Center for a New American Security

March 1, 2017

Testimony before the House Committee on the Judiciary

Hearing on Section 702 of the Foreign Intelligence Surveillance Act

Adam Klein
Senior Fellow, Center for a New American Security

—

EXECUTIVE SUMMARY

Findings

- Credible, unclassified assessments—most notably the landmark report of the independent Privacy and Civil Liberties Oversight Board—confirm that Section 702 is a valuable intelligence tool that is legitimate in its basic contours and subject to adequate oversight and transparency in most respects.
- Since the 2012 reauthorization, the USA Freedom Act and the recommendations of the Privacy and Civil Liberties Oversight Board have significantly strengthened the oversight, transparency, and privacy protections applicable to Section 702.
- Section 702 should be reauthorized with its current substantive authorities intact, but with reforms to further enhance transparency and strengthen oversight.
- The Privacy and Civil Liberties Oversight Board's uncertain future is an urgent problem and is inextricably connected to reauthorization of Section 702. Reauthorization should thus be accompanied by legislative measures to save and strengthen this important oversight body.
- An estimate of the scale of incidental collection of U.S.-person information under Section 702 would help inform public debate. Unfortunately, there remain practical obstacles to generating such an estimate.
- The FBI's U.S.-person queries of databases containing 702 data, particularly in non-national-security criminal investigations, raise civil liberties concerns. At the same time, there are colorable reasons for not prohibiting such queries altogether. Greater transparency is needed to better inform the public debate over this practice.
- The analogous capabilities of other countries—including member states of the European Union, which has criticized U.S. surveillance practices as inadequately privacy protective—are subject to less-rigorous legal constraints, oversight mechanisms, and transparency requirements than Section 702.

Recommendations

1. Reauthorize Section 702 with current authorities intact, but with the following reforms to enhance transparency and oversight:
2. Mandate that the Foreign Intelligence Surveillance Court appoint a cleared amicus curiae in every review of an annual certification under Section 702.
3. Require the Foreign Intelligence Surveillance Court to confirm, as a condition of approving the Attorney General and DNI's annual 702 certification, that the President has nominated candidates for any vacancies on the Privacy and Civil Liberties Oversight Board.
4. Exempt the Privacy and Civil Liberties Oversight Board from the Government in the Sunshine Act, which hampers the Board's efforts to oversee sensitive counterterrorism programs.
5. Empower the remaining members of the Privacy and Civil Liberties Oversight Board to collectively exercise the authorities of the Chairman when that position is vacant.
6. Ensure full implementation of Recommendation 9 from the Privacy and Civil Liberties Oversight Board's report on Section 702, including public disclosure (to the extent consistent with national security) of the resulting data about the collection and use of U.S.-person information under Section 702.
7. Encourage the intelligence community to continue to seek a statistically valid, feasible methodology for estimating the volume of incidental collection of U.S.-person data under Section 702. If these efforts do not succeed, consider creating a technical working group, perhaps under the auspices of the National Academy of Sciences, to attempt to formulate a viable approach.
8. Ask the FBI to publicly explain in greater detail why it needs to retain the ability to query databases containing Section 702 information for U.S.-person identifiers.
9. Ask the FBI to consider and explain whether it would be sufficient for it to continue its current practice of querying databases containing 702 data in non-national-security criminal investigations but, where such a query returns a hit, to initially view only the responsive metadata rather than the content.
10. Require the FBI to publish the aggregate number of annual instances in which "FBI personnel 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," a count already compelled by the Foreign Intelligence Surveillance Court.
11. Consider requiring the FBI to estimate the total number of instances in which FBI agents conducting non-national-security criminal investigations query databases containing Section 702 data using U.S.-person identifiers.
12. Require the Justice Department to provide greater detail about which "crimes involving … cybersecurity" would qualify as "serious crimes" for which the government would use 702-derived information in a criminal case.

13. Require the Justice Department to publish its standard for standard for determining whether evidence introduced in a criminal proceeding is "derived from" 702 information, which requires notice to the defendant.
14. Compare the legal, oversight, and policy constraints on Section 702 with those applicable to the analogous capabilities of other countries, particularly those countries that have used economic leverage to challenge U.S. surveillance practices.
15. Consider, as part of 702 reauthorization, using either legislative findings or report language to confirm for European audiences that the Judicial Redress Act remains in effect and, as a duly enacted statute, binds the Executive Branch.

I. INTRODUCTION

Chairman Goodlatte, Ranking Member Conyers, and members of the Committee, thank you for the opportunity to testify today. In today's chaotic world, our country faces a complex array of national security threats, both from adversary nations and from non-state terrorist groups. Recently retired Director of National Intelligence James Clapper said last year that in his 50-year career in intelligence, he could not "recall a more diverse array of challenges and crises than we confront today."[1]

In this challenging geopolitical context, the American people are fortunate to have the world's most capable intelligence services. Intelligence Community personnel work to protect the American people from a range of threats—from terrorism, to the theft of American companies' trade secrets, to subversion of our democratic processes by foreign intelligence services. In a digital world, signals intelligence is an essential tool for detecting and defeating these threats.

Our intelligence agencies, led by the NSA, carry out the signals intelligence mission under what the President Obama's Review Group on Intelligence and Communications Technologies described as a system of "oversight, review, and checks-and-balances" that "reduce[s] the risk that elements of the Intelligence Community would operate outside of the law."[2] The Review Group, which President Obama commissioned in the wake of the Snowden leaks to review U.S. signals intelligence activities, emphasized in its report that it had found "no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity."[3] That accords with other reports that have emphasized the deep-rooted culture of compliance and legal oversight at NSA.[4]

At the same time, the Snowden leaks revealed that the scale of government data collection—even collection that was lawful and approved by the Foreign Intelligence Surveillance Court—was greater than most Americans would have anticipated given the available public information, including the text of the relevant statutes. The resulting climate of skepticism, at home and abroad, continues to harm U.S. interests in various ways.[5]

This is not simply a privacy or civil liberties problem: If allowed to persist, public skepticism is also a problem for national security. That is because public trust is the foundation on which national security powers, including Section 702, ultimately rest. Needed surveillance tools will be politically sustainable only if the public is persuaded that they are necessary, appropriate, and lawful. For that reason, strengthening public confidence in the legal and institutional controls on surveillance powers should be seen as a national security imperative as well as a priority for civil libertarians.

The challenge is how to strengthen transparency, privacy, oversight, and ultimately public confidence without harming needed national security capabilities. In a recent Center for a New American Security report, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, coauthors Michèle Flournoy, Richard Fontaine, and I offered 61 recommendations to build public trust, increase transparency, and strengthen oversight, while preserving important intelligence and counterterrorism tools. Part III of this testimony suggests a number of ways the Committee can advance these goals while reauthorizing Section 702.

II. SECTION 702'S VALUE FOR NATIONAL SECURITY

In our recent report, my co-authors and I concluded, based on the available unclassified sources, that Section 702 "has become a vital intelligence tool, is legitimate in its basic contours, and is subject to adequate transparency in many, but not all, respects."[6] For that reason, we recommended that Section 702 be reauthorized with current authorities intact, but with reforms to enhance transparency and oversight.

The Committee has access to classified information documenting Section 702's value for foreign intelligence and counterterrorism, but most Americans do not. This section briefly summarizes for the general public the unclassified assessments that my co-authors and I found persuasive in reaching our judgment.

The most significant unclassified review of Section 702's efficacy and legality remains the landmark report by the independent Privacy and Civil Liberties Oversight Board.[7] The Board's five members, three Democrats and two Republicans, received classified briefings from the Intelligence Community and Department of Justice, but also consulted with outside civil-society groups, academics, and technology companies. The Board documented its findings and conclusions in a 160-page report, which provided an important public service by explaining for the American public many previously classified details about how 702 operates: the program's PRISM and upstream components, the court-approved targeting and minimization procedures that constrain the agencies' use of these tools and the data they generate, and the multi-layered oversight system that ensures compliance with these rules.

After this review, the Board unanimously reached a measured but broadly positive conclusion about the overall utility, lawfulness, and oversight of Section 702:

> "[T]he information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse."[8]

Publicly available statistics declassified by the Office of the Director of National Intelligence suggest that Section 702 has become a central foreign intelligence tool. Overall, in 2015, the intelligence community targeted 94,368 overseas individuals, groups, or entities under Section 702.[9] That is compared to only 1,695 targets of orders issued under "traditional" FISA.[10] While this is not an apples-to-apples comparison, it does give a rough sense of the significance of Section 702 for our foreign intelligence enterprise.

The available evidence also indicates that Section 702 has been a particularly significant tool for counterterrorism. The Privacy and Civil Liberties Oversight Board reported that, as of 2014, "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[11] The Board also found that "[m]onitoring terrorist networks under Section

702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics"; that it "has led the government to identify previously unknown individuals who are involved in international terrorism"; and that it "has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."[12]

Other sources echo the Board's judgment that Section 702 is a vital tool for counterterrorism and foreign intelligence more broadly. Matthew Olsen, former General Counsel of NSA and former Director of the National Counterterrorism Center, told this Committee's Senate counterpart last spring that Section 702 "has proven to be a vital authority for the collection of foreign intelligence to guard against terrorism and other threats to our national security" and "has significantly contributed to our ability to prevent terrorist attacks inside the United States and around the world."[13] NSA has publicly described Section 702 as the "most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[14]

III. Civil Liberties Safeguards and Concerns

As the Privacy and Civil Liberties Oversight Board explained, Section 702 is subject to both "judicial oversight and extensive internal supervision."[15] To be sure, judicial oversight of Section 702 differs significantly from judicial review under traditional FISA: The Foreign Intelligence Surveillance Court reviews the Section 702 program *as a whole*, on an annual basis, rather than reviewing each target individually. Once a year, the Director of National Intelligence and the Attorney General must submit to the FISC a joint "certification" specifying how the program will be administered and what safeguards apply.[16] The FISC then reviews and approves or disapproves that certification, as well as agency minimization and targeting procedures, subject to any conditions the court imposes.[17] As required by the USA Freedom Act, many significant FISC opinions, including the court's review of the 2015 Section 702 certification, have been declassified and published.[18]

As we wrote in our recent Center for a New American Security report, programmatic rather than individualized judicial review is appropriate for Section 702 "given that the targets are non-U.S. persons living outside the United States."[19] Section 702 occupies, legally speaking, a novel middle ground between traditional domestic surveillance under FISA and overseas surveillance governed by Executive Order 12333. Traditional FISA requires, generally speaking, individualized judicial orders for foreign-intelligence surveillance, conducted in the United States, of those *present in the United States*.[20] By contrast, those targeted under Section 702—non-U.S. persons overseas—are not protected by the Fourth Amendment,[21] and their messages to other non-Americans have traditionally been subject to surveillance without judicial oversight.[22] On the other hand, 702 surveillance transpires on U.S. soil and foreseeably results in the interception of a significant (but unknown) number of messages with one U.S. communicant, which previously could have been collected on U.S. soil only with a FISA warrant.[23] Section 702's annual, programmatic judicial oversight strikes a reasonable middle ground between the geographic location of the surveillance (in the U.S.), the geographic location and nationality of the targets (non-U.S. persons located overseas), and the foreseeable consequence that some messages with a U.S. communicant will be collected.

Surveillance under Section 702, and the subsequent retention and dissemination of information it produces, must also comply with detailed, 702-specific targeting and minimization

procedures, which are reviewed and approved by the Foreign Intelligence Surveillance Court during its annual review.[24] The Office of the Director of National Intelligence has published online, with relatively few redactions, the 702 minimization rules for the NSA, FBI, CIA, and National Counterterrorism Center.[25] Recent compliance assessments by the Attorney General and the Office of the Director of National Intelligence have found a low rate of inadvertent "compliance incidents" and no intentional attempts to circumvent these rules.[26]

It is important to note that the implementation and oversight constraints applicable to Section 702 have changed significantly since the program's last reauthorization five years ago. Since the Snowden leaks in 2013, Section 702 has undergone many significant privacy, transparency, and governance reforms. Most importantly, the government has fully implemented most of the recommendations in the Privacy and Civil Liberties Oversight Board's report on Section 702, and is working to implement those that remain. These include:

- Revising the FBI's minimization procedures to accurately reflect its querying of 702 data in investigations unrelated to foreign intelligence,[27]
- Requiring better documentation of the foreign-intelligence purpose of NSA and CIA queries of 702 data using U.S.-person identifiers,[28]
- Enhancing the FISC's ability to review 702 targeting practices and U.S.-person query terms used by the NSA and CIA,[29]
- Periodically reassessing whether upstream collection under Section 702 uses the best available technology to ensure that only authorized communications are collected,[30] and
- Making publicly available the current NSA, CIA, and FBI minimization procedures for Section 702.[31]

In addition, the USA Freedom Act implemented a number of changes with spillover benefits for accountability and oversight of Section 702. These include:

- Enabling the Foreign Intelligence Surveillance Court to appoint cleared amici curiae to present "legal arguments that advance the protection of individual privacy and civil liberties" in cases presenting novel legal issues,[32]
- Expanding appellate review of FISC decisions,[33]
- Releasing to the public, to the extent consistent with national security, past and future FISC decisions in cases presenting significant or novel issues,[34] and
- Allowing private companies subject to FISA orders to provide the public with more detail about the volume of surveillance orders they receive.[35]

One relatively simple way for Congress to build on this progress and further strengthen 702 oversight would be to mandate the appointment of a FISC amicus curiae in every review of annual certifications under Section 702. One of the cleared FISC advocates, Amy Jeffress, participated constructively in the FISC's review of the government's 2015 certifications for the Section 702 program.[36] Under current law, whether to appoint an amicus is in the court's discretion.[37]

Guaranteeing that an amicus will be appointed in this narrow, but very important, category of cases would strengthen the public credibility of Section 702's programmatic judicial oversight.

The Privacy and Civil Liberties Oversight Board

In my opinion, the most urgent privacy and civil liberties issue before the Committee during this reauthorization process is the crisis facing the Privacy and Civil Liberties Oversight Board. This is somewhat counterintuitive, as the Board was not created by the FISA Amendments Act and its responsibilities are broader than Section 702. In recent years, however, the Board has been an essential source of public-facing oversight and accountability for the government's implementation of Section 702. Unfortunately, the Board is now in crisis, unable to take official action and in danger of fading into permanent paralysis.

The Board emerged from a recommendation of the 9/11 Commission, which called for a "board within the executive branch to oversee … the commitment the government makes to defend our civil liberties."[38] Since 2013, the Board has become a prominent feature of the oversight landscape for counterterrorism and surveillance programs. Most important have been the Board's comprehensive and well-regarded public reports—particularly its report on Section 702, which enhanced public understanding by declassifying many basic facts about how the program operates.

Importantly, the Board's value extends beyond privacy and civil liberties: A credible, independent Board also benefits national security and the intelligence community. Precisely because of the Board's independence and bipartisan credibility, its statement that Section 702 is "valuable and effective" provides a powerful argument for reauthorizing the program in its current form. The Board's reputation as a vigorous and independent voice also helps intelligence officials make the case to other countries that U.S. surveillance programs are subject to robust oversight and legal controls. For example, in a letter designed to address European concerns related to the Privacy Shield agreement, the General Counsel of the Office of the Director of National Intelligence cited the Board and its public reports as evidence of the "rigorous and multi-layered" oversight of U.S. intelligence.[39]

Unfortunately, the Board is on the verge of becoming defunct: With only two of five Senate-confirmed members remaining, it lacks a quorum and thus cannot take official action. (One of those two remaining members has now been nominated for a senior position in the Justice Department.) Another institutional challenge is that without a Chairman, the Board has been unable to hire new staff since last summer.

The crisis facing the Board is intimately connected to reauthorization of Section 702. Strong national security powers—which we need to keep our country safe—must be balanced by strong and credible oversight. That comes first and foremost from the Congress, but also (subject to constitutional and statutory limits) from the courts and from internal Executive Branch bodies like the Board. As the Board's 702 report and its subsequent recommendations-assessment reports demonstrate, a functioning, independent Board is a key element of the "rigorous and multi-layered" oversight of Section 702.[40]

In reauthorizing Section 702, Congress should also act to revive the Board and ensure its future viability. Specifically, in the reauthorization legislation, Congress should require the FISC to confirm, as a condition of approving the Attorney General and DNI's annual 702 certification, that the President has nominated candidates for any vacancies on the Board.[41] This will ensure that Presidents have an adequate incentive to make nominations to the board. There is no reason why requiring nominations (as opposed to confirmation of those nominees) to be in place would obstruct or delay annual recertifications of the program.

In addition, to enhance the Board's functioning Congress should, as part of Section 702 reauthorization, enact legislation exempting the Board from the Government in the Sunshine Act. That statute requires that meetings—which are vaguely defined as "deliberations" involving more than two members—take place in public if they "result in the joint conduct or disposition of official agency business."[42] There are several reasons why this is unnecessary for the Board.

First, and most importantly, the Sunshine Act's purpose—ensuring that regulatory power is exercised in public rather than in smoke-filled back rooms—does not apply to the Board. The Board exercises no regulatory power; its only authorities are to conduct oversight and provide advice. For an oversight body, the benefits of informal collaboration far outweigh any possible concern about opaque decisionmaking. Indeed, because the Sunshine Act obstructs the Board's oversight work, it perversely *impedes* efforts to bring "sunshine" to counterterrorism programs.

Another reason why the Sunshine Act is a poor fit is that the Board's work is overwhelmingly classified. This means that it is forced to squander substantial time repeatedly invoking the Act's cumbersome procedures for closing meetings.[43] In addition, because four of the Board's five members are part-time and have outside obligations, their schedules make it challenging to hold frequent formal meetings. Congress should remove this nuisance, which, ironically undermines transparency by preventing the Board from being as effective as it might be.

Finally, to ensure that the Board is not hampered in the future by the absence of a Chairman, Congress should enact legislation permitting the remaining members to collectively exercise the authorities of the Chairman if the position of Chairman is vacant.[44]

Incidental Collection

Even with the many legal, oversight, and compliance safeguards in place, Section 702 raises legitimate concerns for domestic civil liberties. The most noteworthy is the incidental collection of communications of or about U.S. persons and the subsequent use of such information. While Section 702 cannot be used to *target* U.S. persons, their communications can be "incidentally collected" if they communicated with a targeted non-U.S. person. Foreign-foreign communications may also contain information about a U.S. person, even if he or she is not one of the communicants.

No one knows how much U.S.-person information is incidentally collected under Section 702. As the Privacy and Civil Liberties Oversight Board explained: "[L]awmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702."[45] The public debate over Section 702's implications for domestic civil liberties would

be better informed if the public had a more accurate sense of how much U.S.-person data is collected.

Recommendation 9 in the Privacy and Civil Liberties Oversight Board's report on Section 702 urged the NSA to track five measures that would "shed some light on the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized under Section 702."[46] These were:

1. The number of telephone communications acquired in which one caller is located in the United States;
2. The number of Internet communications acquired through upstream collection that originate or terminate in the United States;
3. The number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work;
4. The number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and
5. The number of instances in which the NSA disseminates non-public information about U.S. persons.[47]

As of last February, NSA had implemented two of these measures in substantial part, but had "confronted a variety of challenges" in implementing the final three.[48] As it works toward reauthorizing Section 702, Congress should ensure that NSA fully implements Recommendation 9, and should encourage the maximum public reporting of these figures that is consistent with national security.

Some members of this Committee and a number of advocacy groups have urged NSA to attempt a statistical estimate of all incidental collection, by counting the number of U.S.-person communications within a representative sample of communications gathered under 702.[49] The government has noted that such a review would inflict some additional privacy harm on those Americans whose incidentally collected communications would otherwise have "aged off" NSA servers before being reviewed.[50] On balance, however, this limited harm would be justified by the benefits an estimate of incidental collection would produce for public accountability—*if* a statistically valid, feasible methodology of conducting such an estimate can be found.

Unfortunately, a viable methodology has proven difficult to find, and ultimately may not exist. The primary reason is that electronic communications collected under Section 702 typically lack information that would enable officials to determine the nationality of the communicants. Emails, for example, do not list the nationality of the sender and recipient, much less of people mentioned in the body text. Undertaking additional investigation beyond the four corners of the communication to determine the nationality of the communicants and others discussed in the message would be intrusive from a privacy perspective and unreasonably labor-intensive.

Given the potential value of a valid estimate, it is worth continuing to attempt to surmount these obstacles, even if no practicable solution is ultimately found. Our report thus recommended that the intelligence community persist in seeking to develop an approach that would yield an accurate, statistically valid estimate of incidental collection. If these efforts do not succeed, Congress should consider convening a technical working group, perhaps under the auspices of the National Academy of Sciences, to attempt to develop a viable approach.[51]

U.S.-Person Queries

One of the most challenging civil-liberties issues facing Congress during the reauthorization process is the practice of querying Section 702 data for U.S.-person identifiers—particularly in criminal investigations unrelated to national security. As a routine investigative step, FBI agents and analysts may check to see what information the Bureau's records already contain about a person. At least one of those databases contains foreign intelligence information, including intelligence collected both under Section 702 and from traditional FISA.[52] While the Foreign Intelligence Surveillance Court has held that such queries comport with the Fourth Amendment,[53] they nonetheless raise legitimate privacy concerns—particularly if such information flows downstream into the criminal justice system.

On the other hand, there are also colorable arguments for not prohibiting such queries altogether. The 9/11 Commission explained that one of the key reasons the 9/11 attacks succeeded was the government's failure to synthesize pieces of information that different agencies possessed. Put simply, government agencies failed to "connect the dots" in time to disrupt the attacks.[54] This failure was particularly pronounced across what the Commission termed the "foreign-domestic divide"—the gap between foreign intelligence and domestic law-enforcement investigations. For example, within the Justice Department and FBI, many believed that the Bureau "could not share any intelligence information with criminal investigators," with the result that "relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators."[55] These information-sharing blockages contributed to the tragic failure to locate 9/11 hijacker Khalid al Mihdhar, whom the government knew had entered the United States.[56] Had Mihdhar been arrested, the government might well have foiled the 9/11 attacks.[57]

If there is a connection between a person under FBI investigation in the United States and foreign-intelligence information the government has already collected under 702—including the communications of known terrorists—it is important for the FBI to be aware of that. Indeed, Section 702 is particularly likely to identify connections relevant to transnational threats like terrorism, foreign espionage, and proliferation. That is because Section 702 is used to target individuals of foreign-intelligence interest (that is, non-U.S. "persons assessed to possess foreign intelligence information or who are reasonably likely to receive or communicate foreign intelligence information").[58] If an FBI agent conducting a domestic investigation receives a hit when querying 702 information, that means that the subject of the query communicated with, or was mentioned in a communication to or from, a person of foreign-intelligence interest. Some (perhaps many) such connections will be innocent, but others will be problematic and previously unknown to investigators. The latter represent the type of foreign-domestic linkages that can help the FBI detect and prevent terrorist attacks.

Unfortunately, relatively little public information is available about these queries: their frequency, how often they return 702 information, and precisely why the FBI views them as valuable. The result is that estimates of both the practice's value for national security and its civil-liberties implications are unavoidably conjectural. Greater transparency is needed to better inform the public debate. Our recent report offered several recommendations in this vein.

First, the FBI should publicly explain in greater detail why it values the ability to query databases containing Section 702 information for U.S.-person identifiers. In so doing, it should also explain why other investigative techniques would not be as effective. To be sure, there may be persuasive answers to these questions.[59] Even so, more information about the role these queries play in FBI investigations and the suitability of possible alternatives could help strengthen the public legitimacy of this practice.

Second, Congress should ask the Bureau to consider whether an alternative form of these queries would suffice to enable it to identify previously unknown, problematic foreign-domestic connections. Specifically, the FBI should consider and explain whether it would be sufficient for it to continue its current practice of querying databases containing 702 data in non-national-security investigations but, where such a search returns a hit, *to view only the responsive metadata* rather than the content.

This is worth considering because the key function of these queries appears to be identifying previously unknown, potentially significant foreign-domestic links. In most cases, the metadata of responsive communications should suffice to reveal those connections. If metadata suggests a problematic connection, it could be used to establish individualized suspicion to view the underlying content and to deploy other investigative tools in the FBI's arsenal.

Third, as part of Section 702's reauthorization, Congress should provide for increased public transparency about the querying and use of 702 information about U.S.-persons in non-national-security FBI investigations. The FBI reports that it is "extremely unlikely that an agent or analyst who is conducting an assessment of a non-national-security crime would get a responsive result from the query against the [FBI's] Section 702-acquired data."[60] One possible reason for this is that the FBI does not receive data from 702's upstream component, which for technical reasons "has a higher likelihood than PRISM of collecting … some wholly domestic communications."[61]

If there is indeed a reassuring story to tell here, greater public transparency would help the FBI tell it. To that end, Congress should:

i. Require the FBI to publish the number of annual instances in which "FBI personnel 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."[62] The FISC already requires the Bureau to report these instances to the Court,[63] so counting them should not impose an additional administrative burden. While the details of these reports must remain classified, it is hard to imagine any national security harm that would result from publishing the overall number of such occurrences.

ii. Consider requiring the FBI to estimate the total number of instances in which FBI agents conducting non-national-security criminal investigations query databases containing Section 702 data using U.S.-person identifiers. The FBI's systems are not designed to "identify whether the query terms are U.S.-person identifiers,"[64] because "nationality is not relevant to most criminal investigations."[65] The Bureau should not be asked to revamp its record-keeping system in order to produce this data; a statistically representative sample of cases would suffice.

Fifth, Congress should require increased public transparency about the downstream use in the criminal-justice system of information derived from Section 702. Specifically:

i. Congress should require the Justice Department to provide greater detail about which "crimes involving … cybersecurity"—a broad category potentially encompassing both very grave and less consequential offenses[66]—would qualify as "serious crimes" for which the government would use 702-derived information in a criminal case.[67]

ii. Congress should also require the Justice Department to publish its standard for whether evidence introduced in a criminal proceeding was "derived from" 702 information, which requires notice to the defendant.

IV. Section 702 in International Perspective

Since 2013's Snowden leaks, the United States has faced international pressure over its surveillance practices, particularly from the European Union. This pressure has been heightened by the leverage that European privacy law provides over U.S. companies' transfers of European data to the United States. The scramble in late 2015 and early 2016 to find a replacement to the U.S.-EU Safe Harbor agreement, and the concessions that the United States made to obtain the successor Privacy Shield accord, demonstrate that this leverage is significant.[68]

It is in the U.S. national interest to reduce conflict with Europe over surveillance policy—in particular, to ensure that the economically important Privacy Shield agreement remains in force. That does not mean, however, that the United States should make additional unreciprocated concessions to European critics of U.S. surveillance practices. More to the point: Congress should not materially alter Section 702 in an attempt to appease European critics. To begin with, the significant unreciprocated concessions that the United States already made in the wake of the Snowden leaks are not well known in Europe and have generated little goodwill for the United States. For example, one German expert told our CNAS team that most Germans are "totally unaware" of Presidential Policy Directive 28, a commitment without apparent historical precedent, and which no other country has matched. What's more, European allies benefit directly from Section 702 by way of intelligence sharing from the United States. The problem is that European security services have little incentive, and ample political disincentive, to publicize this cooperation.

A better approach to shoring up Privacy Shield would be for the United States to demonstrate that the terms of that agreement are being robustly enforced, while at the same time (i) encouraging an amicable comparison between our legal and oversight regime and those of our European allies, and (ii) quietly demonstrating to Europe that the United States has a "Plan B,"

other than further unilateral concessions, should the European Court of Justice issue another flawed decision like *Schrems v. Data Protection Commissioner*. That decision, which effectively killed the Safe Harbor agreement, was informed, at least in part, by an inaccurate understanding of Section 702. Our recent Center for a New American Security report proposes numerous concrete steps the United States can take to effectuate this approach.[69]

In particular, the United States should welcome and encourage a comparison between its privacy and oversight regime and Europe's. Since the Snowden leaks, the U.S. has made commitments to respect the privacy rights of Europeans that far outstrip anything European nations have done in return. For example, no European country has reciprocated for Americans the commitments in Presidential Policy Directive 28. The closest comparator of which I am aware is Germany's recent law, analogous to Section 702, governing domestic collection of foreign-foreign communications.[70] That law grants heightened privacy protections to EU institutions, EU member states, and EU citizens, but nothing for Americans. Nor have EU member states offered Americans a privacy Ombudsperson and judicial-redress rights like those the United States gave Europeans as part of the Privacy Shield.[71]

More broadly, the United States' legal and oversight regime for government surveillance, including against non-U.S. persons, is equivalent to or stronger than the systems in place in leading European countries. Only two of the EU countries analyzed in a study by the law firm Sidley Austin "require judicial authorization for intelligence surveillance"; instead, "most place such authorization in the hands of government ministers."[72] Most relevant here, France, Germany, the United Kingdom, and the Netherlands all "explicitly permit certain types of surveillance that," unlike the selector-based Section 702, "are not targeted at identified suspected individuals."[73] None of these countries' laws explicitly require minimization, while retention limits apply only to a few narrow categories of data.[74]

This reauthorization process offers an opportunity to correct misperceptions about Section 702 that are widely held overseas. To that end, Congress can perform a valuable public service by comparing, whether through hearings or oversight reports, the substantive scope of Section 702 and the applicable legal constraints, oversight mechanisms, and transparency requirements, with the analogous programs of other countries—particularly countries that have criticized the United States for its surveillance practices.

One final issue bears brief mention here. The recent Executive Order on "Enhancing Public Safety in the Interior of the United States" ordered federal agencies, "to the extent consistent with applicable law," to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[75] This triggered alarm among some privacy advocates, and apparently some European observers, that the order had revoked protections that the United States promised European citizens as part of the Privacy Shield. That was incorrect: The Judicial Redress Act of 2015 extends the relevant rights by statute, which could not be (and thus was not) superseded by the Executive Order.[76]

Clearing up any such misconceptions and clarifying that the elements of the deal underlying Privacy Shield remain in place could increase the odds that it survives European judicial review. To

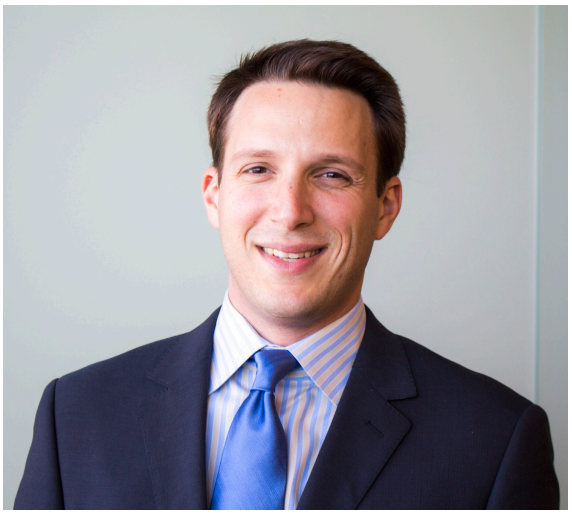
that end, Congress should consider, as part of 702 reauthorization, using either legislative findings or report language to confirm that the Judicial Redress Act remains in effect and, as a duly enacted statute, binds the Executive Branch.

Thank you again for the opportunity to testify.

* * *

Biography

Adam Klein
Senior Fellow, Center for a New American Security



Adam Klein is a Senior Fellow at the Center for a New American Security, a bipartisan national security research organization in Washington. His research centers on the intersection of national security policy and law, including government surveillance in the digital age, counterterrorism, and rules governing the use of military force. Before coming to CNAS, Adam served as a law clerk to Justice Antonin Scalia of the United States Supreme Court and Judge Brett Kavanaugh of the U.S. Court of Appeals for the D.C. Circuit, and was a Senior Associate at WilmerHale, an international law firm. He is currently a member of the Executive Committee of the Federalist Society's International and National Security Law Practice Group. Adam has also worked on national security policy at the RAND Corporation, at the 9/11 Public Discourse Project, the nonprofit successor to the 9/11 Commission, and in the office of U.S. Representative C.W. "Bill" Young. Adam speaks German and French and is a former Robert Bosch Foundation Fellow in Berlin.

ENDNOTES

[1] Mark Landler, *North Korea Nuclear Threat Cited by James Clapper, Intelligence Chief*, N.Y. Times, Feb. 9, 2016, *available at* http://www.nytimes.com/2016/02/10/world/asia/north-koreanuclear-effort-seen-as-a-top-threat-to-the-us.html.

[2] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 75 (Dec. 12, 2013).

[3] *Id.* At 31-32.

[4] *See, e.g.,* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 103 (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf ("The Board has been impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program.") (hereinafter "PCLOB 702 Report").

[5] *See* A. Klein, M. Flournoy, & R. Fontaine, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond* 17-21 (Dec. 2016), *available at* https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Surveillance-Final.pdf (hereinafter "CNAS Surveillance Policy Report").

[6] CNAS Surveillance Policy Report, *supra* note 5, at 24.

[7] PCLOB 702 Report, *supra* note 4.

[8] *Id.* at 2.

[9] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2015*, at 5, *at* https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.

[10] *Id.* at 4.

[11] *Id.* at 10.

[12] *Id.*

[13] Testimony before the Senate Committee on the Judiciary (May 10, 2016), *at* https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf.

[14] NSA, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* (Aug. 9, 2013), *at* https://www.nsa.gov/news-features/press-room/statements/2013-08-09-thensa-story.shtml.

[15] PCLOB 702 Report, *supra* note 4, at 2.

[16] *See* 50 U.S.C. § 1881a(g).

[17] *See* 50 U.S.C. § 1881a(i).

[18] *See infra* note 24.

[19] CNAS Surveillance Policy Report, *supra* note 5, at 24.

[20] *See* 50 U.S.C. § 1801 *et seq.* Other provisions of the FISA Amendments Act require individualized judicial orders to target *U.S. persons* overseas. *See* 50 U.S.C. §§ 1881b-1881c.

[21] *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). *Verdugo* includes the caveat that the alien involved lacked a preexisting "substantial connection" to the United States. *Id.* at 271-272.

[22] *Cf.* Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702*, Hoover Institution Aegis Paper Series, No. 1604 (2016), *at* http://www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf.

[23] *See* 50 U.S.C. § 1801(f)(2); David Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, Hoover Institution Aegis Paper Series No. 1601, at 3 (2016), *at* http://www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf.

[24] *See, e.g.*, Memorandum Opinion and Order, No. [redacted], at 12 (F.I.S.C. Nov. 6, 2015), *at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (hereinafter "2015 FISC Opinion").

[25] Office of the Director of National Intelligence, *Release of 2015 Section 702 Minimization Procedures* (Aug. 11, 2016), https://icontherecord.tumblr.com/tagged/section-702.

[26] *See* Department of Justice & Office of the Director of National Intelligence, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence* 27-28 (Nov. 2016).

[27] Privacy and Civil Liberties Oversight Board, Recommendations Assessment Report 16 (Feb. 5, 2016).

[28] *Id.* at 18.

[29] *Id.* at 19.

[30] *Id.* at 21.

[31] *Id.* at 23.

[32] *See* 50 U.S.C. § 1803(i).

[33] *See* PCLOB Recommendations Assessment Report, *supra* note 27, at 5-6.

[34] *See id.* at 7-8.

[35] *See id.* at 10.

[36] *See generally* 2015 FISC Opinion, *supra* note 24.

[37] *See* 50 U.S.C. § 1803(i).

[38] *See, e.g.*, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* 395 (2004).

[39] Letter from Robert Litt to Justin Antonipillai, Counselor, Department of Commerce, and Ted Dean, Deputy Assistant Secretary, International Trade Administration (February 22, 2016), at 7, *at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

[40] *See id.*

[41] *See* 42 U.S.C. § 2000ee(h)(1).

[42] 5 U.S.C. § 552b.

[43] *See* Patricia Wald, Responses to Sen. Chuck Grassley Questions for the Record 5, *at* https://www.judiciary.senate.gov/imo/media/doc/Wald-Reappoint-Responses-to-Grassley.pdf.

[44] *Cf.* S. 3017, Intelligence Authorization Act for Fiscal Year 2017, 114th Cong., § 602.

[45] PCLOB 702 Report, *supra* note 4, at 147.

[46] *Id.* at 146-147.

[47] *Id.* at 146.

[48] PCLOB Recommendations Assessment Report, *supra* note 27, at 25.

[49] Letter from House Judiciary Committee Members to Director of National Intelligence James Clapper (Apr. 22, 2016), *at* https://assets.documentcloud.org/documents/2811050/Letter-to-Director-Clapper-4-22.pdf; Letter from Privacy Groups to Clapper (Oct. 29, 2015), *at*

https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[50] *See* PCLOB 702 Report, *supra* note 4, at 147.

[51] *Cf.* National Academies, *Committee Membership: Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs* (Sept. 7, 2016), *at* https://www8.nationalacademies.org/cp/CommitteeView.aspx?key=49806.

[52] PCLOB 702 Report, *supra* note 4, at 59.

[53] 2015 FISC Opinion, *supra* note 24.

[54] *9/11 Commission Report* at 355-356.

[55] *Id.* at 79.

[56] *Id.* at 269-272.

[57] *See id.* at 272 (concluding that detention of Mihdhar or Nawaf al Hazmi "could have derailed the plan").

[58] PCLOB 702 Report, *supra* note 4, at 22 n.56.

[59] *See* CNAS Surveillance Policy Report, *supra* note 5, at 36.

[60] PCLOB 702 Report, *supra* note 4, at 60.

[61] Testimony of Rachel Brand before the Senate Committee on the Judiciary 5 (May 10, 2016), *at* https://pclob.gov/library/20160510-R%20Brand%20testimony%20SJC.pdf.

[62] *See* 2015 FISC Opinion, *supra* note 24, at 78.

[63] *See id.*; *see also DOJ/ODNI Semiannual Assessment*, *supra* note 26, at 16.

[64] PCLOB 702 Report, *supra* note 4, at 59.

[65] Brand Testimony, *supra* note 61, at 9.

[66] *See, e.g.*, *United States v. Nosal*, Nos. 14-10037 & 14-10275 (9th Cir. Dec. 8, 2016).

[67] *See* Remarks of Robert Litt at the Brookings Institution (Feb. 4, 2015), *at* https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on; CNAS Surveillance Policy Report, *supra* note 5, at 38.

[68] *See id.* at 57.

[69] *See id.* at 50-57.

[70] *Available at* http://dip21.bundestag.de/dip21/btd/18/090/1809041.pdf; *see also* Library of Congress Global Legal Monitor, *Germany: Powers of Federal Intelligence Service Expanded*, *at* http://www.loc.gov/law/foreign-news/article/germany-powers-of-federal-intelligence-service-expanded/.

[71] *See* CNAS Surveillance Policy Report, *supra* note 5, at 53.

[72] Jacques Bourgeois et al., Sidley Austin LLP, *Essentially Equivalent: A comparison of the legal orders for privacy and data protection in the European Union and United States* 5 (Jan. 2016), http://www.sidley.com/~/media/publications/essentially-equivalent---final.pdf.

[73] *Id.* at 37.

[74] *Id.* at 51.

[75] *Available at* https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[76] This is discussed in greater detail in *The "Interior Security" Executive Order, the Privacy Act, and Privacy Shield*, Carrie Cordero & Adam Klein, Lawfare, Jan. 27, 2017, *at* https://lawfareblog.com/interior-security-executive-order-privacy-act-and-privacy-shield.