June 27, 2017

Testimony before the Senate Committee on the Judiciary

Hearing on The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties

Adam Klein
Robert M. Gates Senior Fellow, Center for a New American Security

—

Executive Summary

Principal Findings

- Section 702 is a valuable intelligence tool that is legitimate in its basic contours and subject to adequate oversight and transparency in most respects. It should be reauthorized with existing statutory authorities intact.
- The government's implementation of Section 702 has already undergone significant reform since Congress last reauthorized the FISA Amendments Act in 2012.
- Targeted reforms to enhance transparency, oversight, and accountability could strengthen public trust without harming national security.
- Congress should be careful to avoid changes that would reduce Section 702's operational utility, increasing the risks of future terrorist attacks. In particular, Congress should not require agencies to obtain a court order in order to query data already collected under 702.

Key Recommendations

- Reauthorize Section 702 with existing statutory authorities intact.
- Mandate that the Foreign Intelligence Surveillance Court appoint a cleared amicus curiae in every review of an annual certification under Section 702.
- 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.
- Require the Justice Department to provide greater detail about which "serious crimes" the government would use 702 information to prosecute, and about how it determines whether evidence introduced in a criminal proceeding is "derived from" 702.
- Consider targeted reforms to deter leaks of U.S.-person information derived from foreign-intelligence intercepts and to enhance oversight of politically sensitive unmasking requests.

- Exempt the Privacy and Civil Liberties Oversight Board from the Government in the Sunshine Act, which is unnecessary given existing, Board-specific transparency requirements and impedes the Board's efforts to oversee sensitive counterterrorism programs.
- 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.

I. INTRODUCTION

Chairman Grassley, Ranking Member Feinstein, and members of the Committee, thank you for the opportunity to testify. Our nation faces an unusually complex array of national security threats, ranging from adversary powers, to non-state terrorist groups, to cyber intruders whose identities are often unclear. 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]

The American people are fortunate to have the world's most capable intelligence services to confront these threats. Our intelligence agencies carry out the signals intelligence mission under what the President'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 2013 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 recognized the culture of compliance and legal oversight at NSA.[4] Most importantly, the Privacy and Civil Liberties Oversight Board found "no evidence of intentional abuse" in its review of Section 702.[5]

At the same time, the 2013 disclosures 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.[6] Recent controversies involving leaks and alleged partisan unmasking of U.S.-person identifiers have amplified and broadened this skepticism.

This is not merely a civil liberties problem: Public skepticism is also a problem for national security, because public trust is the foundation on which national security powers, including Section 702, ultimately rest. Needed surveillance authorities will be politically sustainable only if the public believes 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.

The challenge is how to strengthen transparency, privacy, oversight, and ultimately public confidence without harming needed national security capabilities. In a 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. 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 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."[7] For that reason, we recommended that Section 702 be reauthorized with existing statutory authorities intact.

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 2014 report by the independent Privacy and Civil Liberties Oversight Board.[8] The Board's five members, three Democrats and two Republicans, received classified briefings from the implementing agencies, 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 explained to the American public many previously classified details about how 702 operates: the program's downstream (PRISM) and upstream components, the court-approved targeting and minimization procedures that constrain agencies' use of these tools and the data they generate, and the multi-layered oversight system that ensures compliance.

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."[9]

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 2016, the intelligence community targeted 106,469 overseas individuals, groups, or entities under Section 702, up from 94,368 last year.[10] That is compared to only 1,687 targets of court orders issued under "traditional" FISA.[11] 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."[12] The Board also found that 702 "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."[13] NSA has 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]

In several publicly reported cases, 702 is known to have played a key role in a significant counterterrorism success. The best-known case is that of Najibullah Zazi, a Colorado resident who emailed an al Qaeda courier in Pakistan seeking advice on building explosives. Fortunately, the courier's email was being collected by NSA under Section 702. That collection enabled the FBI to identify Zazi and arrest him and his co-conspirators before they could execute their "imminent plans" to bomb the New York City subway.[15] Mohamed Mohamud, an Oregon resident, communicated with a foreigner abroad who was targeted under 702. Alerted by that contact, the FBI began investigating Mohamud, who was ultimately convicted of trying to bomb Portland's annual Christmas Tree Lighting ceremony.[16] Most recently, Director of National Intelligence Coats reported that intelligence from Section 702 enabled U.S. Special Forces to track down Abd al-Rahman Mustafa al-Qaduli (aka "Hajji Imam"), a top-level member of ISIS's leadership in Syria. The IC provided several additional real-world examples in a recent Fact Sheet.[17]

It is important to note, however, that Section 702's value for counterterrorism cannot be measured solely in terms of specific, identifiable plots disrupted. The Privacy and Civil Liberties Oversight Board explained 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."[18] These broader insights are enormously valuable in the global struggle against terrorist groups. Moreover, intelligence operations and analytic assessments typically rely on a mosaic of sources, meaning that it is often hard to identify one source as exclusively responsible for a given success.

Taking a significant piece out of the broader mosaic of information available to our intelligence agencies will make our efforts against terrorism, espionage, cyber intrusions, counterproliferation, and other intelligence challenges less effective. That effect may be hard to quantify, but the publicly available evidence suggests that it would be significant.

III. Safeguards and Transparency

The people's representatives in Congress are the ultimate overseers of all intelligence programs. But Section 702 is also subject to extensive oversight by the Judiciary and within the Executive Branch.

Judicial Oversight

As the Privacy and Civil Liberties Oversight Board explained, Section 702 is subject to both "judicial oversight and extensive internal supervision."[19] To be sure, judicial oversight of Section 702 differs significantly from judicial review under traditional FISA: The Foreign Intelligence Surveillance Court reviews the 702 program 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.[20] The FISC then reviews and approves or disapproves certifications submitted by the AG and DNI, as well as agency minimization and targeting procedures, subject to any conditions

the court imposes.[21] As required by the USA Freedom Act, many significant FISC opinions, including key opinions on Section 702 from 2015 and 2017, have been declassified.[22]

As my co-authors and I 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."[23] Section 702 occupies a middle ground between traditional domestic surveillance under Title I of 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*.[24] Those targeted under Section 702—non-U.S. persons overseas—are not protected by the Fourth Amendment,[25] and their messages to other non-Americans have traditionally been subject to surveillance without judicial oversight.[26]

On the other hand, 702 surveillance transpires on U.S. soil and foreseeably results in the interception of some messages involving a U.S. communicant.[27] Section 702's programmatic judicial oversight strikes a reasonable middle ground between the location of the surveillance (in the U.S.), the 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 incidentally collected.

Minimization and Targeting Rules and Executive Branch Oversight

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.[28] 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.[29] Compliance assessments by the Attorney General and the Office of the Director of National Intelligence have found no intentional attempts to circumvent these rules.[30]

Compliance with these limitations is subject to extensive oversight within the Executive Branch: by attorneys and compliance officers at the implementing agencies; by the Justice Department's National Security Division, whose attorneys review *every selector* tasked by *NSA* under Section 702 and conduct bimonthly reviews to ensure that querying practices comply with the minimization procedures[31]; by inspectors general[32]; and by the independent Privacy and Civil Liberties Oversight Board, which is discussed in more detail below.

All told, Section 702 is enmeshed in a web of supervision that spans all three branches of government. Few government powers are subject to such comprehensive, multi-layered oversight.

Transparency

Finally, the Intelligence Community's own transparency efforts have given the public and the press far greater insight into how Section 702 operates. ODNI's annual statistical transparency reports and publication of agency minimization procedures provide an invaluable resource for those of us who study these issues outside of the government. The wealth of information available on IC On the Record, the IC's official transparency website, demonstrates that the IC's commitment to its

Principles of Intelligence Transparency is real and meaningful. No other country provides a remotely comparable level transparency about its classified intelligence operations.

As my co-authors and I argued in our CNAS *Surveillance Policy* report, future "surveillance policy will have to account not merely for national security needs, but also respond to the public's demand for rigorous oversight and transparency."[33] By any objective measure, the IC—and especially the NSA, long known for its deep secrecy—have adapted well to the unprecedented level of public scrutiny they have faced since 2013. Senior IC leaders are now publicly known figures who venture forth to explain their policies and practices to the American people. IC transparency reports and declassified FISC opinions have disclosed, in a responsible way, useful information about intelligence practices. Collectively, the IC has provided "greater transparency—albeit at [a] high-altitude level of detail—without compromising the effectiveness of intelligence operations."[34] This all helps strengthen the bond of trust between the intelligence community and the public it protects.

IV. Reforms Already Undertaken Since the 2012 Reauthorization

Since Congress last reauthorized the FISA Amendments Act in 2012, 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,[35]
- Requiring better documentation of the foreign-intelligence purpose of NSA and CIA queries of 702 data using U.S.-person identifiers,[36]
- Enhancing the FISC's ability to review 702 targeting practices and U.S.-person query terms used by the NSA and CIA,[37]
- Periodically reassessing whether upstream collection under Section 702 uses the best available technology to ensure that only authorized communications are collected,[38] and
- Making publicly available the current NSA, CIA, and FBI minimization procedures for Section 702.[39]

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,[40]
- Expanding appellate review of FISC decisions,[41]
- Releasing to the public, to the extent consistent with national security, past and future FISC decisions in cases presenting significant or novel issues,[42] and

- Allowing private companies subject to FISA orders to provide the public with more detail about the volume of surveillance orders they receive.[43]

Finally, at least two significant changes have resulted from the oversight of the Foreign Intelligence Surveillance Court:

- Recently, FISC oversight led the NSA to end so-called "about" collection—that is, collection of messages that mention a targeted selector but are neither to nor from a targeted selector—under 702's "upstream" component. This is discussed in greater detail below.
- The FISC required the FBI to record and report to the court each time a database query using a U.S.-person identifier in a non-national-security criminal investigation returns 702 data.[44] ODNI recently declassified the overall number of such instances in Calendar Year 2016, revealing that only one such FBI query returned 702-acquired data.[45]

V. CIVIL LIBERTIES CONCERNS

Even with the many legal, oversight, and compliance safeguards in place, Section 702, like any powerful government authority, implicates Americans' civil liberties and privacy. Members are right to explore these concerns and consider ways to mitigate them. At the same time, with the United States and our allies confronting grave transnational threats, including terrorism, foreign spying and subversion, and state-backed cyber intrusions, Congress should ensure that any reforms undertaken do not reduce our intelligence community's ability to combat these threats.

This section considers some of the key privacy and civil liberties concerns associated with Section 702 and suggests ways to address them without diminishing 702's effectiveness.

Strengthening Oversight Institutions

One relatively simple way for Congress to strengthen public trust surrounding 702, with no cost to intelligence and counterterrorism, is to bolster the institutions that oversee it. While Congress itself is the ultimate overseer of all intelligence programs, institutions in other branches also play an important role.

As noted above, the USA Freedom Act authorized the Foreign Intelligence Surveillance Court to appoint a cleared amicus curiae in significant cases. One of these advocates, Amy Jeffress, participated constructively in the FISC's review of the government's 2015 certifications for the Section 702 program.[46]

Under current law, however, whether to appoint an amicus is in the court's discretion.[47] The court appears not to have appointed an amicus in the most recent series of hearings on 702. Congress could strengthen public confidence that 702 is receiving rigorous judicial testing by mandating the appointment of a cleared amicus curiae in every review of annual certifications under Section 702. 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. Just as importantly, it would not hamper the government's ability to use 702 to nimbly confront security threats.

In recent years, the Privacy and Civil Liberties Oversight Board has been an essential source of public-facing oversight and accountability for the government's implementation of Section 702. Unfortunately, the Board now lacks a quorum, leaving it unable to take official action. That means that the Board has been unable, among other things, to update its valuable Recommendations Assessment Reports, the last of which was published in February 2016.[48]

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."[49] Since 2013, the Board has become an important feature of the oversight landscape for counterterrorism and surveillance programs. Most valuable for the public have been the Board's public reports—particularly its report on Section 702, which enhanced public understanding by declassifying many basic facts about how the program operates.

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.[50]

Unfortunately, with only one of five Senate-confirmed members remaining, it lacks a quorum and thus cannot take official action. Another institutional challenge is that without a Chairman, the Board has been unable to hire new staff since last summer. The Board's remaining member, Elisebeth Collins, and Board staff have worked diligently to continue the Board's existing projects and strengthen the Board's institutional capacity. In the long term, however, a sub-quorum status is not sustainable.

As it reauthorizes Section 702, Congress also has an opportunity to strengthen the Board and enhance its future effectiveness. The most pressing challenge is the Board's lack of members, a problem that has dogged the Board since its inception ten years ago. The new administration should be given time to address the vacancies it inherited. In the long term, if persistent vacancies prove to be a recurrent problem, I have elsewhere suggested ways Congress could incentivize the Executive Branch to prioritize appointments to the Board.[51]

In the meantime, to enhance the Board's functioning, Congress should exempt the Board from the Government in the Sunshine Act. The Board's organic statute already contains Board-specific transparency requirements, so the generic requirements in the Sunshine Act are superfluous here. Specifically, the Sunshine Act 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."[52] 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.[53] 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.[54]

Incidental Collection

The most significant privacy concerns associated with Section 702 arise from 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 communicate with a targeted non-U.S. person, or if their communications are part of a "multiple communication transaction" that includes a message to or from a targeted non-U.S. person.[55]

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."[56]

Some Members of Congress 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.[57] 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.[58] On balance, however, this limited harm would be justified by the benefits an estimate of incidental collection would produce for public debate—*if*, that is, a statistically valid, feasible methodology of conducting such an estimate can be found.

The rub is that 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 reliably 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. Nonetheless, it is worth continuing to attempt to surmount these obstacles, even if no practicable solution is ultimately found.

That said, the pursuit of an all-encompassing estimate should not distract from other, more targeted ways to measure 702's effect on Americans. Specifically, 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."[59] 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.[60]

As of last February, NSA had implemented Recommendations 9(4) and 9(5) and has reported these figures in the intelligence community's annual transparency report. It has, however, "confronted a variety of challenges" in implementing the other three.[61] As it works toward reauthorizing Section 702, Congress should ensure that NSA continues working to implement Recommendation 9, and should encourage the maximum public reporting of these figures that is consistent with national security.

"About" Collection

The debate over incidental collection should not overlook an important recent change that "should reduce the number of communications acquired under Section 702 to which a U.S. person or a person in the United States is a party."[62] Until recently, under the program's upstream component, NSA collected from internet backbone cables messages not only to or from a tasked selector (such as an email address), but also messages *about* the tasked selector—that is, messages "in which the tasked selector is referenced within the acquired Internet transaction," even though "the target is not necessarily a participant in the communication."[63] According to the Privacy and Civil Liberties Oversight Board, for technical reasons, "'about' collection," as this practice is known, "is necessary to acquire even some communications that are 'to' and 'from' a tasked selector."[64] Courts have held that FISA permits "about" collection, although that legal interpretation is disputed.[65]

Because "about" collection had a higher chance of pulling in some wholly domestic messages, the NSA's court-approved minimization procedures for Section 702 prohibited analysts from using U.S.-person identifiers to query data collected under upstream. It was recently revealed, however, that NSA analysts were including upstream in such queries around 5% of the time.[66] These were serious compliance incidents, which NSA investigated and eventually self-reported to the FISC. The apparent cause was a system design that "automatically defaulted" to include upstream, placing the onus on analysts to remove it from their search criteria.[67] After attempting to remedy these compliance problems, NSA ultimately opted to end "about" collection, thus limiting upstream collection "to internet communications that are sent directly to or from a foreign target."[68]

Some have proposed amending the statute to permanently bar "about" collection. This would freeze NSA's methods in place based on the current limitations of its technology, preventing NSA from resuming "about" collection (and thus collecting those communications to or from a target that, for technical reasons, can only be gathered through "about" collection) even if it finds a technological solution to the associated privacy challenges. The FISC's evident vigilance, and willingness to impose consequences, with respect to "about" collection and related compliance issues suggest that the court is capable of managing this issue flexibly as technology evolves.

U.S.-Person Queries

Perhaps the most contentious issue 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. The greatest concerns have surrounded the FBI's federated database queries. 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 traditional FISA.[69]

While the Foreign Intelligence Surveillance Court has held that such queries comport with the Fourth Amendment,[70] they nonetheless raise legitimate privacy concerns—particularly if such information flows downstream into the criminal justice system. As Gen. Michael Hayden recently quipped, "even to this former director of NSA, using U.S. person data to query lawfully collected foreign intelligence is a not trivial privacy question."[71] But blocking intelligence agencies from detecting connections between pieces of information they already possess would be the wrong way to address those concerns.

Specifically, Congress should not require agencies to obtain a court order before searching their own databases for 702 information about U.S. persons.[72] 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 about the hijackers that different agencies possessed. In short, the government failed to "connect the dots" in time to disrupt the attacks.[73] That failure was particularly pronounced across what the Commission termed the "foreign-domestic divide"—that is, the separation between foreign intelligence and domestic law enforcement. Within the Justice Department and FBI, many believed that the Bureau "could not share any intelligence information with criminal investigators" (the infamous "wall"), with the result that "relevant information from the National Security Agency and the CIA often failed to make its way to criminal investigators."[74] These information-sharing

blockages contributed, among other near-misses, to the tragic failure to locate hijacker Khalid al Mihdhar, whom the government knew had entered the United States.[75] Had Mihdhar been found and interrogated, the government might well have foiled the 9/11 attacks.[76]

Imposing a warrant requirement for U.S.-person queries would, for the first time since 9/11, move us back toward the information "stovepipes" that prevented agencies from connecting the dots and stopping the 9/11 attacks.[77] This will impede counterterrorism, increasing the risk of terrorist attacks in the United States. Some may be willing to accept that risk, but we should be under no illusions: imposing a warrant requirement for database queries would make the homeland less secure.

Another factor weighing against such a requirement is that the available evidence does not suggest that such queries are frequently pulling foreign-intelligence data into routine criminal investigations. This year's intelligence community transparency report revealed that an FBI U.S.-person query retrieved 702-acquired information in an ordinary criminal investigation in *only one* case in 2016.[78] In that case, "an FBI analyst reviewing 702 information found an email message in which a person in the United States gave detailed descriptions of violent, abusive acts" involving children.[79]

This count confirms the FBI's statement to the Privacy and Civil Liberties Oversight Board 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."[80] 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."[81] But in the rare case where there is a connection between a person under FBI scrutiny in the United States and information the Bureau has already received from 702 collection—including the communications of known terrorists—it is important for the FBI to be aware of that.

In sum, given what we now know to be the limited scale of this practice, a warrant requirement would be an overcorrection, with significant costs for counterterrorism. Enhanced transparency and oversight of these queries are a better way to address privacy concerns.

A productive first step in reaching a better-informed public discussion of these queries would be for the FBI to publicly explain in greater detail why it is important for it to continue to conduct these queries. In so doing, it should also explain why other investigative techniques would not be as effective. To be sure, I believe that there are persuasive explanations on both points, and have done my best to approximate them here. But more information about the role these queries play in FBI investigations and the suitability of possible alternatives—from those best informed about them, and whose operations would be most affected by any change—could help strengthen the public legitimacy of current querying practices.

Second, to ensure that the increased transparency surrounding these queries continues, Congress could codify the requirement that the FBI track and 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."[82] This would not impose any additional administrative

burden on the FBI: The FISC already requires the Bureau to report each of these instances to the Court,[83] and the intelligence community, to its credit, chose to publish the overall number of such occurrences (one) in this year's statistical transparency report.[84]

Third, Congress should ask the Bureau to consider whether an alternative form of these queries, in a limited set of cases, would meet its investigative needs. Specifically, the FBI should consider and explain whether it would be sufficient for it to continue its current querying practices, but, where a query "not designed to find and extract foreign intelligence information" returns 702 data, to initially view only the responsive metadata rather than the content. (There is some evidence that such a two-step process should be technically feasible: Where a query conducted by a non-FISA-trained analyst returns FISA information, the FBI's systems notify the analyst that responsive data exists, but require supervisory approval to view the underlying content.[85]) If metadata suggests a problematic connection, that could be used to establish individualized suspicion to view the underlying content and to deploy other investigative tools in the FBI's arsenal.

Finally, and perhaps most importantly, Congress should require increased public transparency about the downstream use in the criminal-justice system of information derived from Section 702. Reforms to the government's use of 702 information in the courts, unlike new barriers to querying and analysis within the intelligence community, should not harm counterterrorism, counterintelligence, cyberdefense, or other intelligence missions.

Specifically, 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[86]—would qualify as "serious crimes" for which the government would use 702 information as evidence.[87] 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.[88]

Leaks and Unmasking

Recent controversies involving foreign intelligence programs, though not specific to Section 702, have made the political climate for reauthorization more challenging. Like the other civil liberties issues discussed above, these are legitimate concerns and should not be brushed aside. At the same time, these concerns can and should be addressed without undermining Section 702 or other lawful and valuable intelligence activities.

Unfortunately, leaks of classified information remain a consistent problem. Illegal disclosures have repeatedly harmed ongoing intelligence programs.[89] More recently, a disturbing new trend has emerged: Leaks of information from classified foreign-intelligence intercepts, with the aim of harming politically active American citizens. For example, Members of Congress have rightly objected to the leak of classified information about former National Security Adviser Michael Flynn's phone calls with the Russian ambassador.

Such leaks are a breach of the trust and confidence reposed in those granted access to signals-intelligence reporting. "Americans entrust their government with these powers on the understanding that they will be used for legitimate purposes alone—and not turned inward against

those they are meant to protect."[90] The misuse of intelligence intercepts for political purposes recalls the bad old days before the Church and Pike Committees and the reforms of the 1970s. Selective leaking of intelligence information for political purposes must not become the norm.

The most obvious remedy is for the Justice Department to find and prosecute those responsible. Congress can and should use its oversight powers to ensure that this is a priority. If Congress wishes to take legislative action, it could consider enacting a new criminal prohibition or sentencing enhancement for leaks of information about U.S. persons collected under foreign-intelligence authorities. While leaks of classified information are already illegal, a specific prohibition covering leaks about U.S. persons would further reinforce the norm that this behavior is unacceptable.

Some have also raised concerns about reports that former senior officials requested unmasking of the identities of Trump transition aides mentioned in intelligence reports. The standard for unmasking—whether the U.S. person's identity is necessary to understand foreign intelligence information or assess its importance—is broad and subjective, and thus vests significant discretion in those who apply it.[91] Whether any individual unmasking request was inappropriate depends on the surrounding facts and circumstances, most of which are classified. Members of Congress and Executive Branch officials with access to the classified context for each request are right to inquire further.

At the same time, it is important to recognize that dissemination of unmasked U.S. person identities is often necessary and valuable.[92] Indeed, it can benefit the U.S. person: For example, a U.S. person (including, under FISA, a U.S. company or association) may be the victim or intended target of an act of terrorism, cyberintrusion, financial crime, or recruitment by a foreign intelligence service. In such cases, the identity enables intelligence and law-enforcement officials to protect the U.S. person from a foreign threat. In other cases, a U.S. person may be involved, wittingly or unwittingly, in such activities, making that person or entity a legitimate subject of foreign intelligence concern.

Any legislative response to alleged political unmasking should be narrowly tailored to address that problem, and should employ post hoc accountability mechanisms rather than creating new, up-front bureaucratic hurdles for unmasking requests, which could obstruct legitimate and valuable intelligence sharing. For example, Congress could require after-the-fact audits and reporting to the relevant congressional committees of all unmasking requests concerning (i) elected officials, or (ii) known associates of political campaigns or transition teams.

VI. Section 702 in International Perspective

Since 2013's illegal disclosures, 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 early last year to find a replacement to the U.S.-EU Safe Harbor agreement demonstrates that this leverage is significant.[93]

But while it is in the U.S. national interest to reduce conflict with Europe over surveillance policy, 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 2013 leaks are not well known in Europe and have generated little goodwill for the United States. Moreover, European allies benefit directly from Section 702 by way of intelligence sharing from our intelligence community. The problem is that European security services have little incentive, and ample domestic political disincentive, to publicize this cooperation.

Instead, the United States should encourage a comparison between our privacy and oversight regime and Europe's. Our government has made commitments to respect the privacy rights of Europeans that far outstrip anything European nations have offered 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.[94] 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.[95] More importantly, some of our European allies are known to engage in aggressive economic espionage against U.S. companies for the benefit of their own economic "national champions"—a practice the U.S. has long forsworn.[96]

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."[97] 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."[98] None of these countries' laws explicitly require minimization, while retention limits apply only to a few narrow categories of data.[99]

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 encouraging a comparison between U.S. surveillance authorities and the applicable legal constraints, oversight mechanisms, and transparency requirements, and the analogous programs of other countries—particularly countries that have criticized the United States for its surveillance practices.

Thank you again for the opportunity to testify.

* * *

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] *Id.* at 2.

[6] *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").

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

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

[9] *Id.* at 2.

[10] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016*, at 7 (hereinafter "CY 2016 Statistical Transparency Report"); Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2015*, at 5.

[11] CY 2016 Statistical Transparency Report, *supra* note 10, at 4.

[12] PCLOB 702 Report, *supra* note 4, at 10.

[13] *Id.*

[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] ODNI Fact Sheet, *The FISA Amendments Act: Q&A*, at 4 (Apr. 18, 2017), *at* https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

[16] *See United States v. Mohamud*, No. 14-30217 (9th Cir. Dec. 5, 2016) (affirming conviction).

[17] ODNI Fact Sheet, *supra* note 15.

[18] PCLOB 702 Report, *supra* note 4, at 10.

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

[20] *See* 50 U.S.C. § 1881a(g).

[21] *See* 50 U.S.C. § 1881a(i).

[22] *See infra* note 28.

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

[24] *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.

[25] *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

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

[27] *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.

[28] *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").

[29] *Available at* IC On the Record, *Release of the FISC Opinion Approving the 2016 Section 702 Certifications and Other Related Documents* (May 11, 2017).

[30] *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).

[31] PCLOB 702 Report, *supra* note 4, at 71-73.

[32] *See infra* note 66.

[33] CNAS Surveillance Policy Report, *supra* note 6, at 14.

[34] CNAS Surveillance Policy Report, *supra* note 6, at 33.

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

[36] *Id.* at 18.

[37] *Id.* at 19.

[38] *Id.* at 21.

[39] *Id.* at 23.

[40] *See* 50 U.S.C. § 1803(i).

[41] *See* PCLOB Recommendations Assessment Report, *supra* note 35, at 5-6.

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

[43] *See id.* at 10.

[44] *See* 2015 FISC Opinion, *supra* note 28, at 78.

[45] *See* Adam Klein, *Today's Big News About "Backdoor Searches,"* Lawfare, May 2, 2017, at https://www.lawfareblog.com/todays-big-news-about-backdoor-searches.

[46] *See generally* 2015 FISC Opinion, *supra* note 28.

[47] *See* 50 U.S.C. § 1803(i).

[48] *See supra* note 35.

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

[50] 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.

[51] *See* Adam Klein, Prepared Statement Before the House Committee on the Judiciary, Hearing on Section 702 of the Foreign Intelligence Surveillance Act, at 9 (Mar. 1, 2017), *available at* https://www.cnas.org/publications/congressional-testimony/adam-klein-before-the-house-judiciary-committee.

[52] 5 U.S.C. § 552b.

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

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

[55] *See* PCLOB 702 Report, *supra* note 4, at 87.

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

[57] 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.

58 *See* PCLOB 702 Report, *supra* note 4, at 147.
59 *Id.* at 146-147.
60 *Id.* at 146.
61 PCLOB Recommendations Assessment Report, *supra* note 35, at 25.
62 Memorandum Opinion and Order, at 62 n.51 (F.I.S.C. Apr. 26, 2017)
63 PCLOB 702 Report, *supra* note 4, at 37.
64 *Id.* at 38.
65 *Id.* at 37-38 & note 137.
66 NSA/CSS Inspector General Report 7 (Jan. 7, 2016), *available at* https://www.dni.gov/files/documents/icotr/51117/NSA_IG_Report_1_7_16_ST-15-0002.pdf.
67 *Id.* at 8.
68 NSA Press Release, *NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702* (Apr. 28, 2017), *at* https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml.
69 PCLOB 702 Report, *supra* note 4, at 59.
70 2015 FISC Opinion, *supra* note 28.
71 *Quoted in Expert View: Changing NSA's Email Collection Program*, The Cipher Brief, May 2, 2017, *at* https://www.thecipherbrief.com/article/exclusive/cipher-brief-expert-view-changing-nsas-email-collection-program-1091.
72 *See* Charlie Savage, *Fight Brews Over Push to Shield Americans in Warrantless Surveillance*, N.Y. Times, May 6, 2017, *available at* https://www.nytimes.com/2017/05/06/us/politics/congress-surveillance-nsa-privacy.html (reporting that a "bipartisan coalition of privacy-minded lawmakers" is considering "a new requirement that a warrant be obtained to search for Americans' information" collected under 702).
73 *9/11 Commission Report* at 355-356.
74 *Id.* at 79.
75 *Id.* at 269-272.
76 *See id.* at 272 (concluding that detention of Mihdhar or Nawaf al Hazmi "could have derailed the plan").
77 *Cf., e.g., Final Report of the William H. Webster Commission on the FBI, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009*, at 32 (2012) ("[O]ur investigation found that … consolidating and conforming the contents of these diverse databases are vital to the FBI's ability to respond to the threat of terrorism.").
78 *See* Klein, *supra* note 45.
79 Memorandum Opinion and Order, *supra* note 62, at 64-65 (F.I.S.C. Apr. 26, 2017). This case usefully illustrates how U.S.-person queries of 702 information can sometimes benefit the U.S. person: The analyst queried 702 data using the name of the apparent victim, as well as the suspected abuser.
80 PCLOB 702 Report, *supra* note 4, at 60.
81 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.
82 *See* 2015 FISC Opinion, *supra* note 28, at 78.
83 *See id.*; *see also* DOJ/ODNI Semiannual Assessment, *supra* note 30, at 16.
84 *See supra* note 78.
85 *See* CNAS Surveillance Policy Report, *supra* note 6, at 37.
86 *See, e.g.*, *United States v. Nosal*, Nos. 14-10037 & 14-10275 (9th Cir. Dec. 8, 2016).
87 *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 6, at 38.
88 *See* 50 U.S.C. § 1806(c); 50 U.S.C. § 1881e(a).
89 *See* CNAS Surveillance Policy Report, *supra* note 6, at 17-18.

[90] Adam Klein, *It's Not About Mike Flynn*, Lawfare, Feb. 17, 2017, *at* https://lawfareblog.com/its-not-about-mike-flynn.

[91] *See* Adam Klein, *Don't Dismiss Concerns About Transition-Period Unmasking (At Least Not Yet)*, Lawfare, Apr. 14, 2017, *at* https://www.lawfareblog.com/dont-dismiss-concerns-about-transition-period-unmasking-least-not-yet.

[92] *Cf.* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016*, at 13 (NSA 702 reports contained 1,200 unmasked U.S. person identities; in 1,934 other instances, NSA later "unmasked" a U.S.-person identity in response to a specific request).

[93] *See id.* at 57.

[94] *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/.

[95] *See* CNAS Surveillance Policy Report, *supra* note 6, at 53.

[96] *See id.* at 56.

[97] 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.

[98] *Id.* at 37.

[99] *Id.* at 51.