the years before the NSA informed the Court that it was collecting wholly domestic communications, or in the subsequent years when this data was supposedly off limits to U.S. person queries — had this surveillance operated within the bounds of the Constitution.

Nonetheless, the NSA waited for several months before informing the FISA Court of the problem, which it blamed on "human error" and "system design issues."[114] The Court chided the government for this "institutional lack of candor."[115] It granted short-term extensions of Section 702 surveillance authority while the government attempted to resolve the issue, but as of late January 2017, "[t]he government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries,"[116] and as of March, "continued to . . . investigate potential root causes of non-compliant querying practices."[117] With no resolution in sight, and with the Court unwilling to certify the program for another year while the problem remained, the NSA made the only possible choice: to halt "abouts" collection for the time being.

The Court's April 2017 opinion also includes a long list of other compliance failures. For instance, between November 2015 and May 2016, no less than *85 percent* of queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying

---

[112] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 2 (Apr. 3, 2020), *available at* https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Order%20PJ%20JEB%20200403.pdf.
[113] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 19.
[114] *Id.* at 20.
[115] *Id.* at 19.
[116] *Id.* at 21.
[117] *Id.* at 23.

of Section 702 data.[118] The Court also found that the FBI had shared raw Section 702 information with a redacted entity "largely staffed by private contractors," and that "the [redacted] contractors had access to raw FISA information that went well beyond what was necessary" to perform their jobs.[119] And the Court noted that "[r]ecent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements," resulting in "indefinite retention" of some data.[120]

More compliance incidents followed. As recounted in the FISA Court's December 2019 opinion, the NSA determined that it was losing foreign intelligence information as a result of a court-ordered rule that required the agency to use certain technical methods to limit collection of purely domestic communications. Its solution was to disregard the rule. Only when Section 702 was next up for reauthorization did the NSA disclose the violation and ask the Court to rescind the requirement. The Court, in a model of understatement, noted that "the proper course would have been to seek amendment of the procedures earlier, rather than unilaterally deciding to deviate from them."[121] The Court's November 2020 decision also makes reference to a heavily redacted "potential compliance incident" involving NSA that was under investigation by the government.[122]

The most recent revelation of NSA non-compliance came just this week, when the agency responded to a Freedom of Information Act request filed six years ago by releasing a heavily redacted 2016 report of the NSA's Inspector General.[123] The report details how one NSA analyst launched a surveillance project in early 2013 that targeted Americans' communications without a FISA Court order and without a foreign intelligence purpose, in violation of FISA, Executive Order 12333, and multiple agency policies. Despite whistleblowers' complaints, NSA officials allowed the project to continue because — as they explained to the Inspector General — the project was complex and they didn't understand it. This illegal project continued for three years until the Inspector General's office completed its investigation.

Former NSA Director Keith Alexander, commenting on the report's release, asserted that "[w]hen somebody does the wrong thing, we find them, and we hold them accountable."[124] In fact, the Inspector General's report specifically found that oversight by NSA officials was inadequate, and the NSA has refused to answer questions about whether any action was taken against the analyst who developed and ran the illegal program.[125]

---

[118] *Id.* at 82.
[119] *Id.* at 84.
[120] *Id.* at 87–9.
[121] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 13.
[122] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 78, at 37–8.
[123] OFF. INSPECTOR GEN., NAT'L SEC. AGENCY, REPORT OF INVESTIGATION: MISUSE OF SIGINT SYSTEMS (Feb. 12, 2016), *available at* https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rgMApjakmUtM/v0.
[124] Jason Leopold, Katrina Manson & William Turton, *NSA Watchdog Concluded One Analyst's Surveillance Project Went Too Far*, BLOOMBERG (Nov. 1, 2022), https://www.bloomberg.com/news/articles/2022-11-01/nsa-watchdog-concluded-one-analyst-s-surveillance-project-went-too-far.
[125] *Id.*

The long, unbroken string of violations recounted here paints a vivid and unmistakable picture of foreign intelligence surveillance operating outside the constraints of the law. It is unclear whether the violations are occurring because agencies are not putting sufficient effort into compliance, because they lack the technical capability to ensure compliance, or for some other reason. It may be the case that collection programs have become so massive in scope, and the systems for retaining and processing the data so technically complex, that it is simply impossible to achieve consistent compliance with the rules governing their use. Whatever the explanation, the fact that the government's widespread failures to honor privacy protections have been mostly inadvertent is of limited comfort when the government is asking Congress and the public to entrust it with immense quantities of Americans' private data.

IV. The Artificial Distinction Between Section 702 and EO 12333

As a general matter, FISA applies when the government collects foreign intelligence inside the United States or from U.S.-based companies. When the government collects foreign intelligence overseas, it proceeds under Executive Order 12333, unless it is targeting a specific, known U.S. person or intentionally collecting purely domestic communications. There is one caveat to this rule: While FISA is the exclusive means by which the government may conduct "electronic surveillance,"[126] the definition of that term[127] does not cover the collection of many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data. Accordingly, collection of such information inside the United States may also take place under EO 12333.

A geographic limitation on FISA's reach might have made some sense in 1978 (the year of FISA's enactment), when surveillance inside the United States generally meant surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. Today, however, communications are routed and stored all over the world. Indeed, the fact that purely foreign communications may be stored by internet service providers inside the United States — which, under FISA as originally enacted, would have triggered the requirement to obtain a probable-cause order[128] — is one of the main reasons the government sought to "modernize" FISA in 2008 through the enactment of Section 702.

The government notably failed to seek a solution to the other half of this problem: the fact that Americans' communications and other personal data are routinely routed and stored overseas, removing them from FISA's protections and exposing them to EO 12333 surveillance. Particularly when the government engages in bulk collection — i.e., the collection of information without the use of selectors that would identify particular targets — it is almost certain to sweep

[126] 50 U.S.C. § 1812.
[127] 50 U.S.C. § 1801(f).
[128] *See* Ex Parte Brief for Respondents at 8–9, *In re* Directives to Yahoo Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (FISA Ct. Rev. 2008), *available at* https://cdt.org/wp-content/uploads/2014/09/2-yahoo702-governments-ex-parte-merits-brief.pdf (noting that when the government obtains stored emails from an internet service provider, this acquisition is covered by the fourth prong of the definition of "electronic surveillance," which applies to collection inside the United States regardless of the U.S. person status of the communicants).

in Americans' information, including wholly domestic communications, potentially in large amounts. Bulk collection is prohibited under FISA, but it is permitted under EO 12333.

In February of this year, Americans learned that the CIA had been conducting bulk collection programs that pull in an unknown quantity of Americans' data. At the request of Senators Ron Wyden and Martin Heinrich, the CIA released documents pertaining to two reports authored by the PCLOB, titled "Deep Dive I"[129] and "Deep Dive II."[130] The surveillance described in Deep Dive I includes the bulk acquisition of information about financial transactions involving Americans and others. For Deep Dive II, the CIA has disclosed neither what type of information it is collecting in bulk nor for what purpose. However, the CIA's sparse public statements on the program suggest that the collection impacts "Americans who are in contact with foreign nationals,"[131] which implies that this program involves communications records. The two pages of PCLOB staff recommendations released by the CIA show that CIA analysts query the data acquired under this program for information about US persons, and that they do so without recording the justification for the queries — making it virtually impossible to conduct even internal oversight.

Even when EO 12333 surveillance is targeted, it will acquire the communications of Americans in contact with the targets, just as Section 702 surveillance does. The FISA Court has recognized that the collection of communications between foreigners overseas and Americans implicates the Fourth Amendment.[132] Congress clearly shares this understanding and has therefore included minimization and close oversight by the FISA Court as critical elements of Section 702. Although these protections have proven insufficient in practice (as detailed above), they far exceed the protections established by EO 12333, even as supplemented by President Biden's recent executive order.

Two critical distinctions suffice to prove the point. First, under Section 702, the government must submit its targeting, minimization, and querying procedures to the FISA Court on an annual basis, and the Court must find that these procedures — both on paper, and in practice — comport with the statute and the Constitution. The government must report significant instances of non-compliance to the Court and implement any remedies that the Court orders. No such judicial oversight — indeed, no judicial oversight whatsoever — exists for EO 12333 surveillance.

---

[129] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON CIA FINANCIAL DATA ACTIVITIES IN SUPPORT ON ISIL-RELATED COUNTERTERRORISM EFFORTS (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/63f697addbbd30a4d64432ff28bbc6d6/OPCL-PCLOB-Report-on-CIA-Activities.pdf.
[130] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS FROM PCLOB STAFF (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/f61ca00cbcda9b5d46a04e0b53b5f2b9/OPCL-Recommendations-from-PCLOB-Staff.pdf.
[131] Katie Bo Lillis, *Senators allege CIA collected data on Americans in warrantless searches*, CNN (Feb. 11, 2022), https://www.cnn.com/2022/02/10/politics/cia-data-collection-americans/index.html.
[132] *See, e.g.,* [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 61–2 (acknowledging that Section 702 surveillance "implicates interests protected by the Fourth Amendment" insofar as it captures communications to or from Americans).

Second, while the NSA[133] and NCTC[134] have procedures in place that include substantive restrictions on U.S. person queries of EO 12333 data (albeit without any judicial oversight to ensure compliance), there are no meaningful constraints on U.S. person queries by the CIA or FBI. The CIA's EO 12333 procedures allow it to run U.S. person queries for any information "related to a duly authorized activity of the CIA"[135] — a much broader standard than that contained in the agency's Section 702 querying procedures, under which queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA."[136] The distinction is even more stark when it comes to U.S. person queries by the FBI. For Section 702 data, such queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime."[137] For data obtained under EO 12333, there are no specific restrictions on querying. Rather, under the Attorney General's Guidelines for Domestic FBI Operations, there is simply a general admonition that "[a]ll activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines."[138]

There is no justification for giving lesser protections to Americans' constitutional rights based simply on where the data was obtained. If anything, the privacy implications of EO 12333 for Americans are likely even greater than those of Section 702. The government has acknowledged that the majority of its foreign intelligence surveillance activities take place under

---

[133] DEP'T OF DEFENSE, DOD MANUAL S-5240.01-A, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES GOVERNING SIGNALS INTELLIGENCE INFORMATION AND DATA COLLECTED PURSUANT TO SECTION 1.7(C) OF E.O. 12333 (Jan. 7, 2021), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/Redacted%20Annex%20DODM%205240.01-A(1).pdf.

[134] NAT'L COUNTERTERRORISM CTR., NATIONAL COUNTERTERRORISM CENTER IMPLEMENTATION PROCEDURES FOR THE ODNI INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 (accessed Oct. 31, 2022), *available at* https://www.dni.gov/files/NCTC/documents/news_documents/NCTC_Implementation_Procedures_executed_3_22_21_U_final.pdf.

[135] CENTRAL INTELLIGENCE AGENCY, THE CIA'S UPDATED EXECUTIVE ORDER 12333 ATTORNEY GENERAL GUIDELINES 6 (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/100ea2eab2f739cab617eb40f98fac85/Detailed-Overview-CIA-AG-Guidelines.pdf.

[136] WILLIAM BARR, U.S. DEP'T OF JUSTICE, QUERYING 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 § IV.A (Sept. 16, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_CIA%20Querying%20Procedures_10.19.2020.pdf.

[137] WILLIAM BARR, U.S. DEP'T OF JUSTICE, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § IV.A.1 (Sept. 16, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Querying%20Procedures_10.19.2020.pdf.

[138] U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 13 (accessed Oct. 31, 2022), *available at* https://www.justice.gov/archive/opa/docs/guidelines.pdf.

EO 12333.[139] Accordingly, it reasonable to expect that there is more "incidental" collection of Americans' information under EO 12333 than under Section 702, even when such surveillance is targeted. And, of course, bulk collection has the potential to sweep in Americans' data in amounts that far exceed what normally occurs during targeted surveillance.

V. Projects PCLOB Should Undertake

After fourteen years of Section 702 surveillance operating in violation of the statute, the Constitution, and the legitimate privacy expectations of Americans, it is time for Congress to reform Section 702. In many cases, the necessary reforms are clear; these are discussed in Part VI. Nonetheless, concrete information about the impact of Section 702 on Americans would help frame the debate over reauthorization. In addition, certain information regarding targeting practices and the use of Section 702 for cybersecurity investigations would assist in developing appropriate reforms.

The PCLOB should undertake three projects designed to elicit information on these matters. In its previous investigation of Section 702, culminating in a 191-page report issued in 2014, the PCLOB was remarkably successful in securing the declassification of extensive information about the program's workings. That information continues to inform the public debate over Section 702 today. The PCLOB can perform a similar service here — and can enhance its own ability to issue substantive recommendations — with respect to key aspects of Section 702 surveillance that remain obscure.

A. Obtain Estimate of the Scope of "Incidental" Collection

The government has resisted calls to produce an estimate of how many communications involving a U.S. person are collected under Section 702. However, that is no reason to abandon this important inquiry. Circumstances have changed since Section 702 was last reauthorized. There is a new administration in place, including a Director of National Intelligence who has pledged to prioritize transparency.[140] In addition, computer scientists have proposed a new solution to the problem of how to generate such an estimate without compromising personal privacy.

It is important to bear in mind that lawmakers have requested an *estimate* of the scope of incidental collection — not an exact number. Surely, if our national security depended on the intelligence community producing a rough approximation of Section 702's impact on Americans, it would be produced. Even if all the government could provide was an order of magnitude (e.g., "millions" or "tens of millions"), that would richly inform the debate over Section 702 by

---

[139] Nat'l Sec. Agency, *Legal Fact Sheet: Executive Order 12333* (Jun. 19, 2013), *available at* https://www.aclu.org/sites/default/files/field_document/Legal%20Fact%20Sheet%20Executive%20Order%2012333_0.pdf.

[140] *Nomination of Avril Haines to be the Director of National Intelligence, Hearing Before the S. Comm. on Intelligence*, 117th Cong. 2 (Jan. 19, 2021) (statement of Avril Haines), *available at* https://www.intelligence.senate.gov/sites/default/files/documents/os-ahaines-011921.pdf.

helping to dispel the misconception that the term "incidental" has created among lawmakers and the American public.

The PCLOB should work with the intelligence community to identify and implement a method for generating this estimate. The estimate should be made public before the deadline for reauthorization. As noted above, if the government itself has literally *no* sense of how many Americans' communications it is collecting — and no way to acquire such a sense — Congress should reconsider whether to entrust the government with this powerful authority.

B. Investigate Targeting Decisions

As discussed above, the statutory restrictions on the permissible targets Section 702 surveillance are minimal, given FISA's expansive definition of "foreign intelligence information." Moreover, the legitimate objectives of surveillance identified in the recent executive order do not necessarily translate into a smaller pool of surveillance targets. The scope of permissible targets significantly impacts Americans' civil liberties, as it determines the breadth of "incidental" collection. The PCLOB accordingly should undertake an investigation of Section 702 targeting decisions with an eye toward recommending reforms that would narrow collection.

One reform that has been recommended by multiple organizations, including the Brennan Center, is to require the government to have a reasonable belief, based on specific and articulable facts, that targets are foreign powers (FP) or agents of foreign powers (AFP), as defined in FISA. (This would still be a lower bar than the pre-Section 702 requirement, under which the FISA Court had to find probable cause that each target was a FP/AFP.) To assess the likely impact of such a change, the PCLOB should work with the relevant agencies to determine what proportion of Section 702 targets, if any, is comprised of persons who do *not* qualify as FPs/AFPs. This will likely involve sampling, as analyzing more than 200,000 targets might not be feasible.

If analysis of the sample indicates that the vast majority of targets are reasonably suspected to be FPs/AFPs, that suggests that advocates' proposed reform is appropriate and workable. On the other hand, if PCLOB's analysis indicates that a significant percentage of targets do not fall within those definitions, PCLOB should ask agency officials to articulate why surveillance of these targets, in each instance, is likely to produce information that is directly relevant to one of the twelve objectives identified in President Biden's executive order.[141] If officials cannot satisfactorily answer this question and support their answer with documentation,

[141] In conducting this inquiry, PCLOB should rely on a slightly modified version of the objectives. First, with respect to the goal of "understanding or assessing the capabilities, intentions, or activities of . . . a foreign-based political organization," PCLOB should interpret the term "foreign-based political organization" to exclude civil society non-governmental organizations. Second, the goal of protecting against "transnational criminal threats" should apply only to serious crimes that significantly impact the lives, safety, or property of U.S. persons or the national security of the United States. Third, the goal protecting the integrity of U.S. "government property" should apply only where there is a threat of significant property damage involving a risk to the personal safety of persons on or near the property. *See* Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, JUST SEC. (Oct. 31, 2022), https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/.

then those targets should be considered inappropriate. If, however, officials are able to make such a showing, PCLOB should identify the *narrowest* substantive criteria that would capture the non-FPs/AFPs (or categories of non-FPs/AFPs) in question.[142] These can then serve as the basis for a legislative reform recommendation.

C. Investigate the Use of Section 702 for Cybersecurity Purposes

The number of U.S. person queries the FBI conducted in 2021 was more than twice that of the previous year. The ODNI explained the fluctuation as follows: "In the first half of the year, there were a number of large batch queries related to attempts to compromise U.S. critical infrastructure by foreign cyber actors. These queries, which included approximately 1.9 million query terms related to potential victims — including U.S. persons — accounted for the vast majority of the increase in U.S. person queries conducted by FBI over the prior year."[143]

Although this statement was intended to allay concerns, it raises alarm bells. In no domestic cybersecurity investigation could the FBI obtain warrants to search 1.9 million Americans' communications simply because they might be victims of the crime. The fact that these Americans' communications may already have been collected through Section 702 does not change the privacy calculus. Even if the search is performed only to identify malicious code embedded in the victims' communications, the result is to expose their personal information to manual review. As Professor Orin Kerr has explained, collection constitutes a seizure, while querying constitutes a search — separate Fourth Amendment events, each of which constitutes a distinct intrusion on privacy.[144]

The PCLOB should investigate how Section 702 is used for cybersecurity purposes,[145] and the degree to which cybersecurity investigations result in extensive targeting or querying of persons not suspected of any wrongdoing. The risk of overbroad surveillance is particularly high in such investigations; as noted above, protecting cybersecurity could in theory justify constant monitoring of the Internet. The role of the PCLOB, however, is to ensure that the government's

---

[142] Under this approach, the *broadest* possible criterion would be a reasonable likelihood that the target is communicating information that is directly relevant to one of the legitimate objectives. Such a criterion, general as it is, would provide an additional constraint on the standard currently set forth in NSA targeting procedures — i.e., "[T]he targeted is expected to possess, receive, and/or is likely to communicate foreign intelligence information" concerning one of the foreign powers or territories identified in the agency's certifications. WILLIAM BARR, U.S. DEP'T OF JUSTICE, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (Oct. 19, 2020), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Targeting%20Procedures_10.19.2020.pdf.

[143] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 20.

[144] Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of crimes*, WASH. POST (Oct. 20, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-and-querying-the-702-database-for-evidence-of-crimes/.

[145] The Brennan Center recognizes that the PCLOB's statutory mandate is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. Much like Section 702 itself, cybersecurity sometimes involves terrorism and sometimes does not. It therefore should be understood to fall within the PCLOB's jurisdiction.

efforts to keep the nation safe are balanced with the need to protect privacy and civil liberties. The query numbers reported by ODNI suggest that the government is not striking the right balance in this area.

The PCLOB should release a public report with its findings. One goal of the investigation should be to inform the PCLOB's recommendations for reforming targeting and U.S. person query practices, as discussed in Part VI.A & B. In developing any recommendations that relate specifically to cybersecurity investigations, the PCLOB should consult with experts in the field of privacy and technology as well as relying on its own staff technologists. Conducting this investigation and, if necessary, issuing cybersecurity-specific reform recommendations might well require hiring additional staff with technological expertise.

VI. Reforms that PCLOB Should Recommend

There are several reforms that would go far toward mitigating the privacy risks posed by Section 702, while retaining the core functionality of the statute: the ability of the government to conduct warrantless surveillance of foreigners overseas who may pose a threat to the U.S. or its interests. These reforms include narrowing the scope of Section 702 collection; shoring up protections for "incidentally" acquired U.S. person information by requiring agencies to obtain a warrant, court order, or subpoena before running U.S. person queries of Section 702 data, and by placing stricter limits on retention; modernizing FISA by establishing basic rules and requiring FISA Court oversight for EO 12333 surveillance; and increasing transparency and accountability in the operations of Section 702 and EO 12333. Given the troubled history of Section 702 surveillance, the PCLOB should recommend that Congress make these changes as a precondition to reauthorization of the statute.

A. Narrow the Scope of Collection

Congress should narrow the scope of permissible Section 702 targets, which will in turn reduce the volume of "incidental" collection and increase the likelihood of a U.S.-EU data-sharing agreement withstanding European courts' scrutiny. Currently, the statute allows the government to target anyone reasonably believed to be a foreigner overseas, as long as the purpose of collection is to acquire information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[146] Although President Biden's recent executive order further restricts surveillance by defining legitimate objectives, those objectives may be expanded in secret or revoked by a future president, and they do not necessarily limit the scope of collection.

The PCLOB should recommend two measures in this area. First, subject to the findings of the investigations proposed above, it should recommend that Congress require the government to have a reasonable belief, based on specific and articulable facts, that the target of surveillance is a foreign power or an agent of a foreign power, as broadly defined in FISA. The FP/AFP determination would be an internal one; it would not have to be submitted to the FISA Court for

[146] 50 U.S.C. § 1801(e)(2).

case-by-case approval or meet a "probable cause" standard. However, Congress should require the FISA Court to review a sample of targeting decisions as part of its annual approval process.

Second, in addition to imposing a FP/AFP requirement, Congress should codify the legitimate objectives identified in President Biden's executive order (with a small number of revisions[147]) and prohibit the adoption of additional objectives without congressional authorization. It also should translate these objectives into constraints on targeting. Specifically, Congress should require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to provide information that is directly relevant to one or more of the objectives. The statute should make clear that the absence of information cannot itself be deemed relevant for this purpose — i.e., it is not permissible to target groups or individuals simply to "rule them out" as sources of useful information.

Congress also should codify the current cessation of "abouts" collection. This type of surveillance greatly increases the chances of pulling in wholly domestic communications, not to mention other completely innocent communications between people who are not themselves permissible targets of surveillance. Moreover, although "abouts" collection poses uniquely significant risks to privacy, it was a relatively small part of the upstream program, which itself comprises less than one tenth of Section 702 collection.[148] This is clearly a situation in which the privacy risks outweigh the benefits — a point the NSA effectively acknowledged when it stopped "abouts" collection in April 2017.[149]

B. Shore Up Protections for "Incidentally" Acquired U.S. Person Information

Narrowing the scope of surveillance will reduce the amount of "incidental" collection of Americans' communications that can take place, but it will not and cannot eliminate "incidental" collection altogether. It is thus critical that Congress breathe life into its statutory command to agencies to "minimize" the retention, use, and sharing of Americans' information acquired through Section 702 surveillance.

First and foremost, the PCLOB should recommend that Congress require all government agencies to obtain a warrant or a Title I FISA Court order before using U.S. person identifiers to query the contents of communications or other Fourth Amendment-protected information (such as geolocation data) obtained under Section 702. This would close the loophole that currently allows the government to read Americans' e-mails and listen to their phone calls without any factual predicate to suspect wrongdoing, let alone a warrant. What makes the warrantless surveillance lawful in the first instance is the government's certification that it is targeting *only* foreigners. That representation becomes a semantic sleight of hand when the government

---

[147] See *supra* note 141 and accompanying text.
[148] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[149] *See* Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities* (Apr. 28, 2017), *available at* https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml ("NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate 'about' communications from its upstream 702 collection without also excluding some of the relevant communications directly 'to or from' its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.").

simultaneously adopts procedures allowing it to search the data for particular Americans' communications.

Section 702 surveillance also can result in the "incidental" collection of other types of sensitive data that do not receive full Fourth Amendment protection but that Congress has chosen to protect by statute. Depending on the data in question, the government may be required to obtain a court order (e.g., under 18 U.S.C. §2703(d) or Section 215 of the U.S.A. Patriot Act[150]) or a subpoena (e.g., under §2703(c)(2) or with a National Security Letter) to obtain it. Before performing a U.S. person query of such data, agencies should be required to follow the legal process that would apply if the agencies were collecting the data in the first instance.

The FBI has pointed out that its databases contain information from multiple sources, and other agencies may also conduct federated searches that run against multiple data sets. Section 702 data, however, is specially tagged to enable compliance with notification requirements as well as legal limitations on who may access it. Currently, if an FBI agent performs a query that returns Section 702 data, the agent is notified of its 702 status. The systems could instead be configured not to return Section 702 data at all, unless the agent enters into the system a certification, accompanied by supporting documentation, that one of two conditions is met: (1) the query term is associated with someone reasonably believed to be a foreigner overseas, or (2) the government has obtained the required warrant, court order, or subpoena.

Indeed, with or without a warrant requirement, the system should be configured not to return Section 702 data unless agents, at the time they perform the query, enter a certification and supporting documentation indicating that they have complied with the applicable restrictions. It is unclear whether this technical barrier will succeed in preventing violations of querying limits. What is clear is that nothing short of such a barrier has any chance of doing so. The record establishes that if a query returns Section 702 information in the first instance, FBI agents will frequently access that information regardless of any rules prohibiting such access.

Based on the fact that the FBI ran 1.9 million U.S. person queries relating to potential victims of cyberattacks in 2021, the government will likely argue that a warrant requirement would be unworkable for cybersecurity investigations. If a search of non-contents information could suffice in these instances, however, agencies could proceed with something less than a warrant. In any event, as part of the proposed investigation into the uses of Section 702 for cybersecurity purposes, the PCLOB should thoroughly probe any claim of unworkability. For queries of communications content and other Fourth Amendment-protected information, an exception to the warrant requirement should be made only if there is an applicable exemption under Fourth Amendment jurisprudence. In addition, any such exception — along with any exception from the court order/subpoena requirement when accessing other types of sensitive data — should be as narrowly drawn as possible, and it should be combined with protections to ensure that non-pertinent content is not subject to manual review.

---

[150] Although Section 215 expired in 2020, it is still available for investigations commenced before the provision expired, as well as investigations into actions that took place before the expiration. *See* USA Patriot Act Improvement and Reauthorization Act, Pub. L. 109-177, 109th Cong. § 102(b)(2) (2005) (as amended by Pub. L. 116-69, 116th Cong. § 1703(a) (2019)).

In addition to these limits on querying, the PCLOB should recommend that Congress add specificity to its definition of "minimization." In the absence of objective statutory criteria, there has been a predictable steady slide toward wider sharing of raw data, greater access to the data by agency personnel, and more exceptions to retention limits. On retention in particular, Congress should clarify that keeping Americans' information for five years, and for even longer in cases where that information has been reviewed and no determination of its status has been made, is not "minimization." Congress should specify that all information not subject to a "litigation hold" shall be destroyed within three years of the authorization for the acquisition, unless it has been reviewed and determined to be foreign intelligence or evidence of a crime.[151]

C. Modernize FISA by Establishing Basic Rules and Requiring FISA Court Oversight for Executive Order 12333 Surveillance

The fact that EO 12333 surveillance is subject to almost no legislative limits and no judicial oversight is a constitutionally untenable anachronism, rooted in modes and methods of communication that no longer exist. Overseas surveillance today — whether targeted or in bulk — results in the collection of Americans' communications and other personal information, almost certainly in massive amounts. And there are holes in FISA's coverage that allow the government to target Americans under EO 12333 and collect sensitive non-contents information within the United States. The Supreme Court has made clear that the Constitution "most assuredly envisions a role for all three branches [of government] when individual liberties are at stake."[152] That is undeniably the case here.

The PCLOB should recommend that Congress bring certain aspects of EO 12333 surveillance within FISA. Reauthorization of Section 702 is the best vehicle for accomplishing this. After all, the primary distinction between Section 702 surveillance and EO 12333 surveillance is the location of the collection (or of the companies from which the information is collected), and that has become a distinction without a difference when it comes to Americans' privacy. Any reauthorization of Section 702 should recognize this reality and address EO 12333 surveillance as well.

As a threshold matter, Congress should provide that existing FISA authorities constitute the exclusive means by which the government may conduct any type of foreign intelligence collection (not just "electronic surveillance") that targets U.S. persons, obtains wholly domestic communications, takes place inside the United States, or obtains information from U.S. companies. This would prevent the government from evading FISA's legal processes for

---

[151] In its review of the NSA's bulk collection program, the PCLOB concluded that the collected metadata began to lose its usefulness after three years. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 170 (2014), *available at* https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf. It seems likely that this would also be true for the data obtained under Section 702. Of course, information that has been reviewed and determined to constitute foreign intelligence information or evidence of a crime could be retained for longer periods.

[152] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

obtaining sensitive non-contents information by purchasing that information from data brokers or employing similar workarounds.[153] Congress should then establish basic rules for foreign intelligence collection that does not target U.S. persons or obtain wholly domestic communications, that takes place outside the United States, and that does not involve collection from U.S. companies — collection that currently takes place solely under EO 12333.

The first such rule should be to prohibit bulk collection. The dangers of bulk collection are discussed in Part IV. In brief, as the Court of Justice for the European Union has recognized, bulk collection cannot be reconciled with respect for the privacy rights of foreign nationals. It also opens the door to the "incidental" collection of vast quantities of Americans' personal data, including purely domestic communications and related records. Notably, even though Section 702 has a targeting requirement, the intelligence community has consistently described it as one of the most effective tools in its arsenal; the government has never suggested that the targeting requirement makes Section 702 less effective or results in the loss of vital intelligence.

Next, Congress should address the permissible targets of EO 12333 surveillance. Congress should codify the legitimate objectives set forth in President Biden's recent executive order (with modifications[154]) and require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to produce information directly relevant to one or more objectives. Congress also should specify that, unless the surveillance is highly unlikely to result in the acquisition of U.S. person information, the target must be a foreign power or agent of a foreign power.

As for U.S. person information "incidentally" collected under EO 12333, there is no principled justification for giving this information less protection than similar information "incidentally" acquired through Section 702. In both cases, Congress should require agencies to obtain a warrant, court order, or subpoena to perform a U.S. person query, depending on the type of data being queried. And Congress should tighten the existing statutory limits on retention of incidentally-collected EO 12333 data — the only aspect of EO 12333 surveillance that has ever been made subject to legislation[155] — by changing the retention period from five years to three years and eliminating the many exemptions.

Finally, surveillance activities under EO 12333, with the exception of activities that are highly unlikely to result in the acquisition of U.S. person information, should be subject to oversight by the FISA Court. When it comes to protecting and preserving Americans' constitutional rights, judicial review is indispensable. The fact that the government has been able to collect, store, and access Americans' communications for decades without the possibility of judicial review in any forum is a glaring departure from the rule of law and constitutional principles.

---

[153] *See Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (Jul. 19, 2022) (testimony of Elizabeth Goitein), *available at* https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf.
[154] See *supra* note 141 and accompanying text.
[155] *See* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293, 113th Cong. § 309 (2014).

EO 12333 surveillance activities affecting U.S. persons should be authorized by the FISA Court on an annual basis, in a manner similar to Section 702 surveillance. Court approval of such surveillance activities would be contingent on a finding that they comport with FISA (as amended), the Constitution, and the relevant executive orders and agency policies. Agencies should be required to report incidents of non-compliance to the FISA Court immediately upon detection and implement any remedies the Court may order. The government should be required to conduct declassification reviews of significant FISA Court opinions and make them public, with redactions as necessary to protect properly classified information.

These changes will help bring FISA fully into the twenty-first century. In 2007 and 2008, the government observed that changes in technology had resulted in purely foreign communications being stored in the United States, forcing the government to obtain a FISA Court order to collect them. But of course, the converse was true as well: Those same changes in technology meant that Americans' communications were being routed and stored overseas in a way that stripped them of FISA's protections. The government sought and obtained a (markedly overbroad) solution to the first half of the problem. Congress must now address the second half, however belatedly. The PCLOB should urge Congress to complete the unfinished business of modernizing FISA by bringing EO 12333 surveillance that affects Americans within its reach.

D. Increase Transparency and Accountability

The PCLOB should recommend that Congress enact various reforms to increase the transparency and accountability of Section 702 and EO 12333 surveillance.

1. Require Reporting on U.S. Person Queries, Additional Reporting on EO 12333 Surveillance, and an Estimate of Incidental Collection Under Section 702

To ensure informed decision-making by lawmakers and the public, more information is needed about the impact of Section 702 and EO 12333 surveillance on Americans. The PCLOB should recommend three reforms in this area.

First, Congress should require *all* agencies that are authorized to perform U.S. person queries, including the FBI, to report how many times they perform such queries on an annual basis. This year, the government voluntarily reported how many U.S. person queries of Section 702 data it conducted in calendar years 2020 and 2021. Congress should make clear that continued reporting of this number is mandatory, and it should extend this requirement to U.S. person queries of information acquired under EO 12333.[156] This obligation should remain in place even if Congress enacts a warrant requirement for U.S. person queries. Lawmakers and the public need this information to understand and evaluate the impact on Americans of surveillance authorities that are nominally directed at foreigners overseas.

[156] Responsibly tracking how U.S. person information acquired under EO 12333 is maintained and accessed might require a reconfiguration of existing data systems. If so, this requirement could be phased in over a reasonable time period.

Second, assuming Congress brings aspects of EO 12333 surveillance under FISA, it should extend existing Section 702 reporting requirements to such surveillance. In particular, the government should report on FISA Court adjudications of EO 12333 surveillance activities (50 U.S.C. § 1873(a)); numbers of targets and queries (50 U.S.C. § 1873(b)(2)); and numbers of notifications in criminal proceedings, as discussed below (50 U.S.C. § 1873(b)(4)).

Third, if intelligence agencies refuse to work with the PCLOB to develop an estimate of how many Americans' communications are obtained under Section 702, the PCLOB should recommend that Congress require the government to provide such an estimate. As noted above, the FBI claimed for years that there was no workable way to count how many U.S. person queries it performs. But after Congress required the Bureau to keep records of such queries, and after the FISA Court made clear that the FBI could not dodge this requirement, the FBI produced the number.

2. Remove Barriers to Review by Regular Article III Courts

The PCLOB should recommend that Congress address the barriers that are blocking legal challenges to unlawful foreign intelligence surveillance.

Even though Congress clearly intended for defendants to be able to challenge the use of Section 702-derived evidence in criminal cases, the government's notification policies are thwarting this intent. Congress should clarify that evidence is "derived" from Section 702 surveillance if the government would not otherwise have possessed this evidence, regardless of any claim that the evidence is attenuated from the surveillance, would inevitably have been discovered, or was subsequently reobtained through other means.

Congress also clearly intended for civil lawsuits to serve as a means to challenge electronic surveillance activities. Two doctrines are frustrating this intent: standing and the state secrets privilege. With respect to standing, Congress should specify that a person has standing to bring a civil lawsuit if she has a reasonable basis to believe her information has been (or will be) acquired, and if she has expended (or will expend) time or resources in an attempt to avoid acquisition. With respect to the state secrets privilege, Congress should amend section 1806(f) of FISA — which governs courts' review of national security information in electronic surveillance cases — to clarify that this subsection displaces the normal operation of the privilege. Such clarification is needed in light of the Supreme Court's recent ruling in *FBI v. Fazaga*,[157] which held that section 1806(f) does not displace the privilege — a holding that will effectively nullify 1806(f)'s application to civil lawsuits and stymie accountability for unlawful surveillance.[158]

Finally, Congress should ensure that criminal defendants and civil plaintiffs are able to bring challenges when they are victims of unlawful EO 12333 surveillance. To that end, Congress should require the government to notify parties to legal proceedings when it intends to

[157] 142 S. Ct. 1051 (2022).
[158] *See* Elizabeth Goitein, *The State Secrets Sidestep:* Zubaydah *and* Fazaga *Offer Little Guidance on Core Questions of Accountability*, CATO S. Ct. Rev. (2022): 193–225, *available at* https://www.cato.org/sites/cato.org/files/2022-09/Supreme-Court-Review-2022-Chapter-8.pdf.

introduce evidence obtained or derived from EO 12333 surveillance (using the above definition of "derived"). It should apply the criteria for standing in Section 702 challenges to EO 12333 challenges. And it should extend the reach of section 1806(f) to proceedings where EO 12333 surveillance is at issue.

3. Improve the functioning of the FISA Court

The PCLOB should recommend that Congress enact the reforms to FISA Court proceedings set forth in the "Lee-Leahy" amendment — an amendment to the USA Freedom Act Reauthorization Act of 2020 offered by Senators Mike Lee and Patrick Leahy.[159] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[160]

The amendment seeks to ensure that the panel of *amici* established in the USA Freedom Act provide the FISA Court with a perspective other than the government's —including a presentation of any privacy and civil liberties concerns — in the cases where such a perspective is most needed; that *amici* have access to the materials they need to do their job; that the government has court-approved procedures in place to ensure the accuracy of its submissions to the FISA Court; and that the government informs both the FISA Court and *amici* of any exculpatory evidence in its possession. There is no legitimate argument against such basic accountability-enhancing measures, which is why the amendment received such a strong showing of support in 2020.

***

An important caveat is in order. While reforms that promote transparency and accountability are critical, they are not a substitute for limiting the scope of Section 702 surveillance, shoring up privacy protections for Americans whose communications are "incidentally" collected, and establishing basic rules for EO 12333 surveillance. The most stringent of oversight provisions cannot justify amassing the personal data of ordinary, law-abiding private citizens. Nor can they legitimize the warrantless searching of Americans' phone calls and e-mails. Procedural protections are only as good as the substantive rights and limitations they enforce. That is why Congress should reform Section 702 to bolster those rights and limitations while preserving the core of the statute: warrantless surveillance of foreigners who pose a threat to our nation.

Conclusion

Since Section 702 was last reauthorized, it has become increasingly apparent that its impact on Americans is anything but "incidental." Intelligence agencies are leveraging this authority on a systemic basis to access Americans' communications and other personal information in ways that violate FISA, the Constitution, and court-ordered policies. Congress should not reauthorize Section 702 without sweeping reforms. The PCLOB can play two vital

[159] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020).
[160] *Id.* (as agreed to in Senate, May 13, 2020).

roles in this process: procuring information that will assist in developing reforms, and recommending the changes Congress must enact to bring Section 702 surveillance in line with Americans' constitutional rights and legitimate privacy expectations.

Respectfully submitted,

Elizabeth Goitein
Senior Director
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue, NW
Eleventh Floor
Washington, DC 20036

PUBLIC SUBMISSION

As of: 11/8/22, 8:47 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-2y9d-qvhg
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0031
Comment on FR Doc # 2022-20415

Submitter Information

Email: baumohl@epic.org
Organization: Electronic Privacy Information Center

General Comment

See attached file(s)

Attachments

EPIC PCLOB Section 702 Comments_Final

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

PUBLIC SUBMISSION

As of: 11/8/22, 8:49 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-4ilp-dzfg
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0032
Comment on FR Doc # 2022-20415

Submitter Information

Email: sarkesian@opentechinstitute.org
Organization: New America's Open Technology Institute

General Comment

See attached file(s)

Attachments

OTI Comments to PCLOB re 702 - 11.4.22

November 4, 2022

To the Members of the Privacy and Civil Liberties Oversight Board:

New America's Open Technology Institute submits the following comments detailing the organization's views and recommendations regarding the surveillance operated under Section 702 of FISA, in anticipation of the December 2023 sunset date and the upcoming public and Congressional consideration of its reauthorization, and in response to Privacy and Civil Liberties Oversight Board ("PCLOB") request for public comment. These comments are intended to aid the PCLOB in its research and recommendations as it examines the adequacy of existing privacy and civil liberties safeguards with respect to FISA Section 702 programs.

Narrowing the Definition of Foreign Intelligence

FISA Section 702 allows for broad targeting due to its sweeping definition of what constitutes "foreign intelligence." When Section 702 became law in 2008, it was sold to Congress and the public as authorizing surveillance that was necessary to stop terrorist threats and espionage. Yet, Section 702 permits surveillance that goes well beyond protecting national security. The definition for foreign intelligence information also permits surveillance that is merely relevant to the foreign affairs of the United States.[1] The "foreign affairs" provision of the definition of foreign intelligence information is not necessary to national security, and allows the NSA to sweep up the communications of political or human rights activists, journalists, students, and business people working abroad, and it should be struck from the authorized purposes for surveillance under Section 702.

The expansive FISA definition of foreign intelligence information includes such matters as those relating to the national defense and foreign affairs of the United States. And, under Section 702, targets can be any non-U.S. person, regardless of that person's level of connection to a foreign power.[2] The targeting procedures require that the surveillance of the target must be likely to lead to the collection of foreign intelligence information within the scope of one of the "certifications" or topics for which surveillance has been approved by the FISA Court—such as counterterrorism or weapons of mass destruction. This standard could permit targeting of people who may unwittingly or unknowingly possess information that meets the broad definition of "foreign intelligence." It has remained unclear whether the intelligence agencies interpret this

[1] 19 50 U.S. Code § 1801.
[2] 19 50 U.S.C. § 1881(a).

definition quite as expansively as the language appears to allow, both with respect to foreign persons and U.S. persons.

President Biden's October 7 2022 Executive Order on safeguards for signals intelligence activities seems aimed to narrow the definition of foreign intelligence by setting out twelve "legitimate objectives" for collection.[3] However, as experts have already begun to point out, as applied to Section 702 surveillance, while the twelve objectives effectively narrow the statutory definition of "foreign intelligence" set forth in the statute, the caveats in the Executive Order are quite significant, calling into question whether the definition will in fact be narrower.[4]

For example, the third listed legitimate objective is quite expansive: "understanding or assessing transnational threats that impact global security, including climate and other ecological change, public health risks, humanitarian threats, political instability, and geographic rivalry".[5] It is difficult to know at this point whether and how this could limit the definition further than the "foreign affairs" provision already in the definition. Other terms in the legitimate objectives are likewise unclear and potentially broad in scope. The first objective would allow surveillance to understand or assess the capabilities, intentions, or activities of a foreign government, a foreign military, a faction of a foreign nation, or a "foreign-based political organization," which remains undefined. Finally, the October Executive Order gives the president authority to expand the list of objectives—and to do so secretly, if publishing the updated list "would pose a risk to the national security of the United States," again underscoring the need for Congress to take action and better define what constitutes lawful surveillance under Section 702.

In the course of its review, perhaps the PCLOB can clarify to the public how the twelve legitimate objectives of surveillance differ from surveillance under the more traditional FISA Section 702 definition, and therefore whether and how the new Executive Order does limit surveillance.

Strengthening & narrowing targeting standards

Further, the government should strengthen and narrow the standard for targeting under Section 702 from "reasonably likely to return" foreign intelligence information related to one of the 702 certifications. As other advocates have pointed out, "...the scale of Section 702 surveillance has dramatically increased in the years since PCLOB last released a full report on this topic" due to

[3] Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Oct. 7 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.
[4] Elizabeth Gotein, The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance, Just Security, October 31, 2022, https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/.
[5] Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Oct. 7 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

the steady increase in targets over the years.[6] When the last PCLOB report on Section 702 was released in 2018,[7] there were 89,138 targets[8] – according to the latest Statistical Transparency Report, that figure is now 232,432 targets.[9] This dramatic growth of Section 702 surveillance for both non-U.S. persons, and U.S. persons alike, whose data is incidentally swept up in the course of foreign intelligence collection. The PCLOB should seek to both understand the reasons for this increase in surveillance, and find recommendations that might narrow the targeting standards while not being overly restrictive so as to harm intelligence collection.

Prohibit "About" Collection and Upstream Surveillance

Congress should ensure that the government cannot reinstate "about" collection under Section 702, ensuring that the NSA only collects communications that are "to" or "from" a target. As part of its "upstream" surveillance under Section 702, the NSA used to collect communications that merely reference, or are "about," a target, such as when the email address for a target appears in the body of an email. "About" collection therefore could sweep up communications that are neither to nor from an approved target, creating a significantly greater risk of including the communications of people with no connection to wrongdoing or foreign intelligence. In 2017, the NSA announced that, as a result of persistent compliance issues, it would stop the practice of certain types of "about" collection and delete its stores of U.S. person communications that were obtained via that form of surveillance, claiming that the threat to Americans' privacy outweighed any value from the collection.[10]

Though the NSA suspended "about" collection in 2017 based on its inability to conduct this collection in compliance with applicable privacy protections, the statute permits the NSA to restart "about" collection after obtaining permission from the FISA Court and notifying Congress. Further, c*onsidering* the harmful impact "about" collection has on Americans' privacy, which NSA has recognized, it is indefensible to allow space for the NSA to restart this practice. Congress should pass a reform bill that includes a prohibition against "about" collection. To guarantee a more permanent limit on overbroad surveillance, Congress should also pass a reform bill that includes a prohibition against "about" collection.

Further, through NSA's "Upstream" surveillance program, the NSA is able to sweep up excessive amounts of data, as the government systematically monitors the "backbone of the

---

[6] Jake Laperruque, Testimony to the Privacy and Civil Liberties Oversight Board, Aug. 17, 2020, https://www.pogo.org/testimony/2020/08/testimony-in-support-of-increased-transparency-and-reform-of-fisa-surveillance.
[7] Privacy and Civil Liberties Oversight Board, Report on Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2, 2014, https://irp.fas.org/offdocs/pclob-702.pdf.
[8] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, Statistical Transparency Report Regarding Use of National Security Authorities Annual Statistics for Calendar Year 2013, https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.
[9] Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2021, https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.
[10] https://www.nsa.gov/news-features/press-room/press-releases/2017/.

internet" across which about 80% of global internet traffic transits.[11] This practice is incredibly privacy-invasive, as it subjects everyone's communications to automated scans by the NSA, and is designed to gather all of Americans' international communications, including emails, web-browsing content, and search engine queries, with the help of providers.

As plaintiffs have argued in *Wikimedia v. NSA*,[12] NSA intercepts and copies private communications in bulk while they are in transit, and then searches their contents using tens of thousands of keywords associated with NSA targets, which are chosen by intelligence analysts, and never approved by any court. As the ACLU and plaintiffs have argued, through these general, indiscriminate searches and seizures of Wikimedia's communications, Upstream surveillance invades their Fourth Amendment right to privacy, infringes on their First Amendment rights to free expression and association, and exceeds the statutory limits of Section 702 itself.[13] Unfortunately, the case has been dismissed on "state secrets" privilege grounds, but plenty is known about the government's use of the program already, as the PCLOB detailed in its 2014 report.[14]

When Congress debated the passage of Section 702, it never considered whether the NSA should have such broad authority to intercept internet communications and nothing in the statute suggests this type of surveillance is appropriate.

The PCLOB should seek to make more information publicly available, transparent, and understood as to how Upstream collection works and the widespread impact of this surveillance, so that Congress can make appropriate reforms and likely disallow such collection in 2023.

Close the "Backdoor Search" Loophole

Though Section 702 prohibits targeting of Americans, its programs also sweep up Americans' communications at a scale much larger than the public and many in Congress ever conceived, allowing for routine warrantless searches of Americans' information. (These communications can include Americans' phone calls, e-mails, and other electronic communications.) For years, civil liberties advocates have drawn attention to and pushed against this government practice of conducting warrantless "backdoor" searches, as they constitute a dangerous end-run around the Fourth Amendment.[15] Congress has also prioritized this issue, as amendments have repeatedly been considered and overwhelmingly passed the House of Representatives twice in the past (in 2014 and 2015) on a bipartisan basis.[16]

The intelligence community considers such collection "incidental". But without any judicial oversight or approval, the FBI then conducts routine and unlimited warrantless searches of that

[11] http://www.nybooks.com/articles/2013/08/15/nsa-they-know-much-more-you-think/
[12] *Wikimedia Found. v. NSA*, No. 1:15-cv-00662-TSE (D. Md.), No. 15-2560 (4th Cir.).
[13] https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance
[14] PCLOB Section 702 Report, 2014.
[15] Coalition Letter Urging Reforms to FISA Section 702, https://www.aclu.org/letter/coalition-letter-urging-reforms-section-702-fisa.
[16] https://clerk.house.gov/evs/2014/roll327.xml; https://clerk.house.gov/evs/2015/roll356.xml.

database for Americans' communications, and even uses that information in ordinary criminal investigations and prosecutions, undermining Americans' Fourth Amendment protections.[17] This could include everything from theft to fraud, drug offenses, violent offenses, copyright law violations, or any other crime, even if it is entirely unrelated to national security. Various Foreign Intelligence Surveillance Court opinions and other transparency documents have shown widespread abuse of this practice.[18] These privacy violations underscore the significant threat that the backdoor search loophole poses to the rights of people in the United States, demonstrating the need for court approval of any searches of Section 702 information about U.S. persons.

Congress should again consider closing this "backdoor search" loophole, by prohibiting searches looking for information about U.S. persons absent a probable cause warrant, a recommendation that the PCLOB should explore.

Enhance Post-Collection Protections for Americans' Communications that are Swept Up Under Section 702

While narrowing the scope of surveillance under Section 702 is critically important, it will still result in a large quantity of incidental collection of Americans' communications. For this reason, enhancing the protections for that information once it is in the intelligence community's databases is also essential. Section 702 requires the government to adopt minimization procedures "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[19] The minimization procedures must be approved by the FISA Court on an annual basis. Each participating intelligence agency has adopted its own Section 702 minimization procedures, which generally include use limitations, retention limits, and rules regarding dissemination or sharing of information.

Under Section 702, the Querying Procedures for both the NSA and the CIA provide that all queries, regardless of the search terms used, "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, unless otherwise specifically excepted in these procedures."[20] The FBI's Section 702 Querying Procedures add an additional permissible

---

[17] Sharon Bradford Franklin, Just Security, "The House Intelligence Committee's Section 702 Bill is a Wolf in Sheep's Clothing," January 9, 2018. https://www.justsecurity.org/50801/house-intelligence-committees-section-702-bill-wolf-sheeps-clothing/.

[18] Jake Laperruque, Just Security, "Key Takeaways From the Latest FISA Court Opinion on Section 702 and FBI Warrantless Queries", April 28, 2021, https://www.justsecurity.org/75917/key-takeaways-from-latest-fisa-court-opinion-on-section-702-and-fbi-warrantless-queries/.

[19] 50 U.S.C. § 1821(4).

[20] NSA Querying Procedures Pursuant to Section 702 (2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_NSA_Querying_17Sep19_OCR.pdf; CIA Querying Procedures Pursuant to Section 702 (2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_CIA_Querying_17Sep19_OCR.pdf.

purpose of reasonably likely to retrieve "evidence of a crime."[21] For U.S. person queries, there are also certain procedural requirements designed to impose some rigor to the process. When either the NSA or CIA seeks to conduct a U.S. person query, the agent must produce "a statement of facts showing that the use of that query term" will be reasonably likely to return foreign intelligence information. For the NSA, the procedures also require that any U.S. person query term must first be approved by the NSA's Office of General Counsel, and such approvals will expire after one year unless they are renewed during that time. The FBI's Querying Procedures are somewhat more complicated, but generally require that the FBI produce a statement of facts showing that the query term meets the standard before an agent may review information returned from conducting a U.S. person query. In some limited circumstances, before the FBI accesses the information they need to obtain an order from the FISA Court.[22]

By contrast, when any of these agencies conducts Section 702 queries using terms associated with a particular non-U.S. person, there are no similar documentation or process requirements. For non-U.S. person queries, no agency is required to prepare a written statement of facts showing that the query meets the "reasonably likely to return" standard. Nor is there any requirement, like the one the NSA applies for U.S. person query terms, for prior approval of non-U.S. person query terms.

There has been a significant amount of debate in the United States over strengthening the standards for when it is permissible to conduct U.S. person queries, and it is still critical that the government strengthen those standards.[23] Queries are a critical tool through which U.S. intelligence agencies process data, and processing safeguards for non-U.S. persons are direly needed.

As we have suggested prior, at a minimum, under Section 702, the U.S. government should extend the requirement for a supporting statement of facts to cover all queries seeking information about any specific person, regardless of that person's nationality or location.[24] As noted above, NSA and CIA personnel are already required to document the basis for their U.S. person queries, and the government should expand application of this rule to all agencies participating in Section 702 and to non-U.S. person queries. The rationale for mandating documentation is that it induces agents to think through, and support with facts, their assessment that using the query term will actually meet the query standard. A requirement for a statement of facts in support of query terms will therefore help ensure that queries actually meet

---

[21] FBI Querying Procedures Pursuant to Section 702 (2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Querying_17Sep19_OCR.pdf.
[22] FBI Querying Procedures, Section 4(A), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FBI_Querying_17Sep19_OCR.pdf.
[23] *See* Sharon Bradford Franklin, What Happened at the Court: The Hasbajrami Oral Argument on Section 702 of FISA and the Fourth Amendment, *Just Security* (August 29, 2018), https://www.justsecurity.org/60505/happened-court-hasbajrami-oral-argument-section-702-fisa-fourth-amendment/.
[24] Sharon Bradford Franklin et. al, New America's Open Technology Institute, Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform, April 7, 2021, https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/#authors.

the standard—"reasonably likely to return" foreign intelligence information—that already applies to all queries under Section 702.

Increasing Transparency and Other Oversight Mechanisms

The PCLOB should seek to provide greater transparency to the public regarding Section 702 surveillance programs, procedures, and impact. Greater transparency for the rules governing U.S. surveillance and the scope and scale of data collection would help promote accountability, and provide a check to show that collection is proportionate to intelligence needs. In particular with regard to collection under Section 702, the government should disclose the categories that are the subjects of the certifications approved by the FISA Court. Thus far, the Intelligence Community has disclosed that these subjects include counterterrorism and addressing weapons of mass destruction, but they have not declassified the full list of categories covered by the Section 702 certifications.

While greater transparency is needed[25] and will benefit U.S. and non-U.S. persons alike, it is important to note that any transparency measures should serve as a supplement Congressional efforts to reform collection, targeting, and minimization rules.

In addition to these critical reforms, Congress should consider other important reforms to Section 702, such as strengthening the role of the Court-appointed FISA Amicus, a measure which received robust support in 2020 when Congress last considered surveillance reform.[26] The PCLOB should consider recommending that Congress include this reform in 702 reauthorization by adopting the 2020 Leahy/Lee amendment to USA FREEDOM, which would significantly expand the types of cases in which amici are authorized to participate, beyond cases raising "novel and significant" issues, to also include:

- cases that present "significant concerns" regarding activities protected by the First Amendment;
- "sensitive investigative matters," which are defined to include matters involving domestic public officials or candidates for office, news media, and religious or political organizations;
- matters involving a request for approval of a new program, a new technology, or a new use of existing technology; and
- requests for reauthorization of programmatic surveillance, which would include the annual renewals of authority to conduct surveillance under Section 702 of FISA.[27]

The PCLOB should also recommend that Congress expand the ability of the amici to access information relevant to the matters in which they appear, and as both the House and Senate versions of the USA FREEDOM Reauthorization Act would have done, Congress should provide a procedure for the amici to seek appellate review of decisions as well.

[25] Sharon Bradford Franklin, Statement to the Privacy and Civil Liberties Oversight Board, Aug. 31, 2020 https://d1y8sb8igg2f8e.cloudfront.net/documents/Sharon_Bradford_Franklin_Comments_to_PCLOB_on_FISA_8-31-20.pdf.
[26] https://www.lee.senate.gov/2020/5/senate-passes-lee-leahy-fisa-amendment.
[27] https://www.congress.gov/amendment/116th-congress/senate-amendment/1584/text.

Conclusion

We appreciate the opportunity to provide these comments as the PCLOB continues in protecting the privacy and civil liberties of Americans through its ongoing oversight and review of FISA Section 702. Please do not hesitate to contact Lauren Sarkesian at sarkesian@opentechinstitute.org if we can provide any further information.

Respectfully submitted,

New America's Open Technology Institute

PUBLIC SUBMISSION

As of: 11/8/22, 8:49 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-5p5f-u69t
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0033
Comment on FR Doc # 2022-20415

Submitter Information

Email: sean@demandprogress.org
Organization: Demand Progress Education Fund

General Comment

See attached file(s)

Attachments

Demand Progress Education Fund PCLOB Section 702 Comments

Demand Progress Education Fund's Comments for the Privacy and Civil Liberties Oversight Board's Oversight Project Examining Section 702 of the Foreign Intelligence Surveillance Act
PCLOB-2022-03

November 4, 2022

Dear Chair Franklin and Board Members DiZinno, Felten, LeBlanc, and Williams:

Thank you for inviting comment on the Privacy and Civil Liberties Oversight Board's (the "Board") Oversight Project to examine the surveillance program that the Executive Branch operates pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA). The Board plays a critical role investigating intelligence activities that affect civil liberties of U.S. persons, exercising oversight, offering advice, and providing transparency to the public.

The Board's examination of Section 702-related activities is an important opportunity to inform Congress and the public about the extent and significance of known violations of the applicable rules and laws, about unclear and unknown violations, and about a variety of other aspects of this surveillance that are necessary to inform impending, major policy decisions. This examination further provides a rare opportunity to make recommendations to intelligence agencies regarding their use of Section 702. Accordingly, we urge the Board to specifically investigate the following questions, disclose specific additional information, and issue the following recommendations.

I. The Board should release assessments comparing the volume of records CIA, FBI, NCTC, and NSA acquire pursuant to Section 702 and the records to which these agencies have access in exchange for anything of value absent a court order

Since the Board's last report on Section 702, Congressional inquiries and investigative reporting have unearthed a disturbing and opaque practice: government agencies buying their way around the Fourth Amendment. One recent report revealed that "[m]ultiple branches of the U.S. military have bought access to a powerful internet monitoring tool that claims to cover over 90 percent of the world's internet traffic, and which in some cases provides access to people's email data, browsing history, and other information such as their sensitive internet cookies."[1] Agencies engaging in this practice include, at least, the Department of Defense, Department of Homeland Security (including Customs and Border Protection and Immigration and Customs

[1] Joseph Cox, "U.S. Military Bought Mass Monitoring Tool that Includes Internet Browsing, Email Data," *Motherboard (Vice)*, September 21, 2021, https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data.

Enforcement), the Drug Enforcement Administration, the Federal Bureau of Investigation (FBI), the Internal Revenue Service, and the Secret Service.[2]

The FBI, which has multiple contracts with data brokers and modified its agreement with one in the immediate aftermath of the murder of George Floyd,[3] has a particularly disturbing track record as it relates to Section 702, discussed further in Section III. As Congress and the public generally consider whether and with what changes Section 702 should be reauthorized next year, it will be critical to have a trusted, public assessments of:

> (1) the volume of information the FBI is acquiring pursuant to Section 702 relative to the volume of information it is acquiring or acquiring access to in exchange for anything of value without a court order;
> (2) the extent to which the FBI is purchasing records or access to records to which it has or could have access pursuant to Section 702; and
> (3) the extent to which Section 702 produces for the FBI records to which it has access through the purchase of records or access to records.

This information would at least inform policymakers of the relative use and value of these two methods of acquiring information in certain contexts, including the extent to which the FBI may be circumventing privacy protections that would apply to data were it to be acquired under Section 702.

Further, the Board should assess to what extent the FBI's purchase of records or access to records may inform its nomination decisions under Section 702 and how Section 702 information may guide its purchase of information or access to it — either of which could supercharge these practices and significantly change the civil liberties implications of reauthorizing Section 702.

Although the National Security Agency (NSA) has not been directly implicated in the purchase of records that would otherwise require a court order to compel the production of, the Department of Defense has.[4] And although the Central Intelligence Agency (CIA) and National

---

[2] *See* Sara Morrison, "A Surprising Number of Government Agencies Buy Cellphone Data Records. Lawmakers Want to Know Why," *Vox*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Paul Blest, "ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says," *Vice*, February 7, 2020, https://www.vice.com/en/article/v7479m/ice-is-using-location-data-from-games-and-apps-to-track-and-arrest-immigrants-report-says; Joseph Cox, "Secret Service Bought Phone Location Data from Apps, Contract Confirms," *Motherboard (Vice)*, August 17, 2020, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street; Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Data Without Warrants, Memo Says," *The New York Times*, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," *The Wall Street Journal*, June 19, 2020, https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.

[3] Lee Fang, "FBI Expands Ability to Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show," *The Intercept*, June 24, 2020, https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/.

[4] Joseph Cox, "Pentagon Surveilling Americans Without a Warrant, Senator Reveals," *Motherboard (Vice)*, May 13, 2021,

Counterterrorism Center (NCTC) have also not been directly implicated, other revelations relating to a still-secret report by the Board about CIA activities under Executive Order 12333 appear alarmingly consistent with the practice of purchasing records, in particular that the CIA's activities occur "without any of the judicial, congressional or even executive branch oversight that comes with FISA collection."[5] To the extent that the CIA, NCTC and NSA similarly engage in the purchase of records or access to records that could be obtained pursuant to Section 702, the Board should make the same assessments identified above.

II. The Board should investigate and disclose additional information about a recently revealed Inspector General report into SIGINT misuse, recommend minimum punitive measures for misuse, and recommend additional transparency around such activity

On November 1, 2022, Bloomberg News revealed a 2016 report by the NSA Office of the Inspector General (IG) that examined misuse of SIGINT systems.[6] While the Board should generally supplement the available public record on agencies' violations of Section 702 minimization procedures, FISC orders, and statutes, the Board should also examine and disclose information about the activities at the heart of this report in particular, which the IG report says involve "the possible violation of Titles I and/or VII of the Foreign Intelligence Surveillance Act."[7] Title VII of FISA, as the Board is aware, includes Section 702, and the unredacted details underscore the likelihood of Section 702's involvement.

The IG report described "substantiated" complaints from 2013 that an NSA analyst "had improperly tasked United States Person (USP) [redacted] phone numbers [redacted] for collection," allegedly "without proper authorization and without a foreign intelligence purpose."[8] The whistleblower who alleged misuse further "claimed that the tasking records [redacted] had been improperly entered [redacted]."[9] Alarmingly, officials with knowledge could not determine whether the activity violated the law because, "many of them told the OIG, they did not understand the work [redacted] performed."[10]

---

https://www.vice.com/en/article/88ng8x/pentagon-americans-surveillance-without-warrant-internet-browsing.

[5] Letter from Sens. Martin Heinrich and Ron Wyden to Dir. of Nat'l Intelligence Avril D. Haines and Dir. of the Cent. Intelligence Agency William J. Burns (April 13, 2021), https://www.wyden.senate.gov/imo/media/doc/HainesBurns_WydenHeinrich_13APR21%20-FINAL.pdf.

[6] Jason Leopold, Katrina Manson, William Turton, "NSA Watchdog Concluded One Analyst's Surveillance Project Went Too Far," *Bloomberg News*, November 1, 2022, https://www.bloomberg.com/news/articles/2022-11-01/nsa-watchdog-concluded-one-analyst-s-surveillance-project-went-too-far.

[7] Misuse of SIGINT Systems, Office of the Inspector General of the Nat'l Security Agency/Cent. Security Service, February 12, 2016, at 2 (hereinafter "IG Report"). Available at: https://s3.documentcloud.org/documents/23257185/leopold-nsa-ig-foia-unauthorized-sigint-collection.pdf.

[8] *Id* at 1-2.

[9] *Id*.

[10] *Id*.

The Inspector General concluded that the whistleblower's allegations were "[s]ubstantiated,"[11] and that the:

> activities resulted in, or were at least reasonably likely to result in, the unauthorized collection of communications to or from USPs or persons in the United States, or both. The preponderance of the evidence supports the conclusion that, by doing so, and failing to report the non-compliant activity, [redacted] violated the classified annex of DoD Regulation 5240.1-R, *Procedures Governing the ACtivities of DoD Intelligence Components that Affect United States Persons* and its classified annex, NSA/CSS Policy I-23, United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and U.S. Minimization Procedures*, and USSID SP0019, *NSA/CSS Signals Intelligence Directorate — Oversight and Compliance Policy*.[12]

In addition to the aforementioned possible violation of Title VII, the IG report also specifically stated that "[t]he overarching authorities [redacted] violated are Executive Order (EO) 12333, *United StatesIntelligence Activities*, and Department of Defense (DoD) Directive 5240.01, *DoD Intelligence Activities*."[13]

As the Board is aware, under FISA a "person is guilty of an offense if he intentionally— (1) engages in electronic surveillance under color of law except as authorized by this chapter" or "(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter."[14] This criminal act "is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both."[15]

Despite the potentially severe civil liberties impacts and apparent criminality of the activities described in this report, the Inspector General's recommendations were redacted, and the public remains in the dark as to what consequences, if any, stemmed from these actions — nearly seven years after the report was issued, and over nine years since the original allegations reached the OIG.

One of the doubts most pernicious to the public's faith in the integrity of intelligence surveillance remains the unflinching lack of meaningful accountability for individuals involved in deliberate violations of civil liberties. Some of those instances involve disturbingly individualized invasions of privacy, like instances of LOVEINT, in which some of the people violating the rules in the interest of spying on romantic partners faced mere "administrative action."[16] Others involve programmatic surveillance at a scale so staggering it still eludes full public understanding, like that which occurred under massive and unconstitutional surveillance program codenamed

---

[11] *Id* at 2.
[12] *Id*.
[13] *Id*.
[14] 50 U.S.C. 1809(a).
[15] 50 U.S.C. 1809(c).
[16] Siabhan Gorman, "NSA Officers Spy on Love Interests," *The Wall Street Journal*, August 23, 2013, https://www.wsj.com/articles/BL-WB-40005.

Stellar Wind.[17] Distrust is further fueled by lies and misleading statements, like when then-Director of National Intelligence James Clapper infamously testified to the Senate that the government does "not wittingly" collect records of millions of Americans — while the bulk telephone metadata dragnet was still operating in secret.[18]

Three months after the original allegations at the center of the IG report, The Wall Street Journal reported: The "NSA said in a statement Friday that there have been 'very rare' instances of willful violations of any kind in the past decade, and none have violated key surveillance laws. 'NSA has zero tolerance for willful violations of the agency's authorities' and responds 'as appropriate.'"[19] Although this now appears to be untrue on its face, the Board now has the unique opportunity to examine and disclose how the NSA responded to these substantiated allegations.[20] The Board should also examine whether the whistleblowing source of the allegations, who was forced to take extraordinary steps to trigger any meaningful oversight of the activities in question,[21] faced any adverse actions for reporting the SIGINT misuse.

Unfortunately, in the absence of information that only the Board can provide in time for the upcoming legislative debate around Section 702, the public has strong reason to believe even these "egregious"[22] and "reckless"[23] abuses eluded meaningful accountability, even though the IG concluded the activities, described by concerned colleagues as "blatantly improper,"[24] "did in fact target and collect such communications" (of or about United States persons).[25]

In the interest of assuring the public that individuals who abuse their access to Section 702 and Section 702 information are held accountable, the Board should further recommend that the CIA, FBI, NCTC, and NSA adopt mandatory minimum consequences for employees who misuse Section 702 and Section 702 information, that these minimums be made public, and that relevant actions taken against individuals be made public with only necessary redactions.

---

[17] *See* Annex to the Report on the President's Surveillance Program, Volume III, Offices of the Inspectors General of the Dep't of Def., Dep't of Justice, Cent. Intelligence Agency, Nat'l Security Agency, and Office of the Dir. of Nat'l Intelligence, July 10, 2009. Available at: https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf.

[18] *See* Glenn Kessler, "James Clapper's 'least untruthful' statement to the Senate," *The Washington Post*, June 12, 2013, https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.

[19] Gorman, *supra* note 16.

[20] Notably, the person whom the Office of the Inspector General investigated responded to its tentative conclusions by writing, among other things, "OK, so if I *am* doing something, what of it?" IG Report app. N at 4.

[21] *See id* at 12-37.

[22] *Id* app. N at 17.

[23] *Id* at 53.

[24] *Id* app. C2 at 4.

[25] *Id* at 48.

III. The Board should recommend a complete prohibition on warrantless U.S. person queries by the FBI

The FBI's mission extends to both intelligence and law enforcement efforts, which renders its access to Section 702 information and its ability to nominate selectors for targeting potentially more concerning and more directly consequential to U.S. persons' civil liberties than the CIA, NCTC, and NSA, at least as the impacts are likely to be felt by an individual U.S. person. In brief, the possibility of a counterintelligence agent tipping a law enforcement agent off based on information that will likely never face adversarial process in court, for instance, has profound policy implications — which sets the FBI apart from other agencies.

The FBI's abject and well-documented failure to abide by the laws and rules that govern access to Section 702 information is therefore extremely disturbing, and this inability to comply with Congressionally and judicially mandated safeguards merits a prohibition on its use of U.S. person queries, which the Board should recommend as soon as possible.

U.S. person queries occur when the government knowingly searches unminimized information (including both communications content and noncontent) acquired pursuant to Section 702 using search terms that relate to a U.S. person.[26] This presents acute civil liberties concerns that cannot be meaningfully ameliorated, and as practiced today can directly convert intelligence information into investigative material for law enforcement to use, even in cases that do not involve national security. The practice further flouts Congress's explicit original intent and the public's general understanding of FISA, reflected in Section 702's statutory title: "Procedures for targeting certain persons outside the United States other than United States persons."[27] In 2018, however, Congress stipulated limited circumstances in which the FBI may conduct these queries for exclusively criminal purposes, and required the government to establish procedures that "include a technical procedure whereby a record is kept of each United States person query term used for a query."[28] Importantly, the Annual Statistical Transparency Report issued by the Office of the Director of National Intelligence (ODNI) for 2021 began reporting the FBI's use of U.S. person queries.[29]

The CIA, NCTC, and NSA collectively conducted under 10,000 U.S. person queries of unminimized communications content obtained under Section 702 each year in 2019, 2020, and 2021.[30] From December 2019 — November 2020 and December 2020 — November 2021, however, the FBI conducted up to 1,324,057 and 3,394,053 U.S. person queries, respectively.[31] Although there are some variations in how each agency tracks these queries, none come close

---

[26] *See* Annual Statistical Transparency Report, Office of the Dir. of Nat'l Intelligence, April 2022, (hereinafter "ODNI Transparency Report") at 17. Available at: https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.
[27] 50 U.S.C. 1881a.
[28] 50 U.S.C. 1881a(f)(1)-(2).
[29] ODNI Transparency Report at 19.
[30] *Id*.
[31] *Id* at 21.

to explaining the extreme discrepancy — or to mitigating the massive civil liberties impacts the FBI's use of U.S. person queries results in.[32]

Dramatically exacerbating the volume of FBI's use of U.S. person queries — which in 2014 the Board described as a matter of "routine practice" "[w]hen an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime"[33] — is the fact that the FBI has apparently *never* complied with the statutory requirement to obtain a FISA Court order. As the ODNI describes:

> *Congress required FBI to obtain an order … before accessing the contents of Section 702-acquired communications when:*
>
> *(1) the communications were retrieved using a U.S. person query term;*
> *(2) the query was not designed to find and extract foreign intelligence information; and*
> *(3) the query was performed in connection with a predicated criminal investigation that does not relate to national security.*[34]

These overlapping facts are deeply alarming and depict a system that is disturbingly ripe for abuse — and the most recently publicly available opinions from the FISA Court reveal this abuse is already happening. To take one of the most disturbing publicly known instances of misuse:

> [B]etween April 11, 2019, and July 8, 2019, a technical information specialist in the [redacted] who was conducting "limited background investigations" conducted approximately 124 queries of Section 702-acquired information using the names and other identifiers of: 1) individuals who had requested to participate in FBI's "Citizens Academy" — a program for business, religious, civic, and community leaders designed to foster greater understanding of the role of federal law enforcement in the community; 2) individuals who needed to enter the field office in order to perform a particular service, such as a repair; and 3) individuals who entered the field office seeking to provide a tip or to report that they were victims of a crime.[35]

In other words, in one three-month period a single FBI analyst unlawfully queried Section 702 information 124 times, violating an unknown number of people's privacy — specifically U.S. persons who were trying to work with the FBI as community leaders, U.S. persons performing

---

[32] *Id* at 19-22.
[33] Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board, July 2, 2014, at 137. Available at: https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf.
[34] ODNI Transparency Report at 22.
[35] FISA Ct., Memorandum Opinion and Order, November 18, 2020, (hereinafter November 2020 FISC Opinion) at 39-40. Available at: https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

services for the FBI, and U.S. persons who were victims of crimes. This is unconscionable, and it is all the more alarming considering such errors were not isolated and appear to have been discovered during oversight reviews of only seven[36] — out of 56[37] — field offices.

To borrow the FISA Court's phrasing, the issues identified and how they were identified "suggest that the FBI's failure to properly apply its querying standard when searching Section 702-acquired information [is] more pervasive than was previously believed."[38] The current capacity of one rogue FBI agent to effect staggering civil liberties violations through the misuse of Section 702 information is too great, and the FBI's history of refusing to comply with the law too long. The Board should recommend a complete prohibition on the FBI's use of U.S. person queries, and should further recommend the timely completion and declassification of oversight reviews of all FBI field offices' use of Section 702 information.

IV. The Board should investigate and disclose how many times and under what circumstances Section 702 information has been and may be used in criminal contexts, and to what degree it is used to pressure U.S. persons to act as informants

The government's use of Section 702-acquired information in criminal contexts and for the purposes of recruiting informants remains opaque. Simply put, Congress and the public cannot have an adequately informed policy debate around this controversial authority's reauthorization in the absence of transparency into how it may be or has been used against them or their neighbors.

Meaningful transparency into the use of Section 702 information must reflect both the degree to which it is used in criminal contexts, including for lead or tip purposes, and for the purposes of coercing U.S. persons into acting as informants. In the absence of both, policymakers can have no reliable sense of whether Section 702 information and Section 702-derived information does not show up in criminal contexts because the FBI successfully wields it to pressure individuals into serving as informants in efforts to avoid being criminally prosecuted, or whether its use in criminal contexts is frequent or rare. Both have massive impacts on U.S. persons' civil liberties.

Existing transparency requirements provide virtually no insight into either of these uses. Even if, for instance, the FBI fully complied the law that governs its agents' access to Section 702 information — which, as previously discussed, it does not — it would still fail to reflect these actual uses of information, because the law (similar to relevant FISA Court orders) only requires tracking when a query is made "in connection with a predicated criminal investigation … that does not relate to the national security of the United States."[39]

---

[36] November 2020 FISC Opinion at 43.
[37] *See* FBI Field Offices, Dep't of Justice, January 3, 2022, https://www.justice.gov/jmd/fbi-field-offices.
[38] November 2020 FISC Opinion at 39.
[39] 50 U.S.C. 1881a(f)(2).

It would be difficult to overstate the significance for a U.S. person's civil liberties of the potential use of Section 702 information in criminal contexts and its relation to pressuring individuals to act as informants.[40] As one point of context, the FBI searched Keith Gartenlaub's house in January 2014, as The Washington Post reported, "searching for evidence that Gartenlaub, an information technology manager at Boeing, had leaked computer information about the defense contractor's C-17 military transport plane to people acting on behalf of China."[41] Instead of charging him with being a spy, the government charged him with "possession and receipt of child pornography," securing a conviction that December.[42] Notably, Gartenlaub continues to deny these charges, appeal his conviction, and has asserted he believes he was targeted because his wife is Chinese American and because he has family in China — as millions of U.S. persons do.[43] The Washington Post has further found significant evidence that government claims used to secure the warrant in question were deeply flawed.[44] In any event, at Gartenlaub's initial court appearance, "prosecutors indicated a willingness to reduce or drop the child pornography charges if he would tell them about the C-17, said Sara Naheedy, Gartenlaub's attorney at the time."[45] Meanwhile, like others who have had FISA-derived evidence used against them, he is unable to meaningfully review or effectively challenge the underlying application or information therein, turning foundational concepts of the American justice system on their head.[46]

Although Gartenlaub's case is not publicly known to involve Section 702, it demonstrates the tremendous impact the potential permeation of information acquired pursuant to and derived from Section 702 could have on U.S. persons' civil liberties, in particular at the nexus of criminal prosecutions and coercion of informants, now and in the future. The Board has the opportunity to help identify or put to rest the growing concerns among U.S. persons that FISA surveillance could be unfairly used against them.

The Board should examine and provide the public with the greatest amount of information possible about: the rules that govern criminal uses of Section 702 information against U.S. persons, including the use of any information that the government derived from Section 702 information or that the government would not have but-for Section 702; the frequency with which

---

[40] *See, e.g.,* Janet Reitman, "'I Helped Destroy People,'" *The New York Times*, September 1, 2021, https://www.nytimes.com/2021/09/01/magazine/fbi-terrorism-terry-albury.html.
[41] Ellen Nakashima, "How a federal spy case turned into a child pornography prosecution," *The Washington Post*, April 5, 2016, https://www.washingtonpost.com/world/national-security/how-national-security-powers-are-underpinning-some-ordinary-criminal-cases/2016/04/05/1a7685f4-fa36-11e5-80e4-c381214de1a3_story.html.
[42] *Id*.
[43] Ellen Nakashima, "A former Boeing manager suspected of spying for China says that he, like Carter Page, was the victim of a flawed national security investigation," *The Washington Post*, February 25, 2020, https://www.washingtonpost.com/national-security/a-former-boeing-manager-suspected-of-spying-for-china-says-that-he-like-carter-page-was-the-victim-of-a-flawed-national-security-investigation/2020/02/18/9371dd60-4dd3-11ea-9b5c-eac5b16dafaa_story.html.
[44] *Id*.
[45] Nakashima, *supra* note 41.
[46] *See* Nakashima, *supra* note 43.

is occurs; and the extent to which this information is used to coerce U.S. persons into acting as informants.

V. The Board should investigate and disclose the degree to which acquiring a U.S. Person or person in the United States's communications or information is permitted before triggering the "reverse targeting" threshold

In January 2018, speaking in support of reauthorization of Section 702, then-Majority Leader McConnell said on the Senate floor: "Make no mistake--section 702 does not allow the targeting of American citizens, nor does it permit the targeting of anyone, no matter their nationality, who is known to be located here in the United States."[47] This distinction has been key to Congress's willingness to authorize surveillance pursuant to Section 702 since its initial passage.

Although Section 702 prohibits "intentionally target[ing] a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States,"[48] the public deserves clarity as to what this threshold means in practice, including as it may relate to the FBI's nomination of selectors and the FBI's receipt of "unminimized and unevaluated data."[49]

To accurately consider the impacts on their constituents and neighbors, policymakers and the public need to know if the reverse targeting prohibition is, in practice, implemented as a prohibition on targeting for the sole purpose of obtaining the communications of or information about a U.S. person, or if it is permissible for this to be a primary purpose, among other possibilities. The public, in turn, has a right to know at what point surveillance of U.S. persons is a permissible intended outcome of Section 702 targeting, if not the only intended outcome, especially considering the practical impossibility of identifying and challenging FISA surveillance in criminal contexts.

The Board should further disclose information about how this prohibition is implemented on a more practical level. It would help inform policymakers and the public, for instance, to know what percentage of selectors nominated by the FBI were subsequently reviewed and determined to be violative of the reverse targeting prohibition, how many targets have been reviewed for this purpose, and by whom. However, this information would be misleading in the absence of additional information about what degree of intentionality is permitted-in-practice by the reverse targeting prohibition.

---

[47] 164 Cong. Rec. S265 (January 18, 2018) (statement of Majority Leader McConnell). Available at: https://www.congress.gov/115/crec/2018/01/18/CREC-2018-01-18-pt1-PgS265-6.pdf.
[48] 50 U.S.C. 1881a(b)(2).
[49] Nat'l Security Agency Training on FISA Amendments Act Section 702, "OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160816 FINAL," at 26-27. Available at https://www.intel.gov/assets/documents/702%20Documents/declassified/ACLU%2016-CV-8936%20RMB%20001001-001049%20-%20Doc%2017%20NSA-s%20Training%20on%20FISA%20Amendments%20Act%20Section%20702_OCR.pdf.

The Board should also examine and disclose information about how often two related scenarios occur: the NSA disclosing to the FBI that a target has entered the United States, as provided for by the NSA's minimization procedures,[50] and the waiver of destruction requirements for information acquired pursuant to Section 702. In the latter case, if the NSA determines that targeting a selector has "unintentionally acquired domestic communications, or has acquired communications that must be treated as domestic communications," NSA minimization procedures require the purge of those communications.[51] However, the Director of the NSA may approve a written "Destruction Waiver" with "sufficient facts to allow the Director to make an appropriate decision on a communication-by-communication basis."[52] The frequency of this practice is important for Congress and the public to understand in the interest of assessing to what degree destruction waivers permit the retention of information that the government may not be permitted to acquire if it had accurate information at the outset.

VI. Conclusion

This Board's timely investigation of these issues, issuance of recommendations, and broader examination of Section 702 represents a unique opportunity to inform Congress and the public about key questions of civil liberties impacts on U.S. persons ahead of the debate over whether and, if so, with what reforms to reauthorize Section 702 of FISA. We appreciate the opportunity to offer these comments on that critical work.

Respectfully submitted,

Sean Vitka
Senior Policy Counsel
Demand Progress Education Fund
Sean@demandprogress.org

[50] *See* Nat'l 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," at 11. Available at: https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Minimization%20Procedures_10.19.2020.pdf.
[51] Nat'l Security Agency Training, *supra* note 48 at 67.
[52] *Id*.

PUBLIC SUBMISSION

As of: 11/8/22, 8:51 AM
Received: November 04, 2022
Status: Draft
Tracking No. la3-eblt-1k9b
Comments Due: November 04, 2022
Submission Type: Web

Docket: GSA-GSA-2022-0009
Privacy and Civil Liberties Oversight Board (PCLOB) Notices & Rules

Comment On: GSA-GSA-2022-0009-0017
Oversight Project Examining the Foreign Intelligence Surveillance Act

Document: GSA-GSA-2022-0009-DRAFT-0034
Comment on FR Doc # 2022-20415

Submitter Information

Organization: Princeton University Researchers

General Comment

Please see the attached PDF.

Attachments

PCLOB FISA 702 Comment

PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 4, 2022

Comment of Princeton University Researchers on the PCLOB Oversight Project Examining Section 702 of FISA

Thank you for the opportunity to provide input to PCLOB's oversight of the surveillance program operated pursuant to FISA Section 702, in advance of the upcoming December 2023 legislative sunset. We are academic researchers at Princeton University who study information security and privacy, with backgrounds in computer science and law. One of us previously served on the Senate staff during the most recent reauthorization of Section 702 in January 2018.

We write to offer a question for the Board to explore and a recommendation for the Board to consider making.

Question: How has the Intelligence Community implemented the provision of Section 702 that addresses quantitatively estimating incidental collection of U.S. person communications?

When Congress originally enacted Section 702, it included a provision that anticipated elements of the Intelligence Community would quantitatively estimate incidental collection of U.S. person communications. That provision, currently codified at 50 U.S.C. § 1881a(m)(3)(A), establishes the following requirement.

> The head of each element of the intelligence community conducting an acquisition [under Section 702] shall conduct an annual review . . . . The annual review shall provide, with respect to acquisitions [under Section 702]—
> . . .
> (iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the

communications of United States persons, and the results of any such assessment.

Recipients of the annual review include, per 50 U.S.C. § 1881a(m)(3)(C), the Foreign Intelligence Surveillance Court and congressional oversight committees.

In the nearly 15 years since this provision became law, the Intelligence Community has made concerted efforts to estimate incidental collection. It has not, however, identified a method that it finds adequate for protecting sources and methods, respecting individual privacy, minimizing burden on analytic capacity, and generating a sufficiently accurate estimate.

We encourage the Board to examine how the Intelligence Community has implemented this provision of Section 702. What process, for example, do elements of the Intelligence Community follow for completing the annual review? What personnel and resources have the Intelligence Community dedicated to estimating incidental collection? To what extent has the Intelligence Community drawn on external expertise that might assist in generating an estimate?

Recommendation: The Board should independently evaluate methods for estimating incidental collection and, if it identifies a viable method, recommend implementation by the Intelligence Community in advance of the December 2023 sunset.

Earlier this year, we published a peer-reviewed academic article proposing a new method for estimating incidental collection.[1] The proposal uses novel cryptography to securely analyze data that is privately held by the Intelligence Community and communications services. The method that we describe would maintain the secrecy of sources and methods, respect the confidentiality of personal data, rely on automation rather than manual analysis, and provide highly accurate estimates based on country-level location.

[1] Anunay Kulshrestha & Jonathan Mayer, *Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum*, Usenix Security (2022).

We have already developed a proof-of-concept implementation of our system, which was also peer reviewed for functionality and reproduction of the results in our publication.[2] We have also completed a follow-on paper that describes a quantum-resistant version of our proposal, in order to address the possibility that quantum computing will in future necessitate alternative types of cryptography.[3]

We encourage the Board to independently evaluate whether our new proposed method, or other methods, would be viable for quantitatively estimating incidental collection. The Board's technical expertise, access to classified information, and ability to convene stakeholders with diverse perspectives will strengthen public confidence about the feasibility (or lack thereof) of generating an estimate of incidental collection.

If the Board determines that there is a viable means of estimation, we encourage the further step of recommending implementation in advance of the December 2023 sunset. Transparency about incidental collection would greatly benefit Congress and the public in considering possible amendments to Section 702.

* * *

Thank you again for the opportunity to provide input to the Board's oversight of Section 702. We would be glad to provide additional detail or discussion as would be helpful to the Board.

Sincerely,[4]

Anunay Kulshrestha
Graduate Researcher, Center for Information Technology Policy, Princeton University

Jonathan Mayer
Assistant Professor of Computer Science and Public Affairs, Princeton University

[2] The implementation is available at https://github.com/citp/mps-operations.
[3] Anunay Kulshrestha & Jonathan Mayer, *Surveillance Transparency After Quantum Computing: Quantum-Resistant Multiparty Private Set Operations* (in submission).
[4] We offer this comment as individual academic researchers.