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When Congress originally enacted Section 702, it included a provision that anticipated elements of the Intelligence Community would quantitatively estimate incidental collection of U.S. person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.