Hearing before the Senate Committee on the Judiciary

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

Matthew G. Olsen
Former Director, National Counterterrorism Center
Former General Counsel, National Security Agency

June 27, 2017

I. Introduction

Thank you Chairman Grassley, Ranking Member Feinstein, and distinguished members of the Committee. I am honored to have this opportunity to appear before you to discuss the reauthorization of the FISA Amendments Act (FAA) and, in particular, Section 702.

As the former director of the National Counterterrorism Center, I can attest to the fact that the FAA has proven to be an essential authority for the collection of foreign intelligence to guard against terrorism and other threats to our national security. Section 702 has significantly contributed to our ability to prevent terrorist attacks inside the United States and around the world.

Moreover, as the former general counsel of NSA and as a former senior official in the Justice Department's National Security Division, I was responsible for helping to ensure that the government's implementation of the FAA complied with the law and protected privacy and the civil liberties of Americans. As the Committee is aware, the FAA is subject to oversight and review by all three branches of government, as well as independent reviews by the Privacy and Civil Liberties Oversight Board (PCLOB). These reviews have concluded that the government is properly using its authority under the FAA to conduct foreign intelligence collection.

Enacted in 2008, Congress reauthorized the FAA in 2012. Since the passage of the FAA, and through its extension, this Committee has played an essential role in overseeing the government's use of these surveillance authorities. I appreciate the Committee's decision to hold this hearing today to consider the renewal of this authority, and hope to contribute to the Committee's efforts.

I also am pleased to join with colleagues who bring significant experience and a range of perspectives to the issues surrounding the FAA. For my part, I will focus on the operational aspects of 702, and will begin by describing the complex threat landscape facing the country today. I then will explain the importance of Section 702 to our counterterrorism activities and address a few of the key issues about Section 702. Finally, I will describe the compliance and oversight structure in place to protect civil liberties and privacy.

II. Threat Landscape

Our discussion of FAA-authorized intelligence collection takes place in the context of a persistent and complex threat environment. Thus, to appreciate the value of Section 702, it is important to take a moment to describe the threats the United States faces from terrorist groups and operatives.

Over the past several years, the United States has made significant progress against core al-Qaida leadership, but the range of threats we face from al-Qaida linked groups has become increasingly diverse and geographically expansive. The continuing appeal of the jihadist narrative and the adaptive nature of these groups pose substantial challenges to the efforts of our counterterrorism community.

Without question, the so-called Islamic State, or ISIS, presents the most urgent terrorist threat to our security today. The group has exploited the conflict in Syria and sectarian tensions in Iraq to entrench itself in both countries, now spanning the geographic center of the Middle East. ISIS's sanctuary, while diminished through the efforts of the U.S.-led coalition, enables the group to recruit, train, and execute external attacks—as we have now seen across Europe and the Middle East—and to incite assailants around the world. It has recruited thousands of militants to join its fight in the region and uses its propaganda campaign to radicalize countless others in the West.

Since September 2014, ISIS has reportedly claimed credit for more than 40 terrorist attacks outside of its self-proclaimed caliphate. Several of these attacks were conducted directly by ISIS, where the attackers trained with ISIS in Syria and Iraq. These include the 2015 Paris attack (130 killed) and the 2016 Brussels attack (32 killed), both of which demonstrated that ISIS has both the intent and capability to execute sophisticated and deadly attacks in Western Europe. About 10 of these attacks are best described as ISIS-enabled, where the assailants were in direct communication with ISIS planners and handlers, according to reports. In some of these cases, an ISIS planner acted as advisor and confidante to the attacker. In the balance of cases, it appears that the attackers were simply inspired by ISIS propaganda to carry out the attack, such as the succession of attacks this year in the United Kingdom.

In the United States, the threat from ISIS is on a smaller scale but persistent. We have experienced attacks that ISIS has inspired—including the attacks in San Bernardino and in Garland, Texas—and there has been an overall uptick over the past year in the number of moderate-to-small scale plots. Lone actors or insular groups—often self-directed or inspired by overseas groups, like ISIS—pose the most serious threat to carry out attacks here. Homegrown violent extremists are likely to continue to carry out simpler plots that do not require advanced skills or outside training. The online environment—where potential extremists here interact with ISIS handlers and recruiters—serves a critical role in radicalizing and mobilizing homegrown extremists towards violence. Highlighting the challenge this presents, the FBI has homegrown violent extremist cases, totaling about 1000, in every state. Most of these cases are connected to ISIS

Several factors are driving the trend toward the increasing pace and scale of terrorist violence. First, the sheer number of Westerners who have gone to Iraq and Syria to fight in the

conflict and to join terrorist groups, including ISIS, supplied a steady flow of operatives to the groups. More than 6,000 foreign fighters from the West—including many French, German, British, and Belgian nationals—have travelled to Iraq and Syria to join the fight. This is part of more than approximately 38,000 foreign fighters who have traveled to the region since 2011. Among the estimated thousands who have since departed Iraq and Syria, hundreds have returned to their home countries, battle-hardened and trained in explosives, with access to networks that may be planning attacks in the West. The number of Americans who have travelled to Syria or Iraq, or have tried to, exceeds 285.

As a consequence, we should recognize the potential for an ISIS-directed attack in the United States. While the principal threat from ISIS in the United States is from homegrown, ISIS-inspired actors, the fact that so many Americans have travelled to Syria and Iraq to fight, along with thousands more in Europe, raises the real danger that these individuals could be deployed here to conduct attacks similar to the attacks in Paris and Brussels.

Second, ISIS has developed more advanced tactics in planning and executing these attacks. In both Brussels and Paris, the operatives staged coordinated attacks at multiple sites, effectively hampering police responses. The militants exploited weaknesses in Europe's border controls in order to move relatively freely from Syria to France and Belgium. The group has also moved away from previous efforts to attack symbolically significant targets—such as the 2014 attack on a Jewish museum in Brussels—and appears to have adopted the guidance of a senior ISIS operative in the group's online magazine, who directed followers "to stop looking for specific targets" and to "hit everyone and everything." Further, the explosives used in Paris and likely in Brussels indicate the terrorists have achieved a level of proficiency in bomb-making.

Third, existing networks of extremists in Europe are providing the infrastructure to support the execution of attacks there. The investigations of the Paris and Belgium attacks revealed embedded radical networks that supply foreign fighters to ISIS in Syria and operatives and logistical support for the terrorist attacks in those cities. While such entrenched and isolated networks are not present in the United States, ISIS continues to target Americans for recruitment, including through the use of focused social media and encrypted communications, in order to identify and mobilize operatives here.

Looking more broadly, the rise of ISIS should be viewed as a manifestation of the transformation of the global jihadist movement over the past several years. We have seen this movement diversify and expand in the aftermath of the upheaval and political chaos in the Arab world since 2010. Instability and unrest in large parts of the Middle East and North Africa have led to a lack of security, border control, and effective governance. In the last few years, four states—Iraq, Syria, Libya, and Yemen—have effectively collapsed. ISIS and other terrorist groups exploit these conditions to expand their reach and establish safe havens from where they can carry out external attacks.

III. The Role of Section 702

Against this backdrop of a dynamic and lethal terrorism threat, the ability of the United States to conduct surveillance under Section 702 is vital to our security. Through the surveillance of communications under this authority, the government gains information that is

often unavailable from other sources about the identities of terrorists, their networks, and their plans and capabilities. This surveillance allows the government to peer inside highly secretive terrorist organizations that are difficult to penetrate and to obtain unvarnished intelligence about how these groups operate and seek to carry out attacks, often long before plots are executed.

The Background of Section 702. In describing the value of Section 702 it is important to provide some background about why Congress modified FISA nine years ago by crafting Section 702 and related provisions. Since 1978, when FISA was first enacted, through the late 1990s, the government was authorized to conduct the vast majority of its overseas-focused intelligence collection without the need to obtain individualized court orders.

However, this changed with the shift of long-haul communications from satellites to undersea cables in the 1990s. Because the scope of FISA was defined in part by the technology of the 1970s, this meant that the government was often forced to seek individualized court orders based on probable cause from the Foreign Intelligence Surveillance Court (FISC) to acquire the communications of foreign terrorists or other foreign intelligence targets overseas. This technological change turned nearly 20 years of collection practice under FISA on its head, and the trend continued to accelerate through the early 2000s. In the aftermath of the 9/11 attacks, it became clear that this approach to foreign intelligence collection was becoming untenable, even as the terrorist threat to our nation was growing.

As the Deputy Assistant Attorney General from 2006 to 2009 overseeing DOJ's foreign intelligence surveillance programs, I experienced first-hand the adverse consequences of this pre-FAA approach. In some cases, it simply was not possible to demonstrate probable cause that a proposed target overseas was a "foreign power" or an "agent of a foreign power," as required under FISA's Title I provisions, which were designed to protect U.S. persons. Of course, as courts repeatedly have held, non-U.S. persons outside the United States are not entitled to the protections of the Fourth Amendment.

Second, as the number of foreign intelligence targets overseas increased due to the growing terrorist threat, it was not practical to obtain individualized court orders on a routine basis. And this is true today more than ever, as the terrorist threat has diversified and expanded, including with the recruitment by ISIS of individuals to wage jihad around the globe. This was a significant burden on the Executive and Judicial Branches before the FAA was enacted in 2008—diverting finite resources to cases where Fourth Amendment protections simply did not apply—and would overwhelm the system now.

Last, even where the government was able to demonstrate probable cause, the pre-FAA approach proved cumbersome and slow. As described below, the significantly more agile targeting requirements under Section 702 have contributed to the government's ability to maintain coverage of terrorists who actively seek to evade surveillance and to rapidly move to collect intelligence about newly discovered targets. In short, Section 702 authorizes the government, consistent with the Constitution, to obtain critical intelligence about terrorists and other targets that it cannot obtain through any other practical means.

The Value of Section 702 Collection. As the Director of NCTC from 2011 to 2014, I relied on a daily basis on intelligence collected under Section 702. NCTC serves as the hub of

terrorism information, analysis, and operational planning for the federal government. Section 702 collection was instrumental to our efforts to discern the intentions and capabilities of our terrorist adversaries, contributing both to our strategic judgments and tactical insights.

In the NCTC morning briefings, analysts frequently reported that a critical piece of intelligence was obtained through FAA collection. And I often relied on Section 702 collection in my briefings and updates to other government officials and to the National Security Council.

The Intelligence Community as a whole consistently has emphasized the critical value of Section 702 collection. In a hearing before the Senate Intelligence Committee earlier this month, intelligence community leaders reaffirmed the importance of this authority. In their joint statement, these officials affirmed that "Section 702 provides critical foreign intelligence that cannot practicably be obtained through other methods." The Director of National Intelligence pointed to the "highly valuable and often unique intelligence" that Section 702 has provided. The intelligence community has called the reauthorization of Section 702 its top legislative priority this year, and warned that "[l]osing these authorities would greatly impair the ability of the United States to respond to threats and to exploit important intelligence collection opportunities.

The PCLOB's comprehensive review of the Section 702 program also emphasized the value of this collection. The PCLOB concluded:

> [Section 702] has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

According to the PCLOB, since 2008 the number of signals intelligence reports based in whole or in part on Section 702 has increased exponentially, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. As of 2014, over a quarter of the NSA's reports concerning international terrorism included information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. Moreover, the flexibility of Section 702 collection, according to the PCLOB, enables the government to maintain coverage on particular individuals as they add or switch their modes of communications.

Based on its review of classified information, the PCLOB identified approximately 30 specific cases in which Section 702 information was the initial catalyst that identified previously unknown terrorist operatives or plots. In the typical case, as described in the PCLOB report, the government used Section 702 to conduct targeted surveillance of a specific foreign individual overseas based on the reasonable belief the individual was involved with terrorist activities. This narrowly focused surveillance led to the discovery of a specific plot. The government next engaged in a short, intensive period of further investigation, leading to the identification of associates and the arrest of the plotters. As a result, Section 702 led to the arrest of more than

100 individuals on terrorism-related offenses.

Several specific cases, now declassified, highlight the value of Section 702.

- Counterterrorism analysts at NSA used Section 702 to support a tactical operation against a terrorist leader in Iraq and Syria. Section 702 enabled the analysts to develop a detailed picture of the personal network of the terrorist. This terrorist practiced strict operational security, and only by building out his network of operatives was NSA able to track his movements. Section 702 collection provided the necessary information for tactical teams to conduct a successful military operation, removing the terrorist from the battlefield.

- In September 2009, NSA analysts relied on Section 702 to target an email address used by a suspected al-Qaida courier in Pakistan. Based on this surveillance, NSA discovered a message sent to an individual in the United States, subsequently identified as Najibullah Zazi, who was urgently seeking advice on how to make explosives. Further investigation revealed that Zazi and a group of operatives had imminent plans to bomb the New York subway. The FBI and local law enforcement officials arrested Zazi and his confederates and stopped the attack before it could be executed.

- In 2014, a federal judge sentenced Mohamed Osman Mohamud to 30 years in prison for attempting to carry out a plot to detonate a car bomb at a Christmas tree lighting ceremony in Portland. The FBI based its investigation of Mohamud in part on Section 702 collection. The government was targeting the email account of a foreign national overseas with whom Mohamud was in contact. The FBI was able to use the collection of the email communications between the target overseas and Mohamud in the United to obtain a FISA warrant to surveil Mohamud and his activities, ultimately leading to his arrest and conviction.

- In another example, NSA conducted surveillance under Section 702 of an email address used by a suspected extremist in Yemen. This surveillance led NSA to discover a connection between the extremist and an unknown person in Kansas City, Missouri, who was then identified as Khalid Ouazzani. The FBI's follow-up investigation revealed that Ouazzani was connected to other al-Qaida associates in the United States, who were part of an earlier plot to bomb the New York Stock Exchange. All of these individuals were prosecuted and pled guilty to terrorism offenses.

Beyond the United States, Section 702 has proven to be invaluable in supporting the counterterrorism efforts of our allies. Among the specific cases the PCLOB reviewed, in which Section 702 assisted in ongoing terrorism investigations or provided warnings about continuing threats, the vast majority of these cases involved operatives and plots in foreign countries, including many in Europe. In these cases, the United States shared Section 702 information with our foreign counterparts to support their efforts.

For example, CIA used Section 702 collection to uncover details, including a photograph, that enabled a partner in Africa to arrest two ISIS-affiliated operatives. The operatives had traveled from Turkey and were involved in planning a specific and immediate threat against U.S. personnel. Information recovered from the arrest enabled CIA to obtain actionable intelligence on an ISIS facilitation network and ISIS attack planning.

Given the increasing reach of ISIS and the transnational nature of jihadist groups, the ability of the United States to collect and share intelligence collected under Section 702 has proven to be essential.

Incidental Collection. One issue that has arisen in considering the reauthorization of Section 702 is the "incidental collection" of U.S. persons who are in communication with the overseas targets of Section 702. Section 702 prohibits the government from targeting a U.S. person anywhere in the world, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the United States.

Congress, in enacting Section 702, however, authorized the government to acquire and, when appropriate, to retain and use communications in which a U.S. person is in contact with a foreign target located overseas. This is often referred to as "incidental collection," because it is not accidental or inadvertent, but rather an anticipated consequence of monitoring an overseas target: a person targeted for surveillance who speaks on the phone or communicates over the Internet may often be communicating with someone else who is not a target.

The ability to collect and use such communications has proven be indispensable to our counterterrorism efforts. In the Mohamud, Zazi and Ouazzani cases, for example, the government's collection of the communications of operatives inside the United States, as a consequence of their contacts with Section 702 targets located overseas, was critical to the disruption of plots and to the arrest of al-Qaida operatives here. "Incidental collection" under Section 702 enabled the government to identify suspects and to use other investigative tools, including traditional FISA authority, to advance its investigations. The intelligence community has committed to provide additional information about the scope of "incidental collection" under Section 702. But Congress should resist calls to restrict the government's ability to acquire and use such communications involving U.S. persons.

Queries of Section 702 Data. Under Section 702, intelligence agencies are permitted, with certain restrictions, to query the collection under this authority to find information about specific U.S. persons. While some have complained that such searches are "backdoors" around the Fourth Amendment, these queries are an essential and lawful means for analysts to identify critical intelligence that could otherwise be inaccessible.

From an operational perspective, when intelligence analysts seek to identify terrorist operatives and uncover specific plots, one of their first steps is to check existing databases for potential connections to suspected terrorists. Section 702 is one of the most important sources of such information. This is particularly true for the FBI, which is on the front lines of identifying homegrown terrorists who may have been in communication with suspected terrorist operatives and militants who seek to inspire attacks here. If the FBI suspects that a person in the United States has been radicalized and is mobilizing toward violence, the ability to query existing databases, including Section 702 data, enables the FBI to move quickly to identify communications that the government has already lawfully collected and to find relevant intelligence, without having to sift through each individual communication it has in its databases.

This approach reflects an enduring lesson from the 9/11 attacks: it is imperative for the government to effectively integrate and use the relevant counterterrorism information it holds in disparate government databases. As the 9/11 Commission pointed out, the government failed to "connect the dots"—missing key clues and connections located in the intelligence information it had already collected and failing to fuse information across the foreign-domestic divide. In this light, it is essential for the FBI and other intelligence agencies to be able to effectively access and use as a first line of inquiry the Section 702 data stored in its databases.

Importantly, Section 702 minimization safeguards restrict the ability of analysts to query the databases that hold Section 702 information using an identifier, such as a name or telephone number, that is associated with a U.S. person. For NSA and CIA, queries of Section 702 information are only permitted if they are reasonably designed to identify foreign intelligence information. The FBI also may conduct such queries to identify evidence of a crime, but only agents with the required training are permitted to review the results of these queries. As part of Section 702's oversight, DOJ and ODNI review all U.S. person queries of content to ensure they satisfy these standards.

Some are now urging Congress to impose a probable cause warrant requirement on intelligence agencies before they can search Section 702 data with U.S. person identifiers. In my view, this would undermine the ability of intelligence analysts and agents to move quickly to identify potential threat information. As noted, database checks are typically among the first steps investigators take to determine whether further inquiry is necessary. At this early stage, investigators likely would not be able to establish probable cause and therefore such data would be beyond their reach.

Moreover, a query of a databases containing Section 702 information does not result in any new acquisition of data. Rather, this search instead only involves the review of previously acquired information. Thus, adopting a warrant requirement to search Section 702 data would be contrary to a central lesson from 9/11 by imposing unjustified restrictions on the government's ability to seamlessly identify terrorist connections in the data it has lawfully collected. Indeed, the FISC considered this issue last year and concluded that the FBI's querying procedures strike a reasonable balance between the privacy interests of U.S persons and national security interests, and were consistent with the Fourth Amendment.

IV. Compliance and Oversight

When Congress enacted Section 702 in 2008, it established an unprecedented and comprehensive compliance and oversight regime for Section 702. This approach reflected a careful balancing of the need both to collect vital intelligence and to safeguard privacy and civil liberties. Under this regime, which has been enhanced over the past several years through both congressional and Executive branch action, all three branches of government exercise authority to ensure that the government's use of 702 is consistent with the Constitution, the laws of the United States, and the privacy and civil liberties of Americans around the globe.

Executive branch agencies that implement Section 702 play a central role in ensuring the authority is used properly. This begins with workforce training: NSA, CIA, and the FBI all require personnel involved in targeting decisions to complete training on applicable procedures and policies. At NSA, all Section 702 targeting decisions are reviewed at least twice before collection, and all such decisions are reviewed again by the Department of Justice and NSA compliance officers. Moreover, officials from DOJ's National Security Division and the Office of the Director of National Intelligence exercise broad oversight of NSA, FBI, and CIA activities under Section 702—including reviews of targeting and minimization decisions—generally conducting on-site reviews once every two months. Based on these reviews, the Attorney General and DNI conduct semi-annual compliance assessments, which are routinely provided to Congress and reviewed in detail by the relevant committees.

The judicial branch, through the FISC, is responsible for reviewing the certifications the Attorney General and DNI submit to ensure that the collection under Section 702 is properly aimed at non-U.S. persons located outside the United States for foreign intelligence purposes. The FISC conducts rigorous reviews of the government's targeting and minimization procedures for compliance with the requirements of the statute and the Fourth Amendment. Further, the FISC receives extensive reporting about the operation of Section 702 collection and any compliance incidents. The FISC, when it deems appropriate, requires the government to provide additional information and testimony to ensure that the court has a full understanding of the operation of the Section 702 program. Based on my many years of experience as a federal prosecutor, I have found the FISC to be active and assertive in reviewing, evaluating, and conducting oversight on the surveillance cases it handles, contrary the characterization of the court as a "rubber stamp.

In April 2017, the FISC issued an opinion, which has been publicly released in redacted form, concluding that the government's most recent certifications under Section 702 were consistent with FISA and the Fourth Amendment. In making this determination, the court scrutinized the government's compliance record over the past year, which included several specific compliance incidents, as well as the government's amendments to its proposed certifications. Similarly, in November 2015, the FISC issued an 80-page opinion, concluding that the government's proposed 702 certifications, including the associated targeting and minimization procedures, met all statutory requirements and were consistent with the Fourth Amendment. These decisions exemplify the FISC's significant role in overseeing the government's use of Section 702.

Congress's oversight of Section 702 is an important component of the program's

operation. Pursuant to the FAA, the Attorney General reports twice every year to this Committee and to the Intelligence Committees about the implementation of Section 702. These reports include copies of all certifications and significant pleadings and court orders, as well as descriptions of any compliance matters. These congressional committees also receive assessments from the Attorney General and DNI about the government's adherence to targeting and minimization procedures. Beyond these required submissions, the government engages in ongoing interaction with this Committee and the Intelligence Committees in the course of their active oversight of Section 702.

The government's careful implementation of Section 702 was confirmed in the PCLOB's landmark 2014 report. The PCLOB found no evidence of intentional abuse of Section 702. The Board observed that it was "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" and concluded that "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."

V. Conclusion

In sum, the authority Congress established under Section 702 has played an indispensable role in protecting the nation from terrorist threats. The counterterrorism community, facing a diverse and complex threat landscape, has increasingly relied on the speed, agility, and effectiveness of surveillance conducted under Section 702. And in operating this program under a strict compliance and oversight regime, the government has demonstrated that it can collect vital intelligence in a manner that protects privacy and the civil liberties of Americans.

I urge the Committee to reauthorize Section 702 to ensure that our intelligence and law enforcement communities have the tools they need to defend the nation.