Privacy and Civil Liberties Oversight Board
Public Forum on Foreign Intelligence Surveillance Act Section 702

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

January 12, 2023

Chair Franklin and Members of the Privacy and Civil Liberties Oversight Board (PCLOB), thank you for convening this important and timely public forum on Section 702 of the Foreign Intelligence Surveillance Act (FISA).[1] Section 702 is among the most effective and most contested surveillance authorities available to the U.S. Intelligence Community (IC), and PCLOB will play an essential role as Congress considers reauthorization legislation this year.

I offer that view from firsthand experience. Before joining the Princeton faculty, I served as a staff member in the Senate, where I worked on the Intelligence Committee and Judiciary Committee bills that culminated in the FISA Amendments Reauthorization Act of 2017.[2] That legislative process was a challenge: foreign intelligence surveillance is a complex area of statutory and constitutional law, and IC practices are both technically sophisticated and often classified. Members and staff generally had limited familiarity with Section 702, and key reforms under consideration were intricate amendments to the statutory scheme. Congress had modest benefit of PCLOB's independent expertise, unfortunately, both because the Board lacked a quorum and because the Board's most recent comprehensive evaluation of Section 702 was from years prior.[3] I commend the Board and staff for taking a fresh look at Section 702 and aiming to release a report early in the latest cycle of reauthorization legislation.

In this prepared statement, I would like to elevate a foundational issue for Section 702: how does the surveillance authority affect ordinary Americans? Estimating "incidental" collection of communications to or from people in the United States and U.S. persons abroad is essential context for understanding the authority and evaluating possible reforms. These are persons who are not targets of Section 702 surveillance and who are otherwise protected by FISA and (for domestic collection) Fourth Amendment warrant procedures. My comments address why quantitatively estimating incidental collection is so important, why developing an estimate is so difficult, and a possible path forward.

This statement draws extensively on a recent peer-reviewed scientific publication which I coauthored with graduate researcher Anunay Kulshrestha, as well as a follow-on manuscript that we are currently developing.[4] While the views that I offer at this public forum are solely my own, the research that I describe is very much a collaborative effort.

---

[1] 50 U.S.C. § 1881a.
[2] Pub. L. No. 115-118, 132 Stat. 3 (2018).
[3] U.S. PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).
[4] Anunay Kulshrestha & Jonathan Mayer, Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum, USENIX SEC. SYMP. (2022), *available at* https://www.usenix.org/conference/usenixsecurity22/presentation/kulshrestha; Anunay Kulshrestha & Jonathan

I. Why is estimating incidental collection important?

Section 702 represents a compromise between two established perspectives in U.S. surveillance law. From one point of view, the judicial warrant, predicated on probable cause and particularly describing communications, is a touchstone. Since the seminal *Katz* and *Berger* cases in 1967, the federal courts have generally required a warrant to intercept communications content in the U.S. consistent with the Fourth Amendment.[5] And since Congress enacted the Wiretap Act in 1968, Title I of FISA in 1978, and the Stored Communications Act in 1986, federal statutory law has similarly set a baseline expectation of a warrant for domestic collection of communications content.[6] Section 702 is a downward departure in privacy and civil liberties protections: instead of obtaining an individualized Foreign Intelligence Surveillance Court (FISC) warrant, the IC may collect data based on annual judicial programmatic approval, periodic judicial reviews, and internal executive branch determinations.

From another point of view, Section 702 is an upward departure. When the IC collects communications to and from foreign surveillance targets, using interception vantage points abroad, it has never needed a warrant—nor even had a means of obtaining one. While modern technology now locates many of these communications on servers and networks in the U.S., the argument goes, these are communications that are still fundamentally international in character when targeted for surveillance. Section 702 is a layer of privacy protection above the baseline, in this perspective, because it establishes a role for judicial oversight and accountability.

Incidental collection goes to the compromise at the very core of Section 702. Existing transparency metrics provide some understanding of collection that, but for the target using a U.S.-based communications service, would fall entirely outside of FISA and the Fourth Amendment.[7] But to what extent does Section 702 enable domestic collection of communications content to or from people in the U.S., and U.S. persons abroad, which the IC could otherwise only obtain with a warrant? In other words, Section 702 is a hybrid of two competing analogies about appropriate surveillance procedure; at present we have a degree of transparency about how well one analogy fits but scant transparency about the other analogy.

As a matter of public policy, quantitatively estimating incidental collection would inform whether Section 702 strikes an appropriate balance of national security capability and respect for privacy and civil liberties. As a matter of law, an estimate would bear on whether Section 702 is "reasonable" within the meaning of the Fourth Amendment.

When Congress enacted Section 702, legislators were fully aware that they were designing an intermediate surveillance procedure and of the importance of transparency about incidental collection. Early versions of the FISA Amendments Act of 2008, passed by the House and reported by both the Senate Intelligence Committee and Senate Judiciary Committee, included

---

Mayer, Surveillance Transparency After Quantum Computing: Quantum-Resistant Multiparty Private Set Operations (2023).

[5] Katz v. U.S., 389 U.S. 347 (1967); Berger v. N.Y., 388 U.S. 41 (1967).

[6] 18 U.S.C. §§ 2518, 2703; 50 U.S.C. §§ 1804-1805.

[7] OFF. DIR. NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT (2022).

an outright requirement to periodically quantify incidental collection.[8] The Bush Administration took the position that it could not generate an estimate, so the enacted version of Section 702 shifted to a conditional requirement—if the IC identified a satisfactory method for estimating incidental collection, then it would be required to describe the method and results in an annual report to the FISC and congressional oversight committees.[9]

> 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.

This provision within Section 702 has remained essentially dormant since enactment. According to declassified documents, annual reports from the IC note no progress toward an estimate.[10]

Meanwhile, members of Congress (from both parties) and civil society groups (from across the political spectrum) have repeatedly urged IC leadership to provide an estimate of incidental collection. In the interest of brevity, the following timeline summarizes key events and the voluminous correspondence related to estimating incidental collection.

- **December 17, 2007** – The Bush Administration issues a statement of administration position on pending FISA amendment bills, noting that a requirement to estimate incidental collection "would likely be impossible to implement."[11]

---

[8] H.R. 3773, 110th Cong. (as passed by House, Nov. 15, 2007); S. 2248, 110th Cong. (as reported by Sen. Select Comm. on Intel., Oct. 26, 2007); S. 2248, 110th Cong. (as reported by Sen. Comm. on the Judiciary, Nov. 16, 2007).
[9] 50 U.S.C. § 1881a(m)(3).
[10] E.g., FED. BUREAU OF INVESTIGATION, ANNUAL REPORT ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2014) ("During the relevant reporting period, the FBI did not develop any additional procedures to assess the extent to which the acquisitions authorized under subsection 702(a) acquire the communications of United States persons."), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/fisa/Annual%20Report%20Issued%20Pursuant%20to%20Section%20702%20of%20FISA.pdf; NAT'L SEC. AGENCY, REPORT OF ANNUAL REVIEW PURSUANT TO SECTION 702(L) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT FOR PERIOD 9/1/2012 THROUGH 8/31/2013 5 (2013) ("During the current reporting period, no additional procedures were developed by NSA or approved by the Director of National Intelligence to assess the extent to which the acquisitions authorized under subsection 702(a) of FISA acquire the communications of U.S. persons beyond the procedures referenced within this annual report."), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/NSA-2012-2013-Report-of-Annual-Review.pdf.
[11] Off. of Mgmt. & Budget, Exec. Off. of the President, Statement of Administration Policy on S. 2248 (Dec. 17, 2007), *available at* https://www.justice.gov/archive/ll/docs/sap-on-s2248.pdf.

- **July 14, 2011** – Two members of the Senate write to the Director of National Intelligence (DNI), in advance of the 2012 sunset, requesting an estimate.

- **July 26, 2011** – The DNI responds that an estimate is not feasible.

- **May 4, 2012** – The same two members of the Senate write to the IC Inspector General (IG) and National Security Agency (NSA) IG in advance of the same sunset, again requesting an estimate.

- **June 6, 2012** – The NSA IG reports, with the agreement of agency leadership, that an estimate would not be feasible and could undermine U.S. person privacy.

- **July 26, 2012** – Thirteen members of the Senate write to the DNI in advance of the same sunset, again requesting an estimate.

- **August 24, 2012** – The DNI responds and, in the unclassified portion, does not address the request for an estimate.

- **October 29, 2015** – Civil society groups write to the DNI, in advance of the 2017 sunset, again requesting an estimate.

- **December 23, 2015** – A staff member in the Office of the DNI (ODNI) responds with an excerpt from PCLOB's 2014 report that summarizes the government's position.

- **January 13, 2016** – The same civil society groups again write to the DNI, again requesting an estimate of incidental collection and a specific description of the obstacles to arriving at an estimate.

- **April 22, 2016** – Fourteen members of the House Judiciary Committee write to the DNI in advance of the same sunset, again requesting an estimate.

- **December 16, 2016** – Eleven members of the House Judiciary Committee write to the DNI to memorialize their understanding that ODNI and NSA will provide a prompt estimate.

- **February 28, 2017** – In a Senate Intelligence Committee hearing, the DNI nominee commits to "do[ing] everything I can" to generate an estimate.

- **April 7, 2017** – The Chair and Ranking Member of the House Judiciary Committee write to the DNI, in advance of the same sunset, renewing the request for an estimate and restating the expectation that ODNI and NSA will provide an estimate.

- **June 7, 2017** – In another Senate Intelligence Committee hearing, the DNI explains that after consulting with NSA leadership and staff, he has concluded that an estimate is not feasible. "[I]f someone out there knows how to get to it," he notes, "[the NSA Director]

is welcome to have them come out and tell NSA how to do it."

- **June 12, 2017** – Civil society groups write a letter to the DNI criticizing the change in position and urging him to reconsider.

- **June 13, 2017** – The DNI responds to the Chair and Ranking Member of the House Judiciary Committee, stating the same position that he articulated before the Senate Intelligence Committee.

- **June 27, 2017** – The Chair and Ranking Member of the House Judiciary Committee write to the DNI requesting detail about the estimation methods that the IC has considered, the reasons for concluding that the methods are infeasible, and any preliminary estimates that the IC developed.

- **July 17, 2017** – The DNI responds to the Chair and Ranking Member of the House Judiciary Committee, reaffirming that an estimate is infeasible. The unclassified portion of the letter does not provide further detail.

As for the Board, its comprehensive 2014 report on Section 702 described the volume of incidental collection as "one of the biggest open questions about the program, and a continuing source of public concern."[12] The "unknown and potentially large scope of the incidental collection of U.S. persons' communications," the Board explained, "push[es] the program close to the line of constitutional reasonableness."[13] Because of the "impasse" over estimation methods, "lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."[14]

II. Why is estimating incidental collection difficult?

Generating an estimate of incidental collection is, fundamentally, an exercise in matching data. The IC knows the communications that it has collected under Section 702, at least when those communications arrive in a structured format (e.g., "downstream" collection via communications services). But, by design, the IC typically has limited information about the parties to those communications who are not relevant to a foreign intelligence or law enforcement investigation. Estimating incidental collection inherently involves matching the surveillance data held by the IC with external location or nationality data about the parties to communications, then counting affected persons or communications.[15]

---

[12] U.S. PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 146 (2014).
[13] *Id.* at 9.
[14] *Id.* at 147.
[15] For brevity, I use the term "nationality" as shorthand for whether a natural person is a "U.S. person" under FISA or is protected by the Fourth Amendment when traveling abroad. Citizens and lawful permanent residents (i.e., "green card" holders) are U.S. persons under FISA. 50 U.S.C. § 1801(i). The Supreme Court has held that the Fourth Amendment protects persons with "substantial connections" to the U.S., which presumptively includes lawful permanent residents and possibly others. U.S. v. Verdugo-Urquidez, 494 U.S. 259 (1990).

There are many obstacles to this matching task. Based on my government service, unclassified materials, and extensive unclassified conversations with people who have experience in senior IC leadership positions, I believe the following set of considerations fairly characterize why the IC has encountered so much difficulty in generating an estimate of incidental collection.[16]

- An estimation method must **protect sources and methods**. Any method that would require disclosing classified information about Section 702 collection, such as sharing communications identifiers with a third party for it to generate an estimate, would not be acceptable to the IC.

- Estimation must **respect privacy and civil liberties**. The IC should learn minimal information—ideally no new information—about people who are not surveillance targets and are not relevant to a foreign intelligence or law enforcement investigation. This consideration is partly to avoid the privacy impact of information collection and partly to reinforce the IC's culture and norms about only collecting communications information for national security purposes.

  The estimation method that has previously been a focal point—manual analysis of sampled data—has led to a difference of opinion about the appropriate level of privacy protection. Members of Congress and civil society groups have argued that the additional intrusion would be minimal and acceptable, while the IC has consistently taken the position that it does not want to investigate individuals solely for the purpose of generating an estimate.

- Any estimation process must **comply with the law**. The IC cannot collect information that would run afoul of FISA (absent amendment), the Fourth Amendment, or other relevant federal law. Similarly, a communications service cannot voluntarily disclose information when prohibited by the Electronic Communications Privacy Act (ECPA) or other relevant law. An estimation method could not, as an example, involve using FISA surveillance procedures to collect additional information about parties to communications collected under Section 702.

- Estimation must **impose a limited burden on IC capacity**. The IC allocates its staff and budget to pressing national security concerns; directing resources toward estimation necessarily means (absent new resources from Congress) directing capacity away from other priorities.

  Here, too, there is a difference of opinion about the feasibility of estimation with sampling and manual analysis. Lawmakers and civil society groups view the burden as workable, while the IC believes it would be infeasible.

- An estimation method must **rely on high-quality data** so that the results are rigorous. If the IC were to generate an estimate using notoriously questionable contact, location, or

[16] *See id.*; *Open Hearing on FISA Legislation*, 115th Cong. (statement of Daniel R. Coats, Director of National Intelligence).

nationality information from commercial data brokers, as an example, the resulting figures could be too unreliable to inform policymaking.

- Estimation must **be transparent**. The IC must be able to explain how it arrived at a figure and why the figure is trustworthy. An estimation method that relies on confidential commercial data sources, for instance, may lack sufficient transparency.

- An estimation method must **be repeatable**. While a one-off figure would be an invaluable step, surveillance transparency metrics are typically repeated on an annual (if not more frequent) basis to enable understanding long-term trends.

- If estimation relies on cryptography to protect classified information or personal data, it must **use cryptography standards already approved by the IC**. The IC carefully evaluates cryptographic algorithms and parameters before determining they are satisfactory. Requiring the IC to use alternative types of cryptography to estimate incidental collection would be unrealistic.

- An estimation method must **account for data formatting differences**. Elements of the IC, online services, and telecommunications carriers store communications identifiers in diverse formats. Harmonizing these formats is essential for accurately matching records.

- Estimation must **account for change over time**. People travel to and from the United States and (far less often) change nationality. Methods for estimation must account for this dynamism.

III. How could the Intelligence Community estimate incidental collection?

When I departed the Senate for academia, the DNI's open call for assistance in estimating incidental collection stuck with me. My research group took up the challenge, broadly engaging with expert stakeholders from government, industry, and civil society. We spent several years developing a new estimation method, and we published our primary research article in August. The project is, to my knowledge, both the only peer-reviewed scientific proposal for estimating incidental collection and the only detailed alternative to the sampling and manual analysis methods that the IC has consistently declined.

The key idea in our proposal is that communications services, such as webmail providers and telephone carriers, maintain highly accurate country-level location data in the ordinary course of business. The IC could match its own dataset about Section 702 collection with these external location datasets and compute aggregate estimates of incidental collection. By applying an advanced form of cryptography, secure multiparty computation, the matching process would not reveal information about Section 702 collection to communications services and would not reveal any person's location to the IC. At the conclusion of the protocol that we propose, the IC would possess two transparency statistics for incidental collection: (1) A count of communications identifiers (e.g., email addresses or telephone numbers) that were used by a person in the U.S. and that had a communication collected under Section 702. (2) A count of

communications that were to or from an identifier used by a person in the U.S. and that were collected under Section 702.

We designed our estimation method to address every obstacle that the IC has encountered.

- The proposal would protect sources and methods by encrypting data about Section 702 collection, such that only the IC could decrypt the data.

- The proposal would respect individual privacy and civil liberties by only involving country-level location data that businesses already routinely maintain and by encrypting that data such that only the originating firms can decrypt it.

- Section 702 already authorizes estimating incidental collection, and the use of secure multiparty computation does not appear to trigger FISA, ECPA, or other privacy laws. The FISC could possibly offer an authoritative interpretation in a proceeding to update Section 702 procedures and, if necessary, Congress could provide a safe harbor for implementing the proposal.

- The proposal would be largely automated and could be implemented affordably in a preexisting secure cloud computing environment. We have already developed open-source software for the proposal, which was also peer reviewed. As a point of reference, implementing a prototype of the proposal involved just one graduate researcher and one high-performance server.

- The location data that the proposal would rely on would be both comprehensive (owing to consolidation in the email and telecommunications markets) and highly accurate at the country level. While the data would only reflect location—not nationality—calls to estimate incidental collection have repeatedly indicated that this limitation would be acceptable. The IC also already relies on location as a proxy for nationality in Section 702 procedures. Similarly, while the proposal would count identifiers—not natural persons—existing transparency reporting already has this limitation.

- The methods and data sources for estimating incidental collection could be entirely public.

- The proposal could be re-run at any time with updated input data from the IC about Section 702 collection and from communications services about user locations.

- The cryptography in the proposal relies on building blocks that the NSA has already approved for protecting classified information in the Commercial National Security Algorithm (CNSA) Suite. We have benchmarked the proposal with CNSA algorithms and parameters to confirm that performance is workable. We have also developed and benchmarked a variant of the proposal that uses quantum-resistant cryptography, to ensure that the proposal remains viable even if quantum computing becomes practical.

- The proposal allows the IC and communications services to agree on any format for identifiers. The part of an email address before the "@" could, for example, be lowercase, without "plus addressing," and without periods for Gmail addresses. The remaining part of an email address could be lowercase and converted to a standard representation for internationalized domain names. Telephone numbers could be in an international standard format.

- The proposal allows the IC and communications services to define a window of time for Section 702 collection and user location. In the simplest configuration, the protocol could run on collection over a calendar year and predominant country locations over that year.

* * *

While our proposal for estimating incidental collection under Section 702 appears to be viable at this stage, and I am heartened by the earnest response that our proposal has received from stakeholders in government, industry, and civil society, I also fully acknowledge that taking steps forward will not be easy. There may be additional impediments that we have not identified. Stakeholders may come to disagree with our assessment of aspects of the proposal. Communications services could elect not to voluntarily participate. Legislation could become necessary.

As the Board moves forward with Section 702 oversight, I encourage you to consider assessing how the IC has implemented and could implement the statutory provision that conditionally requires an estimate of incidental collection. PCLOB has a unique combination of expertise in law, technology, and surveillance programs, independence, and access to classified material. The Board could offer a persuasive opinion on the path forward for estimating incidental collection and the possibility of generating an estimate in advance of the December 31 legislative sunset. Congress and the American people have already gone through two cycles of reauthorization without the benefit of this vital information; if there is an opportunity to achieve an estimate in the current reauthorization process, PCLOB should take it.

Thank you again for convening this public forum. I look forward to your questions.