Center for Ethics and the Rule of Law
University of Pennsylvania

Annenberg Public Policy Center
University of Pennsylvania

THE REAUTHORIZATION DEBATE: CHARTING THE PATH AHEAD FOR FISA SECTION 702

CONFERENCE REPORT

PRESENTED BY:

CENTER FOR ETHICS AND THE RULE OF LAW

THE ANNENBERG PUBLIC POLICY CENTER

PREPARED BY:

RAMATOULIE JALLOW

MARY FRANCES BERRY FELLOW
CENTER FOR ETHICS AND THE RULE OF LAW

Conference Background

Section 702 of the Foreign Intelligence Surveillance Act (FISA) establishes a foreign intelligence collection program that empowers the government to gather and share intelligence from non-U.S. persons who are based outside the country to protect U.S. national security interests.[1] According to the National Security Agency (NSA), 59 percent of the President's Daily Brief (PDB) in 2022 contained information derived from Section 702 surveillance.[2]

FISA Section 702 is generally set to expire every six years unless reauthorized by Congress.[3] It was last renewed at the end of 2018 and is set to expire, once again, at the end of 2023 unless Congress votes for its re-extension. This year's reauthorization debate has been particularly controversial amid heightened concerns by civil liberty and privacy activists about the subsequent querying of the Section 702 database for incidental communications with U.S. persons. Critics argue these queries breach the Fourth Amendment's requirement for a warrant and point to the FBI's poor compliance rate with Section 702 querying procedures. Proponents, on the other hand, highlight the critical importance Section 702 plays in defending U.S. national security interests and bring attention to recent FBI reforms that have been put in place to ensure improved compliance with querying procedures.

From October 5-6, 2023, the Center for Ethics and Rule of Law (CERL), in conjunction with the Annenberg Public Policy Center (APPC), hosted a conference entitled *The Reauthorization Debate: Charting the Path Ahead for FISA Section 702*. This conference brought together leading scholars and practitioners in national security, intelligence, surveillance, and civil liberties to engage in robust discussion about the reauthorization of FISA 702. The series of workshop sessions were designed to canvas the importance of the Section, its areas of concern, the

---

[1] The National Security Agency (NSA), Central Intelligence Agency (CIA), National Counterterrorism Center (NCC) and Federal Bureau of Investigation (FBI) can all access the Section 702 database. However, only the NSA and the FBI, to a limited extent, can gather information insofar as conducting Section 702 acquisitions.

[2] Office of the Directorate of National Intelligence, FISA Section 702 Factsheet, available at: https://www.intel.gov/assets/documents/702%20Documents/FISA_Section_702_Fact_Sheet_JUN2023.pdf (Oct. 16, 2023).

[3] Unlike Title I of FISA, Section 702 requires periodic reauthorization. Section 702 previously renewed after every four years (2012), then after every five years (2017). Currently, the Section is set to be renewed every six years.

consequences at stake should Congress vote against reauthorization, and key opportunities for reform of the Section should Congress vote for reauthorization.

The conference began on October 5 with public keynote remarks by Assistant Attorney General for the National Security Division Mathew G. Olsen, followed by a fireside chat with Mr. Olsen and Assistant Attorney General for Legislative Affairs Carlos Felipe Uriarte, moderated by CERL Faculty Director Claire O. Finkelstein. Immediately after, experts in national security and civil liberties discussed renewing the controversial foreign surveillance program in a panel entitled *The FISA Section 702 Reauthorization Debate: What's at Stake.* Panelists included George W. Croner, Senior Fellow, National Security Program, Foreign Policy Research Institute, formerly Operations Division, Office of General Counsel, NSA, and CERL Advisory Council Member; Glenn S. Gerstell, Senior Advisor, International Security Program, Center for Strategic and International Studies (CSIS), and Former General Counsel of the NSA and CSS (2015-2020); Elizabeth Goitein, Senior Director for Liberty and National Security at the Brennan Center for Justice; and Ashley Gorski, Senior Staff Attorney at the American Civil Liberties Union's (ACLU) National Security Project. The panel was moderated by Suzanne Spaulding, the Senior Adviser for Homeland Security and Director of the Defending Democratic Institutions Project at CSIS. The following day, conference participants attended three closed-door sessions covering the following thematic areas: critical issues in the FISA Section 702 renewal debate; objections to reauthorization; and warrant requirements and other compromise proposals for reauthorization.

This report provides a synopsis of the discussions during the closed sessions, which were conducted under Chatham House Rule.[4]

[4] This report was prepared by Ramatoulie Jallow. Gratitude is due to Laura Stanton, Meredith Devine, and Sammi Deutsch for their excellent conference notes. Special gratitude is also due to David Joanson, Jennifer Cohen, and George Croner for their contributions in coordinating, drafting, and editing this report.

Conference Sessions
October 6, 2023

Session 1: Critical Issues in the FISA Section 702 Renewal Debate

Moderator
Claire O. Finkelstein, Algernon Biddle Professor of Law and Professor of Philosophy; Faculty Director, CERL

Briefer
George W. Croner, Senior Fellow, National Security Program, Foreign Policy Research Institute, formerly Operations Division, Office of General Counsel, NSA, and CERL Advisory Council Member

Discussion Summary

Participants set the scene for discussion by outlining how the FISA Section 702 program works together with its targeting, minimization, and querying procedures. The United States benefits from a large flow of information with the fastest fiber-optic cables passing through it. U.S. telecommunications infrastructure is therefore able to offer significant advantages in securing intelligence from foreign actors using their facilities. As highlighted by participants, many big technology companies based in the United States, such as Google, sign up to provide intelligence under the FISA Section 702 program and receive compensation for their assistance.[5] Participants identified the NSA as the principal agency responsible for the administration of FISA Section 702 program. Though the NSA, Central Intelligence Agency (CIA), National Counterterrorism Center (NCC), and Federal Bureau of Investigation (FBI) can all access subsets of the information gathered, only the NSA has access to the database in its entirety. All the information is initially stored anonymously until retrieved by queries under the "reasonably designed to extract foreign intelligence" standard, or, in the case of the FBI, the "evidence of a crime" standard. Once the communication is extracted, it is no longer anonymous and may be stored in other databases containing 702-derived information. Participants reiterated the general targeting procedures, which

[5] One participant, however, flagged that though big technology companies receive compensation, their compliance costs far outweigh the amounts they are compensated.

establish that the target must be outside the United States and a non-U.S. person. The FISA Section 702 program cannot be used initially if the sender and recipient of the communication are both within the United States. To this point, a participant flagged how unpopular these procedures and the broader program are with the European Union. Because non-U.S. persons are not afforded privacy protections under the U.S. Constitution, they are susceptible to targeting under FISA Section 702 procedures.[6]

A central issue for discussion was the incidental collection of data from U.S. persons who are in communication with non-U.S persons being targeted under FISA Section 702. Some participants expressed that this incidental collection of information is a violation of privacy under the Fourth Amendment, which requires that a warrant be granted before such information can be queried. Debate emerged among participants about when exactly a breach of the Fourth Amendment is said to have occurred. Some indicated that a breach occurs at the point when information on U.S. persons is gathered, while others argued that a breach occurs only once the query terms are run.

Participants referred to the Privacy and Civil Liberties Oversight Board (PCLOB) Report, which contains 19 recommendations concerning the reauthorization of FISA Section 702 program. Discussion focused on Recommendation 3 in which the PCLOB calls on Congress to introduce a warrant authorization from the Foreign Intelligence Surveillance Court (FISC) before a query can be run on a U.S. person.[7] As supported by some participants, Recommendation 3 also provides that the FISC should give authorization using the standard of "reasonably likely to retrieve" foreign intelligence information or "reasonably likely to retrieve" evidence of a crime.[8] However, some participants called for a stronger "probable cause" standard while others strongly cautioned against

---

[6] The concerns of the European Union are the subject of several U.S. diplomatic and trade initiatives including, in part, the regulations governing U.S. signals intelligence activities included in Executive Order 14086.

[7] The Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, September 2023, pg. 12 available at: https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf.

[8] Querying Procedures used by the Federal Bureau of Investigation (FBI) in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, (2021) Pgs. 3- 4, available at: https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FBI_Querying_Procedures.pdf.

an authorization requirement from the FISC, advocating instead for authorization from an internal legal counsel, using the "reasonably likely to retrieve" foreign intelligence, "reasonably likely to retrieve" evidence of a crime standards and/or by the consent of the U.S. person.

While some participants argued for the use of the "probable cause" standard, since it is a constitutional requirement, others questioned whether the "probable cause" standard is a constitutional requirement, suggesting that a standard be set by Congress as a matter of policy. Those advocating for a stronger "probable cause" requirement considered the abusive use of FISA Section 702 by the FBI, noting, among other concerns, the collection of Black Lives Matter (BLM) protestors information using this provision.[9] Without a stronger standard, a significant number of queries of U.S. persons may be tainted by illegitimate racial or other biases as opposed to being driven by genuine national security concerns.

The session concluded by examining the intersection between FISA Section 702 and the state secrets doctrine, namely in the case of *Wikimedia v NSA*.[10] The case was ultimately dismissed, as the NSA invoked the state secrets doctrine to prevent disclosure of how the Section 702 program works in the interest of national security. Critics assert that this reliance on the doctrine was a move by the NSA to circumvent Wikimedia's discovery request. Participants stressed the government's record of misusing the state secrets doctrine, which some courts have begun to review.[11]

Session 2: Objections to Reauthorization

Moderator
David Joanson, CERL Executive Director, Former FBI Supervisory Special Agent, Chief Division Counsel.

---

[9] Devlin Barrett, FBI Misuses Surveillance Tool on Jan. 6 Suspects, BLM Arrestees and Others, Washington Post (May 19, 2023) available at: https://www.washingtonpost.com/national-security/2023/05/19/fbi-digital-surveillance-misuse-jan6-blm/.
[10] See American Civil Liberties Union (ACLU), Wikimedia v NSA – Challenge to Upstream Surveillance, available at: https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance.
[11] ACLU, Background on the State Secrets Privilege, (January 31, 2007) available at: https://www.aclu.org/documents/background-state-secrets-privilege.

Briefer
Morton Halperin, CERL Board Chairperson

Discussion Summary

In this session, participants outlined with greater specificity the objections to reauthorizing FISA Section 702. While some expressed concern with so-called "first searches," which may incidentally yield the data of U.S. persons, others voiced issue with so-called "second searches," which result from running targeted U.S. person query terms. Participants emphasized that even when FBI agents have lawful possession of data on U.S. persons, they cannot query U.S. person terms without a warrant due to search and seizure limitations under the Fourth Amendment. Under this provision, even with a warrant, one is still restricted by its precise terms as evident in the case of *Riley v California*.[12] Debate ensued about whether, in the event there is evidence of a crime, a "plain view exception" to the Fourth Amendment exists with respect to the incidental collection of data of U.S. persons under FISA Section 702.

Critics of renewing FISA Section 702 also point to the FBI's poor compliance rate with current procedures. A memorandum opinion and order by the FISC, presided over by Judge Rudolph Contreras, reveals that the FBI misused the 702 database "278,000 times."[13] Even though the FBI has since made reforms to improve their checkered compliance record, some participants voiced concern about reauthorization on these grounds, noting a deep mistrust and skepticism around whether the FBI can internally police itself. Cited as reasons for the FBI's poor compliance were a lack of personnel training and system design controls which, as a default, caused automatic queries of the 702 database. Recent reforms aim to improve these lapses.

In closing this session, participants explored further accountability measures that could be introduced to the FISA Section 702 program. In the event that the FISC is selected to review the suggested warrant requirement for the program, increasing the number of *amici* supporting the Court is one possibility. Because warrant hearings would be *ex parte*, *amici* could step in to raise certain concerns to the FISC, should they arise in a proceeding. Participants also explored the

[12] 573 U.S. 373 (2014).
[13] Tyler McBrien, Unsealed Surveillance Court Document Reveals 702 Misuse, (May 22, 2023) available at: https://www.lawfaremedia.org/article/unsealed-surveillance-court-document-reveals-702-misuse.

possibility of the Department of Justice (DOJ) ensuring compliance under the 702 program and the use of artificial intelligence to further improve compliance.

Session 3: Warrant Requirements and Other Compromise Proposals for Reauthorization

Moderator
Patrick Toomey, Deputy Director at the ACLU under the National Security Project.

Briefer
Ashley Gorski, Senior Staff Attorney at the ACLU National Security Project.

Discussion Summary

Participants considered the current views on and options for reauthorization being explored by Congress. One option is a clean reauthorization of FISA Section 702 without any changes. Participants noted this view has very little support; it is unclear whether reauthorization has enough votes in Congress to pass. Another option is Congress allowing the program to expire. However, participants agreed on the importance of the program and noted correspondence from the Biden administration showing support for reauthorization.[14] Participants once again explored having a warrant requirement with a "probable cause" standard in the case of renewal. If the "probable cause" standard is considered too high, some participants were open to using the standard of "reasonably likely/designed to turn up information on a foreign person," or "reasonable suspicion."

Participants once again weighed the possibility of having an internal review process for FISA Section 702 or having the FISC approving the warrant. Debate emerged about whether the FISC would be able to handle the volume of requests under the program. However, some argued that by changing the standard to "probable cause," the number of cases being submitted to the FISC would be reduced.

[14] White House, Statement by National Security Advisor Jake Sullivan on the Biden-Harris Administration's support for the Reauthorization of Vital Intelligence Collection Authorities (February 28, 2023) available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/28/statement-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-support-for-the-reauthorization-of-vital-intelligence-collection-authorities/.

In smaller working groups, participants explored compromise solutions for renewing the FISA Section 702 program. This session replaced the originally scheduled concluding session on intelligence collection in a post-FISA world. Presentations from each of the breakout groups were moderated by Elizabeth Rindskopf Parker, Non-Resident Senior Advisor, CSIS, Former General Counsel, NSA and CIA, and CERL Executive Board Member. Below are summaries of the presentations from each group.

Group 1

- The group agreed to compromise on the warrant standard for U.S. person queries under the 702 program, suggesting that a standard of "reasonably likely/designed to retrieve foreign intelligence" be codified in the Act.
- Participants were open to removing the "evidence of a crime" from the standard.
- It was also agreed that there be a warrant for the review of a U.S. person query by counsel from the Justice Department, Office of the General Counsel, or from the FBI instead of the FISC.
- The group further agreed to eliminate, or include some sort of restriction for, U.S. person queries at the initial assessment stage along the lines of the "necessary and proportionate" standard, as stated in Executive Order 14086, and to have this codified into the Act.
- Finally, participants agreed that the FBI undergo further reforms to ensure better compliance.

Group 2

- Participants agreed to a standard, applying to all persons subject to FISA Section 702, in which specific and articulable facts are put forward to demonstrate that the person "is or may be an agent of a foreign power or target thereof," and that there is "immediate threat to life or limb or other exigent circumstances."
- It was also agreed that the standard would be reviewed by the FISC post-hoc.
- For purely defensive U.S. person queries, a National Security Division Attorney under the Department of Justice can review the use of Section 702 with the FISC auditing a sample post-hoc.

Group 3

- The group proposed having a two-person review for exigent queries and to have a FISC magistrate handling general query issues in the form of judicial review.
- Participants emphasized the importance of having a judicial review of some kind, preferably at the onset. However, if this is not tenable legislatively, time-sensitive queries could be reviewed after the fact.
- In the event that the FISC is not a realistic body to review queries, participants also suggested attorneys at the Office of the General Counsel.

Group 4

- The standard "reasonably likely/designed to retrieve foreign intelligence" is adequate, and the "evidence of a crime" aspect of the standard could be removed.
- Though there was no agreement on the use of the FISC to review compliance with the standard, most participants supported the idea of an attorney from the Office of the General Counsel reviewing.
- Participants agreed on audits of compliance being made by the Department of Justice, Congress, and/or the CIA.
- Participants highlighted the importance of strengthening the *amicus* system within the FISC and having this as separate from legal advisors to allow the *amici* to advocate on the correct course of action. Participants agreed that legal advisors can be confined to providing purely legal advice.
- To ensure better compliance by the FBI, participants stressed the need for higher consequences in the form of dismissal and loss of access to the database. Participants also agreed that if it was determined that there was no legitimate reason for the collection of data, that data should be promptly removed from the database.