STATEMENT OF

KENNETH L. WAINSTEIN
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

THE REAUTHORIZATION OF THE FISA AMENDMENTS ACT

PRESENTED ON

MAY 10, 2016

STATEMENT OF
KENNETH L. WAINSTEIN
PARTNER, CADWALADER, WICKERSHAM & TAFT LLP

CONCERNING

THE REAUTHORIZATION OF
THE FISA AMENDMENTS ACT

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

MAY 10, 2016

Chairman Grassley, Ranking Member Leahy and distinguished Members of the Committee, thank you for the invitation to appear before you today. My name is Ken Wainstein, and I'm a partner at the law firm of Cadwalader, Wickersham & Taft. I spent many hours testifying before you and other committees during Congress' deliberations leading to the passage of the FISA Amendments Act in 2008 as well as its reauthorization in 2012. It is an honor to be back here once again to support the Act's reauthorization and to discuss the issues it raises with my distinguished fellow panelists.

I. Introduction

Before going into the intricacies of the FISA Amendments Act and its reauthorization, it's important to remind ourselves about the national security threats – and particularly, the threat from international terrorism – that this legislation addresses. Since the attacks of September 11, 2001, we and our allies have been at war with terrorist organizations around the globe – including al Qaeda and its affiliates and the Islamic State (ISIS) – as well as with individuals – like the San Bernardino shooters – whom these organizations have inspired. While we have significantly degraded their effectiveness with strikes against their leadership and operational personnel, they continue to pose a serious threat to the U.S. and our allies.

While many institutional and operational improvements have contributed to that progress over the past decade, none has been more instrumental than the overall enhancement in our intelligence capabilities. We can see the fruits of that effort regularly in the newspaper. Every successful strike against ISIS leaders happens because we have sound intelligence telling us where and when we can find the targets. And every plot prevention happens because we now have a developed network of surveillance capabilities, human assets and international partnerships that provides us insight into our adversaries' planning and operations that we simply did not have before 9/11.

A critical component of our counterterrorism effort – and, for that matter, any investigative effort – is the capability to intercept our adversaries' communications. From my earliest days as a prosecutor investigating narcotics networks here in the District of Columbia, I learned that electronic surveillance can be a tremendous source of intelligence about the inner workings of a conspiracy. That is particularly true in relation to foreign terrorist groups, where leaders and foot soldiers in different parts of the world have to rely on electronic communication for operational coordination.

In recognition of this fact, much of our intelligence effort since 9/11 has focused on tapping into the communication streams of our terrorist adversaries. The government has taken a number of steps to enhance our electronic surveillance capacity over the last fifteen years – refining our collection technologies and devoting more resources and manpower to the effort. But the one development that has contributed the most to that effort was Congress' decision to modernize our national security surveillance efforts by passing the FISA Amendments Act (FAA) in 2008 and reauthorizing it in 2012.

Since its implementation, FAA-authorized surveillance has been absolutely critical to detecting and understanding the threats we face. That was the case when I was reviewing FAA-derived reporting as Homeland Security Advisor in 2008, and it apparently still is the case today. According to a recent Administration briefing of this Committee, the FAA continues to provide "critical foreign intelligence that cannot practicably be obtained through other methods [and that is] vital to our national security."[1]

II. Background of the FISA Amendments Act

In once again considering reauthorization of the FAA, it is important to remind ourselves why it was necessary to modernize the Foreign Intelligence Surveillance Act in the first place.[2] As you know, FISA was passed in 1978 in the aftermath of the Church Committee hearings, which disclosed the flagrant misuse of national security surveillances against dissidents, civil rights groups and other domestic organizations. These revelations persuaded Congress that the Executive should no longer have unilateral authority to conduct domestic national security

---

[1] Briefing on the FISA Amendments Act Before the S. Comm. on the Judiciary, 114 Cong. 9 (2016) (joint statement of Robert S. Litt, Gen. Counsel of the Office of the Dir. of Nat'l Intelligence, Stuart J. Evans, Dep. Asst. Att'y Gen. for Intelligence, U.S. Dept. of Justice, Michael B. Steinbach, Ass. Dir. Counterterrorism Div., Federal Bureau of Investigation & Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, National Security Agency).

[2] For a more comprehensive discussion of the FAA's background and the operational problems it was designed to address, see my testimony at the following hearings: May 1, 2007 Hearing Before the Senate Select Committee on Intelligence Concerning the Need to Bring the Foreign Intelligence Surveillance Act Into the Modern Era; September 6, 2007 Hearing Before the House of Representatives Permanent Select Committee on Intelligence Concerning the Foreign Intelligence Surveillance Act; September 18, 2007 Hearing Before the House of Representatives Committee on the Judiciary Concerning the Foreign Intelligence Surveillance Act; and October 31, 2007 Hearing Before the Senate Committee on the Judiciary Concerning the Foreign Intelligence Surveillance Act.

surveillance and that its use of those surveillance powers should be subject to a process of judicial review and approval.

To effectuate this objective, Congress passed FISA, which established the Foreign Intelligence Surveillance Court – or "FISA Court" – and required by its terms that any "electronic surveillance" of foreign powers or their agents must first be approved by the FISA Court. In crafting this law, however, Congress recognized that it had to balance the need for a judicial review process for domestic surveillance against the government's need to freely conduct surveillance overseas. It accomplished that objective by clearly distinguishing between surveillances directed against persons located within the United States – where constitutional protections apply – and those directed against persons outside the United States, where the Fourth Amendment does not apply. It then imposed the court approval requirement on surveillances directed against persons within the United States and left the Intelligence Community free to conduct surveillance on overseas targets without the undue burden of court process.[3]

The drafters of FISA built that distinction into the statute through its definition of "electronic surveillance," which is the statutory term designating the range of surveillance activities that are subject to the court approval requirement. The statute required the examination of a number of factors – such as the location and nationality of the surveillance target – in determining whether a particular surveillance falls within that definition and the coverage of the statute. Among those factors was the type of communications technology being used by the target – i.e., whether he was communicating by "wire" or "radio." Given that "radio" (satellite) technology was commonly used for international calls at the time and "wire" technology was the norm for domestic calls, it arguably made sense that FISA distinguished between "radio" and "wire" communications in designating which surveillances were sufficiently domestic in character that they would be subject to the court approval requirement and which would be excluded because they targeted foreign communications that did not enjoy Fourth Amendment protection. The result was a technology-based carve-out for surveillances targeting foreign-based communications.

With the change in technology over the intervening years, however, that carve-out started to break down. In particular, the development of a world-wide network of fiber optic "wire" communications resulted in an increasing number of phone calls and emails passing through the United States, whose interception in the United States required court review under the definition of "electronic surveillance." As a result, the government found itself expending significant manpower generating FISA Court applications for surveillances against persons outside the United States – the very category of surveillances that Congress specifically intended to exclude when it imposed the FISA Court approval process in 1978.

---

[3] The report of the House Permanent Select Committee on Intelligence accompanying the passage of FISA clearly acknowledged the infeasibility of imposing a court approval process for NSA's overseas collection and expressed its desire to exclude surveillances of persons overseas from FISA's scope. As it explained, "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances." H.R. Rep. No. 95-1283, at 27 (1978).

With the dramatic increase in counterterrorism surveillance efforts after 9/11, the requirement to obtain a court order for foreign surveillances started to severely strain the Intelligence Community. As a result – and as reported by Intelligence Community professionals at the time – the government expended significant resources with the approval process for these surveillances and was increasingly forced to make tough choices regarding surveillance of worthy counterterrorism targets.

To its enduring credit, Congress recognized that this situation was unacceptable in a post-9/11 world, and in the spring of 2007, it undertook to study how FISA could be revised to bring it more in line with the threats and realities of today's world. Over the next 15 months, the Intelligence and Judiciary Committees held dozens of hearings and briefings – many of which I attended – in which Members sought input and debated how to revise FISA in a way that relieved the Intelligence Community from having to seek individualized FISA orders for overseas surveillances yet retained the court review requirement for those domestic surveillances that directly implicated the Fourth Amendment concerns underlying FISA.

III. The FISA Amendments Act

After considering a number of options and passing stopgap legislation – the Protect America Act – to provide temporary relief for the Intelligence Community, Congress ultimately passed the FISA Amendments Act in July 2008. After further discussion and debate, Congress reauthorized the FAA in December 2012. In both cases, Members from both parties worked in a bipartisan fashion to craft a law that was a significant step forward for both national security and civil liberties.

The statute amended FISA in the following three ways:

1. Approval Process for Surveillances of Foreign Persons Located Overseas

The most significant provision in the FISA Amendments Act is Section 702, which authorizes the FISA Court to approve surveillance of categories of terrorist suspects and other foreign intelligence targets overseas without requiring the government to provide an individualized application as to each particular target. The statute prescribes a new, streamlined process by which categories of overseas targets are approved for surveillance. Under this process, the Attorney General and the Director of National Intelligence (DNI) provide the FISA Court annual certifications identifying the categories of foreign intelligence targets to be subject to this surveillance and certifying that all statutory requirements for that surveillance have been met. The Intelligence Community designs "targeting procedures" for the surveillance categories, which are the operational steps it takes to determine whether each individual surveillance target is outside the United States and therefore subject to this non-individualized collection process. It also draws up "minimization procedures" that lay out the limitations on the handling and dissemination of any information from that surveillance that may identify or relate to U.S.

persons.[4] The government submits the Attorney General and DNI certifications as well as the targeting and minimization procedures for review by the FISA Court. The FISA Court then decides whether to approve the surveillances, based on its assessment whether all statutorily-required steps have been taken in compliance with FISA and the Fourth Amendment.

This process succeeds in bringing the operation of FISA back in line with its original intent. It allows the government to conduct overseas surveillance without individualized court approval while at the same time giving the FISA Court an important role in ensuring that this authority is used only against those non-U.S. persons who are "reasonably believed to be located outside the United States."

2. Oversight of the Implementation of the Surveillance Authority

In addition to requiring FISA Court approval of the certifications and procedures, the FAA tasks various levels of government with conducting oversight over this authority. For example, it directs the Attorney General to adopt guidelines that ensure Section 702 is not used against targets who do not qualify for this surveillance. It tasks the Attorney General and the DNI with conducting and submitting to the FISA Court and Congress a semi-annual assessment of compliance with the statutory requirements. It specifically authorizes the relevant Inspectors General to review compliance with the procedures and guidelines. And it directs the head of each participating Intelligence Community agency to conduct an annual review of the surveillance effort, and to provide that review to the FISA Court and the Intelligence and Judiciary Committees of Congress.

3. Requirement of an Individualized Court Order to Conduct Surveillance on U.S. Persons Overseas

The FAA also added to the protections for U.S. persons in a very significant way. The FAA imposed the requirement, for the very first time, that the government seek and obtain an individualized order from the FISA Court whenever it seeks to conduct overseas intelligence collection on a U.S. person while that person is outside the United States. While the Attorney General previously approved such collection against any U.S. person overseas pursuant to Executive Order 12333, the FAA now obligates the government to seek court approval and demonstrate to the satisfaction of the FISA Court that there is probable cause to believe that the U.S. person target is acting as a foreign power or as an agent, officer, or employee of a foreign power.

In sum, the FISA Amendments Act was a well-calibrated piece of legislation. It provided the Intelligence Community relief from the expanding scope of FISA requirements and spared

---

[4] Following the issuance of Presidential Policy Directive-28, Signals Intelligence Activities, the Intelligence Community also applies minimization protections to personal information of non-U.S. persons collected pursuant to Section 702. *See e.g.*, FEDERAL BUREAU OF INVESTIGATION, PRESIDENTIAL POLICY DIRECTIVE 28 POLICIES AND PROCEDURES (Feb. 2, 2015), *available at* https://www.fbi.gov/about-us/nsb/fbis-policies-and-procedures-presidential-policy-directive-28-1.

the government from filing applications for overseas surveillances that do not implicate the Fourth Amendment. At the same time, it adhered to the original purposes of FISA, maintaining the individualized court review requirement for surveillances directed within the United States and even expanding it to surveillances of U.S. persons outside the country. Moreover, it directed all three branches of government to provide robust oversight to ensure that this authority is implemented in full compliance with FISA and the Constitution.

IV. Intelligence Community Compliance With the FAA

Over the past few years, the leaks by Edward Snowden and the government's transparency efforts have revealed an Intelligence Community committed to compliance with the law. Since 2008, the government has informed the FISA Court of incidents in which the NSA collected information in non-compliance with the FAA. As the government explained, all of these incidents were apparently mistakes and oversights, and none reflected intentional misuse of the FAA authority – a conclusion that was echoed by the findings of the Privacy and Civil Liberties Oversight Board ("PCLOB"), which conducted its own review of the Executive's intelligence collection operations under Section 702 and found that "internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements."[5] The absence of any findings of intentional misconduct over the past eight years is a testament to the Intelligence Community's commitment to compliance.

V. Conclusion

In supporting reauthorization, I ask Congress to focus on the three considerations that have been the focus of my remarks: (1) the vital importance of the FAA surveillance authority to our counterterrorism efforts; (2) the extreme care with which Members of Congress considered, crafted and limited the authority when they passed the FAA in 2008 and reauthorized its provisions four years ago; and (3) the findings that this authority has been implemented to great effect and in compliance with the law and Constitution.

In addition to these considerations, we must also focus on other important consideration – the severity of the terrorist threat that we still face today. While we have certainly weakened them in many ways, our terrorist adversaries still pose a serious danger to our national security, as evidenced by the recent ISIS-inspired attack in San Bernardino that killed 14 Americans and wounded 22 more. Both ISIS and al Qaeda continue to plan attacks against us, as well as against our allies, as we have seen with the recent attacks in Paris and Brussels.

Given that continuing threat, now is not the time to weaken our defenses or scale back on a critical intelligence authority like the FISA Amendments Act. To the contrary, now is the time to ensure that our Intelligence Community operators have the surveillance authorities they need

---

[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 77 (2014), *available at* https://www.pclob.gov/library/702-Report.pdf.

and to reauthorize a statute that has done so much to protect our people and their liberties over the past eight years.

Thank you for giving me the opportunity to speak about this important matter, and I look forward to answering any questions you may have for me.