NSI Law and Policy Paper

Reauthorization of the FISA Amendments Act

Preserving a Critical National Security Tool While Protecting the Privacy and Civil Liberties of Americans

Darren M. Dick & Jamil N. Jaffer[1]

This NSI Law and Policy Paper:

- ✓ **Describes** the history, nature, and scope of authority provided by the FISA Amendments Act, including how it is utilized and the type of intelligence it provides;
- ✓ **Evaluates** the key issues at stake in the reauthorization debate and the key arguments made on both sides;
- ✓ **Argues** that the FISA Amendments Act is critical to our national security and should be reauthorized for as long as possible in its current form; and
- ✓ **Proposes actionable recommendations** that could be responsibly considered to promote enhanced public confidence and a longer reauthorization.

Executive Summary

Essential Background on the FISA Amendments Act

Historical Background: The FISA Amendments Act (including Section 702 of the Foreign Intelligence Surveillance Act) was enacted in 2008 in response to developments in communications technology, which increasingly forced intelligence agencies to seek orders from the Foreign Intelligence Surveillance Court (FISC) before conducting surveillance against foreigners located overseas—a practice FISA had sought to avoid.

What Section 702 Authorizes: FISA Section 702 allows the U.S. intelligence community to collect the communications of foreigners located outside of the United States for foreign intelligence purposes.[2]

Expiration: FISA's Section 702 authority is scheduled to expire on January 19, 2018.[3]

Key Issues at Stake in Reauthorization

Incidental Collection and the Use of U.S. Person Information: Whether the FBI's ability to search or use Section 702 data related to U.S. persons for purposes other than foreign intelligence should be limited or prohibited by law.

"Abouts" Collection: Whether the collection of so-called "abouts" communications—communications that are not to or from a target, but that reference the target—should be limited or prohibited by law (it is currently halted as a policy matter).

Authors' Views

Reauthorization: The FISA Amendments Act is an essential national security tool and should be reauthorized for as long a period as possible in its current form.

Search and Use Restrictions: Under no circumstances should Congress rebuild the "wall" between foreign intelligence and criminal investigations by limiting investigative access to lawfully collected data or prohibiting prosecutorial use of such data.

"Abouts" Collection: A statutory prohibition should be rejected in favor of allowing the government to retain the ability to pursue technical solutions before the FISA Court.

Actionable Recommendations: As a matter of practical necessity, certain steps could be considered to promote public confidence and a substantially longer, if not permanent, reauthorization, including: modest Executive Branch controls concerning the use of Section 702-collected information; Congressional notification and judicial review of any government decision to restart "abouts" collection; and oversight or transparency enhancements around the government's use of Section 702.

Background on the FISA Amendments Act

Historical Background

FISA's Decay. The FISA Amendments Act was enacted in 2008 in order to address a major challenge: increasingly, federal intelligence agencies were being required to seek orders from the Foreign Intelligence Surveillance Court (FISC) to conduct surveillance against foreigners located overseas, including terrorists and other foreign intelligence targets—a practice FISA originally sought to avoid.[4]

- When FISA was created in 1978, it explicitly preserved the U.S. government's ability to collect, without a court order, the global communications of foreigners located overseas through specific carve-outs in the technology-based definitions contained in the statute.[5]

- However, this capability began to decay as a set of fundamental changes in communications technology took place during the late 1990s, including how long-haul communications were transmitted.[6]

- As a result of these technology changes, the communications of foreign intelligence targets overseas were increasingly covered by the FISA statute, requiring the government to seek orders from the FISA Court.[7]

Government Response to the 9/11 Attacks. In the immediate aftermath of the September 11th terrorist attacks, President George W. Bush, relying on his constitutional authority as commander-in-chief and the Authorization for the Use of Military Force provided by Congress, authorized a highly classified collection program aimed in part at filling this gap in collection authority.[8]

- This program raised controversy when it became public, and a few years later, the Bush Administration provided the collection program court oversight under a set of innovative orders issued by the FISA Court.[9]

- Over time, however, the collection program became less effective as judges acting to reauthorize the program began to limit the flexibility offered by the initial, highly innovative court orders.[10]

- As a result, the Executive Branch proposed legislative changes to modify FISA to provide specific statutory authority to the government to collect foreign intelligence by targeting foreigners located overseas under broad orders from the FISA Court.[11]

- Congress created such authority under the FISA Amendments Act.[12]

- The final vote on the FISA Amendments Act was 293-129 in the House and 69-28 in the Senate, a significant bipartisan margin in both chambers.[13]

- The FISA Amendments Act was reauthorized in 2012 without amendment by even broader bipartisan margins of 301-118 in the House and 73-23 in the Senate.[14]

What the FISA Amendments Act Authorizes

Section 702 Authority. Under FISA Section 702, the FISC can approve Executive Branch certifications for the acquisition of foreign intelligence information[15] through the targeting of foreigners[16] located abroad.[17]

- Thus, surveillance under the FISA Amendments Act may target *only*:

  - (1) non-U.S. persons (*e.g.*, not citizens or lawful permanent residents);

  - (2) who are reasonably believed to be outside of the United States; and

  - (3) for the purpose of acquiring foreign intelligence information.[18]

Key Concepts:

- **Executive Branch Certifications.** To conduct surveillance under Section 702, the Attorney General and the Director of National Intelligence must jointly submit a certification to the FISA Court and receive a court order permitting them to authorize the surveillance.[19]

  - These certifications differ from traditional FISA applications in that they describe categories of foreign intelligence information to be acquired through the targeting of foreigners located overseas as opposed to specific targets of the surveillance.[20]

- **Non-U.S. Persons.** Only non-U.S. persons are subject to targeting for surveillance under Section 702. U.S. persons not covered by Section 702 are United States citizens, United States permanent residents, groups substantially composed of United States citizens or permanent residents, and virtually all United States corporations.[21]

- **Foreign Intelligence Information.** Foreign intelligence information is information that relates to the ability of the United States to protect against potential and actual attacks by a foreign power; sabotage, international

terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power.[22]

- Foreign intelligence information also includes information with respect to a foreign power or a foreign territory that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States.[23]

- If the information itself concerns a U.S. person, that information must be "necessary" to the national security goals listed above rather than simply "relate" to them.[24]

- **FISA Court Review**. Under Section 702, the FISA Court must review the government's certifications, targeting procedures, and minimization procedures to determine whether the proposed collection program complies with the statute, including its U.S. person protections, as well as with the Fourth Amendment.[25]

  - "Targeting procedures" are controls intended to ensure that the collection targets only foreigners reasonably believed to be overseas.[26]

  - "Minimization procedures" are measures designed to limit the acquisition, retention, and dissemination of information of U.S. persons.[27]

Limitations on 702 Authority. In providing the core authority to conduct surveillance against foreigners located overseas, Congress also specifically enhanced protections for Americans by requiring a court order for the surveillance of any American, no matter where located, and also put in place other restrictions on how surveillance may be conducted.[28]

- Thus, Section 702 expressly prohibits:

  - intentionally targeting any person known to be in the United States;[29]

  - targeting U.S. persons reasonably believed to be located outside of the United States;[30] and

  - so-called "reverse targeting," or the intentional targeting of a non-U.S. person outside of the United States for the purpose of acquiring the communications of a person in the United States.[31]

Fourth Amendment Implications. Because the targets of Section 702 are foreigners located overseas, they are not entitled to Fourth Amendment protections.[32]

- However, because the program results in the incidental collection of some U.S. person information—for example, where a U.S. person is in communication with a valid non-U.S. person foreign intelligence target located overseas—Fourth Amendment analysis of this aspect of the program is appropriate.
    - Because, as a general matter, courts have held that a warrant is not required for foreign intelligence surveillance, the proper analysis is one that considers the reasonableness of the surveillance under the totality of circumstances.[33]
    - The reasonableness is determined by analyzing the contribution to national security and the degree to which it intrudes on individual privacy.[34]
    - The Foreign Intelligence Surveillance Court has reviewed the Section 702 program annually since the passage of the original legislation in 2008, and with rare exceptions related to compliance incidents, has repeatedly determined the collections are lawful under the Fourth Amendment.[35]

Key Issues at Stake in Reauthorization

Critics of the Section 702 program point to two issues—incidental and so-called "abouts" collection—that raise concerns about the privacy and civil liberties of U.S. persons.

Both issues relate to the fact that, despite only targeting foreigners outside the United States under Section 702, U.S. person information is still collected by the government and, as a result, may be searched and used in investigative or intelligence efforts and may later be used in criminal or other proceedings.

Key Concepts:

- **Incidental Collection**. If a valid foreign intelligence target communicates with a U.S. person, that communication could very well be acquired incidentally through Section 702 collection.

- As a result, Section 702 requires FISA Court approval of government-proposed procedures to minimize the acquisition, retention, and dissemination of U.S. person information collected under the statute.[36]

- **"Abouts" Collection**. Until earlier this year, certain Section 702 collections captured communications that referred to a targeted selector. Such collection was in addition to the collection of communications to or from the targeted selector and was therefore referred to as "abouts" collection.

  - An example of an "abouts" communication is an email "that includes the targeted email address in the text or body of the email, even though the email is between two persons who are not themselves targets."[37]

  - In April 2017, NSA announced that it was ending any upstream collection of communications solely "about" a foreign intelligence target. [38]

Incidental Collection and the Use of U.S. Person Information

The Debate:

Whether the FBI's ability to search or use Section 702 data related to U.S. person identities for purposes beyond foreign intelligence should be limited or prohibited by law.

- **Critics' Views:** Critics of the current Section 702 program argue that since Section 702 prohibits the targeting of U.S. persons, the use of incidentally collected communications should be substantially limited or prohibited altogether in the absence of an individual Fourth Amendment warrant.

  - They argue that government access to U.S. person communications through incidental collection is an end-run around the Fourth Amendment's protections against unreasonable searches and seizures, which, in the criminal context, typically require an individual, particularized warrant based on probable cause to believe a crime has been committed.

  - Critics concerned about incidental collection therefore generally support efforts that would prohibit or significantly limit the searching, as well as the investigative and prosecutorial use of such information, particularly with respect to criminal proceedings.

- **Proponents' Views:** In response to concerns, proponents of the current Section 702 program point out that, as a general matter, foreign intelligence

surveillance is not subject to the warrant requirement, even when U.S. persons are targeted, and, as a result, imposing a warrant requirement would hamper otherwise lawful efforts to defend U.S. national security.

- Further, they argue that Congress clearly understood that U.S. person communications would be incidentally collected and indeed, believed that it was important for the government to be able to identify U.S. persons communicating with potential adversaries.
    - To that end, proponents point out that Congress specifically acted to require the adoption of procedures for the handling of such communications once discovered and knowingly did not exclude such incidental collection from its core authority.
- As a result, proponents of the current program generally oppose any limitations on the investigative or prosecutorial use of such material, arguing that to do so would hamper the government's ability to "connect the dots."
    - They also argue this would recreate a "wall" between criminal and intelligence uses of such information, impeding information sharing and efforts to defend the United States against key national security threats.

Authors' Views:

Under no circumstances should Congress rebuild the "wall" between foreign intelligence collection and criminal investigations by limiting investigative access to lawfully collected data in the hands of the government.

- **Incidental Collection is Inherent and Necessary.** Incidental collection is an inherent part of communications surveillance, whether for foreign intelligence purposes or otherwise.
    - In the case of Section 702 collection, it results from the specific, directed, and intentional targeting of foreigners located overseas that the government reasonably believes are linked to a foreign intelligence investigation and, as a result, are linked to potential threats to the nation and its interests.
        - While foreign intelligence targets may engage in communications with U.S. persons for legitimate purposes, given the nature and scope of potential threats at issue, the

government must be able to quickly identify and act upon any communications that are in fact linked to actual threats.

- Section 702 already has extensive protections in place to preclude the dissemination or other use of wholly legitimate U.S. person communications.

    - Throughout the program's existence, there have been no examples of systematic, intentional abuse of the authority.

- **Limitations on Criminal Investigations Rebuild the "Wall"**

    - Preventing the government from querying Section 702 information in non-foreign intelligence investigations or using such information in prosecutions creates a new standard for the use of lawfully obtained information generally not found in other contexts, and risks rebuilding the "wall" between national security and criminal investigations—a significant factor in the government's failure to identify the September 11, 2001 plot before it was executed.

        - While the concept of neatly distinguishing between criminal matters and foreign intelligence matters may have some superficial appeal, in reality such investigations are often closely related.

        - Many of the activities conducted by foreign intelligence targets overseas—particularly when they are recruiting Americans for terrorist attacks or to steal national secrets—are not only valid intelligence collection topics, but also prosecutable under American law.

        - Moreover, the links between ordinary criminal activity and terrorist groups, for funding and to move money, people, and weapons, are long established.

        - Indeed, we increasingly have seen nation-states and terrorist groups pursue advantage by directly engaging in criminal activity unrelated to traditional espionage, or by developing quasi-criminal organizations or networks themselves, all of which is of considerable consequence to U.S. national security.

- Investigating such crimes often reveals hidden connections and opportunities for further investigation—criminal or intelligence—that may prove necessary to defending the nation.

- Re-erecting the wall through search and review restrictions or after-the-fact use restrictions would simply dismantle over 15 years of work to remove barriers to intelligence sharing within the government.

- **Multiple Reviews are Unnecessary and Harmful.**

  - Proposals requiring after-the-fact review of the query of lawfully obtained information are unnecessary in light of the fact that the FISA Court already reviews Section 702 authorizations for reasonableness under the Fourth Amendment.

  - In addition, such a review would almost certainly discourage and stifle the use of this lawful source of intelligence information and come with little practical benefit given the extensive oversight already in place.

"Abouts" Collection

The Debate:

Whether the collection of "abouts" communications should be limited or prohibited by law.

- **Critics' Views:** Critics concerned with "abouts" collection argue that since Section 702 does not expressly authorize "abouts" collection and such communications may include purely domestic communications, including communications between two U.S. persons, the acquisition of such communications should be prohibited by law.

  - Critics further argue that minimization methods are insufficient and generally support efforts to limit such collection, principally through provisions that would statutorily prohibit the use of Section 702 authority to obtain such communications.

- **Proponents' Views:** Proponents of Section 702 collection generally take the view that "abouts" collection is appropriately within the authority under Section 702 to collect foreign intelligence information about an authorized target and ought to be permitted to continue.

- As a result, they generally oppose efforts to put legal restrictions on such collection, preferring to let the Executive Branch handle the issue as a matter of policy.

Author's Views:

A statutory prohibition should be rejected in favor of allowing the government to retain the ability to pursue technical solutions before the FISA Court.

- "Abouts" collection is a more challenging issue because it involves the collection of information where the target is simply mentioned in the communication but may not be a participant in the communication itself.
  - This capability is highly valuable because it can help identify individuals with relationships to legitimate intelligence targets, but it also raises concerns because of some of the technical challenges the government has historically faced in implementing it consistent with the law.
  - Because of these technical challenges, the government currently has decided—as a matter of policy—to terminate its use of "abouts" collection.
    - In our view, such a policy decision is well within the purview of the Executive Branch and an appropriate use of the authority provided under the statute.
  - However, we have significant concerns with proposals to bar use of "abouts" collection in statute because such a restriction would come with significant collateral degradation of a critically important ability to identify otherwise unknown terrorists with little benefit to privacy and civil liberties if, in fact, an appropriate technical solution that can meet legal requirements becomes available.
    - Were a new technical solution developed and the government wanted to restart its "abouts" collection, it would be required to go back to the FISA Court, brief the issues, and await a ruling on whether such a new proposal would be lawful.
    - We therefore see no reason for Congress to interpose an absolute legal prohibition on this potentially critical tool.

Actionable Recommendations

Reauthorization. Our primary recommendation is that Section 702 be reauthorized with no substantive changes for at least an eight-year period.

Search and Use Reforms. Concerns about incidental collection are understandable and have been addressed through a variety of measures throughout FISA's history. However, it seems clear that additional proposals to address these concerns will be included, in some form, in any final reauthorization bill to ensure that the Section 702 authority is renewed.

- **What is critical, however, is that the "wall" between criminal and intelligence matters not be recreated—whether through investigative or intelligence barriers (e.g., search restrictions) or through after-the-fact use restrictions.**
  - Historical experience has taught that whether access to information is limited through investigative or use barriers matters little, as these restrictions generally function in much the same way, although investigative barriers are more pernicious because they pretermit any practical use of the information whatsoever.
- **To that end, it may be worth considering the use of another standard tool in the legislative-executive toolkit: a legislatively-mandated review and approval process within the Executive Branch with strong congressional reporting.**
  - Such a process would permit the querying and use of Section 702-collected information in all ongoing foreign intelligence and criminal investigations, but would statutorily limit the use of such information to prosecutions of foreign intelligence crimes and certain other major crimes (i.e., Wiretap Act predicates) unless specific, separate approval is obtained.
    - For non-Wiretap Act predicates, the individual approval of the Attorney General, or, if designated, Deputy Attorney General or Assistant Attorney General for National Security, would be required prior to prosecutorial use of Section 702 information.
    - These restrictions would be in addition to, and separate from, other restrictions already in place on the use of FISA information in criminal proceedings.

"Abouts" Collection Reforms. The concerns raised regarding "abouts" collection are not trivial and efforts to address these concerns are also likely to be included in any final reauthorization bill.

- **Given the sensitivity of "abouts" collection, and the challenges the government has faced in implementing such collection, requiring the government to provide detailed technical and legal information to Congress should it seek judicial approval to restart "abouts" collection would seem to be an appropriate step, so long as appropriate emergency authority were also available.**

Additional Transparency Measures. Given the significant public debate surrounding intelligence collection in the last few years, it is also reasonable for Congress to require significantly more detailed reporting from the Executive Branch and to require that more of such reporting be provided in unclassified form and made available to the public, where appropriate.

- **To that end, public reporting on the number of targets subject to surveillance under traditional FISA, including specific reporting on the number of U.S. persons as well as foreigners targeted under Section 702, would be appropriate to require by statute**.

- **In addition, the number and basic nature of certifications obtained under Section 702 ought to be made public along with an accounting of the number of times such authority has been sought and received.**

- **Finally, Congress ought to require the Executive Branch to provide specific justifications for the level and duration of the classification restrictions pertaining to the information in FISA related reports submitted to the Congressional oversight committees.**

Conclusion

Section 702 collection provides a powerful intelligence collection capability that targets terrorists, spies, and foreign powers outside of the United States and also provides a very significant portion of our counterterrorism intelligence. Section 702 collection also comes today with a strong set of privacy and civil liberties protections built into the statute. Given that there has been no evidence of misuse by the government, additional provisions altering the core authority or limiting the collection or use of information collected under Section 702 are unnecessary. As such, Congress should re-authorize Section 702 without delay, for as long as possible, and without additional restrictions.

To the extent Congress is of the view that some modifications are necessary, under no circumstances should it rebuild the "wall" between intelligence collection and criminal investigations. Limiting investigative or prosecutorial access to lawfully collected data makes little sense, particularly where there is no evidence of substantial abuse or misuse of this authority. And given the diversity and nature of the threats we face today, we ought to be broadening access to data, not more strongly limiting it.

Finally, if additional reforms are necessary to ensure passage of reauthorizing legislation, Congress should consider adoption only of Executive Branch internal controls, as described above, on the use of Section 702-derived information in certain criminal prosecutions, as well as certain provisions to enhance oversight and transparency.

---

[1] Darren M. Dick is an Adjunct Professor of Law and Director of Programs at the National Security Institute at the Antonin Scalia Law School at George Mason University. Professor Dick previously served, among other positions, as the Staff Director of the House Permanent Select Committee on Intelligence. Jamil N. Jaffer is an Adjunct Professor of Law and Founder of the National Security Institute and previously served, among other positions, as an Associate Counsel to the President in the Bush Administration. This paper is solely the work of the authors and does not necessarily represent the views of the National Security Institute or any other entity or individual.

[2] *See* 50 U.S.C. § 1881a(a).

[3] *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012) (expiration December 31, 2017); Pub. L. 115-96, Sect. 1002, __ Stat. __ (2017) (extending expiration to January 19, 2018).

[4] *See* Philip M. Bridwell & Jamil N. Jaffer, *Updating the Counterterrorism Toolkit: A Brief Sampling of Post-9/11 Surveillance Laws and Authorities* in THE LAW OF COUNTERTERRORISM at 241 & n. 97-98, ABA Press (2011).

[5] *Id.*

[6] *Id.* at 240-41.

[7] *Id.* at 241.

[8] *Id.* at n. 100.

[9] *Id.*

[10] *Id.*

[11] *Id.* at 241-42.

[12] *Id.* at 243.

[13] *See* Congress.gov, *H.R. 6304 – FISA Amendments Act of 2008: Actions* (June 20, 2008 & July 9, 2008), available online at <https://www.congress.gov/bill/110th-congress/house-bill/6304/actions>.

[14] *See* Congress.gov, *H.R. 5949 – FISA Amendments Act Reauthorization Act of 2012: Actions* (Sept. 12, 2012 & Dec. 12, 2012), available online at <https://www.congress.gov/bill/112th-congress/house-bill/5949/actions>.

[15] *See* 50 U.S.C. 1801(e)(1)-(2).

[16] See 50 U.S.C. § 1801(i).

[17] *See* 50 U.S.C. § 1881a(a).

[18] *Id.*

[19] *Id.*

[20] *See* 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, pp. 24-25.

[21] 50 U.S.C. § 1801(i).

[22] *See* 50 U.S.C. § 1801(e)(1).

[23] *See* 50 U.S.C. § 1801(e)(2).

[24] *See* 50 U.S.C. § 1801(e)(1)-(2).

[25] *See* 50 U.S.C. § 1881a(i)(3)(A)-(B).

[26] *See* 50 U.S.C. § 1881a(d)(1)(A)-(B).

[27] 50 U.S.C. § 1801(h)(1).

[28] *See* Bridwell & Jaffer, *Updating the Counterterrorism Toolkit* at 243.

[29] 50 U.S.C. § 1881a(b)(1).

[30] 50 U.S.C. § 1881a(b)(3).

[31] 50 U.S.C. § 1881b(2).

[32] *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (holding that the Fourth Amendment does not apply to a physical search in a foreign country of the residence of a citizen of that country who has no voluntary attachment to the United States).

[33] *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008)

[34] *See Samson v. California*, 547 U.S. 843 (2006)

[35] *See, e.g., Memorandum Opinion and Order*, For. Int. Surv. Ct. (Apr. 26, 2017) *available online at* <https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf >; see also Chris Mirasola & Yishai Schwartz, *The 18 FISA Court Opinions on Section 702: Summaries*, Lawfare (June 23, 2017), *available online at* <https://www.lawfareblog.com/18-fisa-court-opinions-section-702-summaries> (summarizing 18 FISA Court opinions related to Section 702 released under FOIA).

[36] *See* 50 U.S.C. § 1881a(e), (i)(2)-(3).

[37] National Security Agency Statement, *NSA Stops Certain Section 702 "Upstream" Activities*, April 28, 2017 available at https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml

[38] *Id.*